UNIVERSIDAD INTERNACIONAL DE LA RIOJA

Universidad Internacional de La Rioja

Máster universitario en Seguridad Informática

METODOLOGIA ACRD PARA LA GESTION DE SEGURIDAD EN ENTORNOS VIRTUALES

Trabajo Fin de Máster

Presentado por: Chahin Noreña, Juan Antonio

Director/a: Sierra Cámara, José María

Ciudad: Santa Marta

Fecha: 24 de septiembre del 2015.

Resumen

La virtualización es una tecnología en pleno crecimiento. Cada día toma más fuerza la virtualización de servidores, escritorios, medios de almacenamiento y aplicaciones. Virtualizar sistemas de información, es sinónimo de ahorro en energía, espacio físico y recursos económicos.

Mantener protegidos y disponibles los activos de información en los entornos virtuales, es un reto al que se enfrentan los administradores de los centros de cómputo, puesto que existen brechas en la seguridad que no alcanzan a ser cubiertas por los actuales sistemas utilizados para mitigar amenazas.

Este trabajo de fin de Master, contempla una metodología que permita llenar los vacíos existentes e identificados, en la seguridad de los ambientes virtuales. Para tal fin se realiza un estudio de conceptos y vulnerabilidades específicas que giran en torno a la virtualización. Se analizan los sistemas de gestión de riesgos existentes y se enuncia una metodología que recoge una serie de buenas prácticas, que se deben de utilizar en la implementación de máquinas virtuales.

Con el presente trabajo se intenta demostrar que los estándares y normas de seguridad que se aplican para sistemas de información instalados en medios físicos, no cubren todos los riesgos que implica la virtualización. Para tal fin se presenta una prueba de concepto para reforzar esta tesis y se desarrolla un piloto experimental en donde se aplican los procedimientos expuestos, en la metodología propuesta.

Palabras Clave: Virtualización, Recursos, Información, Seguridad, Metodología.

Abstract

Virtualization technology is growing. Each day takes more strength virtualization of servers, desktops, storage media and applications. Virtualize information systems, it stands for saving energy, space and financial resources.

Keep information assets in virtual environments protected and available, it is a challenge that managers of data centers face, since there are security gaps that fail to be covered by existing systems used to mitigate threats.

This final project Master, provides a methodology to fill identified gaps in security of virtual environments. To this end a study of concepts and specific vulnerabilities revolve around virtualization is done. Management systems risks are analyzed and a methodology that includes a number of good practices that should be used in the implementation of virtual machines is stated.

The present paper attempts to demonstrate that the standards and safety regulations that apply to information systems installed on physical media, do not cover all the risks of virtualization. To that end proof of concept it is presented to reinforce this theory and experimental pilot where the procedures outlined in the proposed methodology is applied develops.

Keywords: Virtualization, Resources, Information Security Methodology.

ÍNDICE DE CONTENIDO

RESUMEN.....2
ABSTRACT…….....3
1. INTRODUCCIÓN.....9
1.1. ANTECEDENTES.....10
1.2. MOTIVACIÓN….....12
1.3. PLANTEAMIENTO DEL TRABAJO.....14
1.4. ESTRUCTURA DEL TRABAJO.....18
2. ESTADO DEL ARTE…….....20
2.1. HISTORIA DE LA VIRTUALIZACION…….20
2.2. TIPOS DE VIRTUALIZACION.....21
2.3. EL HIPERVISOR……24
2.4. COMPARATIVA DESDE EL PUNTO DE VISTA DE LA SEGURIDAD ENTRE UN ENTORNO INFORMATICO REAL Y UNO VIRTUAL……..29
2.5. LA EVOLUCION DE LOS ENTORNOS VIRTUALES……..31
2.6. LAS AMENAZAS QUE ENFRENTAN LOS ENTORNOS VITUALES……...32
3. OBJETIVOS Y METODOLOGÍA DE TRABAJO……...36
3.1. OBJETIVO GENERAL.....36
3.2. OBJETIVOS ESPECÍFICOS DE LA METODOLOGIA A DESARROLLAR.....36
4. DESARROLLO DE LA METODOLOGIA……....37
4.1. METODOLOGIAS PARA LA GESTION DE SEGURIDAD PARA ENTORNOS VIRTUALES…….37
4.1.1. MAGERIT……..37
4.1.2. METODOLOGIA OCTAVE…….39
4.1.3. METODOLOGIA MEHARI……..40
4.2. APLICACION DE L NORMA ISO 27001 EN ENTORNOS VIRTUALES……...40
4.3 .LA NORMA ISO/IEC 27018……46
4.4. MODELO ZERO-TRUST DE FORRESTER……47
4.5. METODOLOGIA ACRD PARA EL CONTROL DE RIESGOS DE SEGURIDAD EN AMBIENTES VIRTUALES…….48
4.5.1. AISLAR……..48
4.5.2. CONTROLAR……...49
4.5.3. REAUTENTICAR…….50

4.5.4. DETECTAR……..50
5. PUESTA EN MARCHA DEL PILOTO EXPERIMENTAL ……..…51
5.1. DESARROLLO DEL ENTORNO VIRTUAL…….……51
5.2. INSTALACION DEL HIPERVISOR……..51
5.3. GESTION DE GRUPOS Y VOLUMENES……..55
5. 4. CREACION DE MAQUINAS VIRTUALES…….57
5.5. APLICACIÓN DE LA METODOLOGIA ACRD……61
5.5.1. AISLAR LAS VM……..61
5.5.2. CONTROL DE LOS RECURSOS EN LAS VM.……66
5.5.3. ACCESO CON DOBLE FACTOR DE AUTENTICACION…….68
5.5.4. DETECCION DE TRAICO ENTRE LAS VM.……68
5.5.5. PRUEBAS Y VALIDACION DE RESULTADOS…….70
5.5.5.1. PRUEBA DE AISLAMIENTO Y CONTROL DE RECURSOS……70
5.5.5.2. PRUEBA DE CONTROL DE ACCESO A MAQUINAS VIRTUALES……73
5.5.5.3. PRUEBA DE DETECCION DE TRÁFICO EN EL ENTORNO VIRTUAL……76
6. CONCLUSIONES Y TRABAJO FUTURO……..79
6. 1. CONCLUSIONES……..79
6.2. TRABAJO FUTURO……...80
7. GLOSARIO……..81
8. BIBLIOGRAFIA…..…….84

INDICE DE IMÁGENES

Figura 1. Fases del desarrollo de la virtualización……..…….10
Figura 2. Comparativa del coste de una aplicación instalada en un entorno virtual y no virtual……..……..12
Figura 3. Estructura básica de un entorno virtual……..15
Figura 4. Estructura de trabajo de XEN Hipervisor……...17
Figura 5. Ilustración del concepto básico del proceso de virtualización……21
Figura 6. Virtualización por hardware……..……...22
Figura 7. Diferencias entre Full Virtualización y Para-virtualización……..……23
Figura 8. Virtualización a nivel de sistema operativo……..……24
Figura 9. Virtualización de aplicaciones……..……...24
Figura 10. Papel del hipervisor XEN en un ambiente Virtual……..25
Figura 11.- Hipervisor Tipo 1: Bare metal……...26
Figura 12.- Hipervisor Tipo 2: Hosted……26
Figura 13. Anillos de privilegio para la arquitectura x86……27
Figura 14. La restauración en máquinas reales y virtuales……31
Figura 15. Comercialización de alquiler de servidores virtuales en Millones de Dólares…...32
Figura 16. Atacante a todo el sistema con la ayuda una VM y del mismo Hipervisor…….34
Figura 17. Distribución de las vulnerabilidades en un entorno virtualizado……..35
Figura 18. Elementos para el análisis de riesgos potenciales Metodología Magerit……..38
Figura 19. Distribución del disco duro para el Piloto experimental……48
Figura 20. Esquema básico del sistema de volúmenes lógicos en Linux……55
Figura 21. Modelo de entradas y salidas de las VM en discos y redes diferentes…….....55
Figura 22. Captura de pantalla de los cuatro volúmenes creados..……57
Figura 23. Listado Máquinas virtuales creadas……..60
Figura 24. Listado con rendimiento de las VM……60
Figura 25. Configuración inicial de red en el Entorno Virtual..……..62
Figura 26. Subred con Bridge br0…….....63
Figura 27. Configuración fichero interfaces…….....64
Figura 28 Con el comando brctl vemos le bridge creado……64
Figura 29 Configuración de red del entorno virtual……...65
Figura 30. Máquinas virtuales apagadas……71
Figura 31. Reporte de actividad en cada VM……...71
Figura 32. Saturación maquina VMubuntu……..71
Figura 33. Acceso denegado por falta de clave pública……74
Figura 34. Generación de clave pública en el escritorio remoto…….....74

Figura 35. Verificación de acceso luego de configurar la clave pública……..75
Figura 36. Acceso remoto denegado, a otra VM del entorno virtual……76
Figura 37. Flujo de tráfico de las Máquinas Virtuales……77
Figura 38. Reporte análisis de trafico Máquinas virtuales……78

INDICE DE TABLAS

Tabla No 1. Información máquinas virtuales……..62
Tabla No 2. Consumo de recursos de las VM en actividad normal……72
Tabla No 3. Maquina VMubuntu saturada……..73

1. INTRODUCCION

La virtualización tiene más de medio siglo de existencia pero en los últimos años ha tomado relevancia en diferentes planos de la actividad humana. Temas como costo, versatilidad y escalabilidad, incide en que muchos gerentes de sistemas de información se decidan por implementar ambientes virtuales para realizar muchas funciones que antes hacían con el hardware tradicional.

El auge de las tecnologías móviles y las redes virtuales contribuyen a que muchas tareas del quehacer humano se puedan realizar a distancia. El comercio, la educación, el trabajo y las relaciones interpersonales en general, pueden prescindir en la actualidad de una presencia física de las entidades que interactúan. Estudios recientes han demostrado que compaginar más activamente la vida laboral con la familiar, aumenta la motivación y eficiencia de muchos empleados.

"El estudio mundial sobre mano de obra realizado en 2008 por la consultora Towers Perrin examinó 50 multinacionales durante un año y relacionó los niveles de empeño de sus empleados con los resultados económicos de la empresa. El estudio descubrió que las empresas en las que los empleados ponen empeño en su trabajo tienen un 19% más de ingresos de explotación que la media, mientras que las empresas con un bajo nivel de motivación ingresan un 32% menos". (Cerda, 2012).

Gracias a la virtualización, tener un puesto de trabajo remoto es perfectamente factible. El problema de emplear un sistema información virtual y distribuido radica en que hay un aumento drástico de la superficie de ataque y las amenazas pueden ser mayores que las que pueden existir en un sistema basado en hardware. Los controles de acceso y la autorización para acceder a recursos deben actuar de una forma más eficiente. El manejo de las máquinas virtuales y el uso de aplicativos a distancia implican una visión integral de todo el sistema en sí, puesto que existe el riesgo que un solo usuario consciente o inconscientemente pueda llegar afectar el rendimiento de todo entorno.

1.1. ANTECEDENTES

Los ambientes virtuales plantean cambios drásticos en la forma como funcionan muchos aspectos de la sociedad, se está estructurando un nuevo paradigma en donde las nuevas tecnologías de la información TICS tienen un papel fundamental en actividades cruciales como el comercio o la educación. Hoy en día la mayor parte de la información que maneja el ser humano esta almacenada en la nube, las empresas están comenzando a implementar la virtualización en sus sistemas de información y en sus centros de procesamiento de datos. Compañías de desarrollo de software ofrecen aplicaciones que corren en la Web, dejando a un lado la forma como anteriormente se usaban y se comercializaban los programas.

A partir del año 2005 se habla de una primera fase en la virtualización en donde se implementan varias Máquinas Virtuales en un servidor físico. En el 2008 surge la segunda fase donde se agrupan varias aplicaciones de producción y se desarrolla aún más el concepto de escritorio virtual. Esta etapa es conocida como virtualización 2.0. En la actualidad nos encontramos en el auge de la virtualización 3.0 que va más allá de los servidores virtuales o de las plataformas de virtualización. Esta virtualización que se presenta como un abanico de servicios, es el desarrollo futuro del concepto y se con el nombre de Cloud Computing.

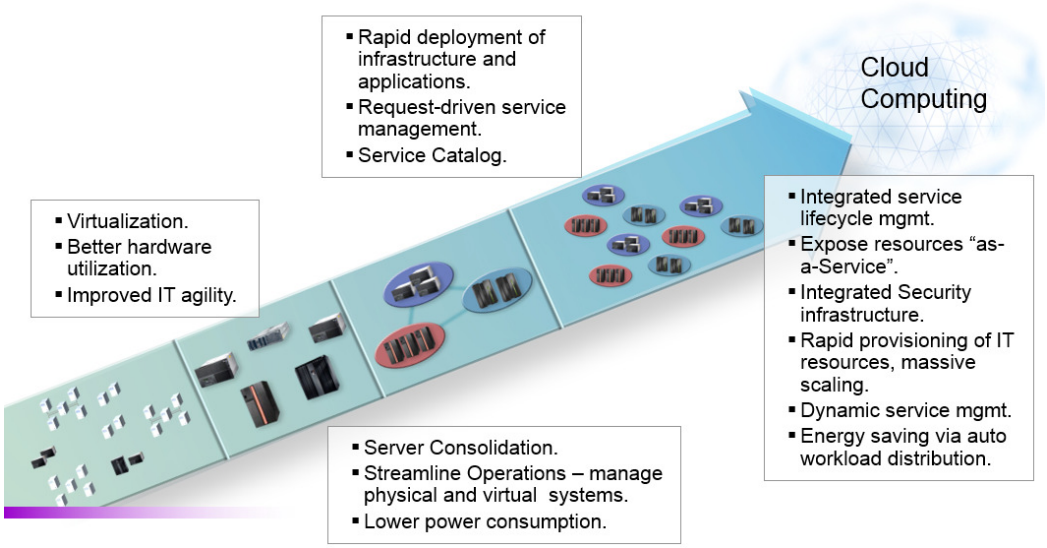

Figura 1. Fases del desarrollo de la virtualización. Fuente. http://www-03.ibm.com/systems/power/software/performance/s.

Los servicios Cloud que pertenecen a esta tercera fase de la virtualización, abundan en internet, dentro lo que ofrecen podemos encontrar equipos virtuales como *Cloud Servers* entre sus características más relevantes tenemos:

- Sistemas de *Raid* con dos o más discos duros.
- servidores virtuales que pueden tener un hardware optimizado (procesadores con más de 10 núcleos, RAM hasta de 128 Gb y conexiones de red de 10 Gbps) se pueden configurar para suplir las labores de procesamiento más exigentes.
- Las Máquinas Virtuales pueden ser configuradas con un hardware acorde a las necesidades de trabajo.
- Escalabilidad en la potencia del hardware, permitiéndonos tener un crecimiento variable a las necesidades de procesamiento, ya sean fijas o temporales.
- Asistencia técnica las 24 horas, administración de la infraestructura y capacitación para que los usuarios aprendan a utilizar los recursos, todo esto a muy bajos costos.

Esta revolución en la forma como se pueden manejar los activos informáticos, plantea un enorme impacto social, económico y cultural. Las empresas se van a ver abocadas a funcionar de una manera diferente, puesto que la perspectiva actual apunta a que no se necesita la presencia física de los sistemas para poder trabajar con ellos.

El hecho que los escritorios puedan ser virtuales plantea la posibilidad de que los empleados no tengan que asistir a la empresa a trabajar, ya que desde la casa, podría acceder remotamente a su puesto de trabajo. El desarrollo de bandas anchas más amplias y que además estén al alcance de todos, beneficia el fácil manejo y acceso a los recursos virtuales. Pero por otro lado, esta entrada remota a las redes virtuales (VPN) implica que debe existir un mayor control de la seguridad en cuanto a las políticas de acceso y un sistema de autenticación de usuarios que vaya más allá de ingresar simplemente, un nombre y una contraseña. Los accesos externos, pueden ser empleados por atacantes, sobre todo cuando se utilizan canales de comunicación inseguros.

Lo que sucede fuera del entorno puede escapar al control de los administradores del sistema, si no existen unas políticas claras en cuanto al uso de normas como los horarios de acceso, la autorización con respecto al manejo de los recursos, los perfiles de los usuarios y los protocolos que se implementen.

Como lo señala Manuel Castells, La era de la información (Castells, 1997), haciendo referencia a los cambios provocados por la digitalización, existe hoy en día una conciencia extendida y mundial sobre la importancia de esta revolución, teniendo presente que aún falta una visión más allá de las particularidades de cada nuevo medio, que nos permita entender la lógica de estos nuevos avances en el presente.

1.2. MOTIVACION.

La motivación que ha impulsado la realización de este trabajo posee dos vertientes una profesional y la otra académica. En primer lugar, en el ámbito profesional el autor ha estado trabajando durante 22 años en la instalación de redes de comunicaciones, servidores y estaciones de trabajo. La virtualización ofrece soluciones que superan en creces los tradicionales centros de cómputo. Instalar un sistema de cableado estructurado y conformar un centro de cómputo con servidores es costoso, en la actualidad se requieren sistemas más eficientes, económicos y que además sean amables con el medio ambiente.

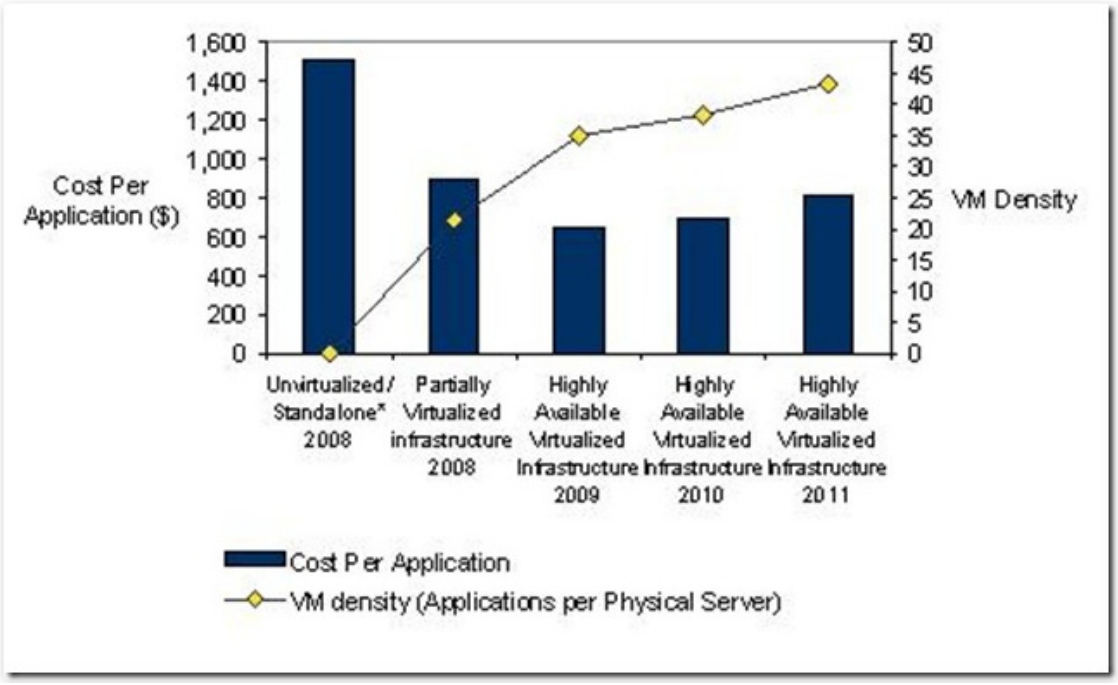

Figura 2. Comparativa del coste de una aplicación instalada en un entorno virtual y no virtual. Fuente. http://blogs.vmware.com/virtualreality/2010/01/the-new-economics-of-a-virtualized-datacenter-moving-towards-an-application-based-cost-model.html

Desde el punto de vista de las aplicaciones la virtualización ofrece una reducción significativa, hasta del 50% del costo por aplicación, al instalarse ésta en un entorno virtual. Este factor ahorro conduce a que esta tecnología, sea aún más atractiva para las empresas. Es importante añadir que esta medida cuantitativa de economía, no incluye otros beneficios de la virtualización, como son el aumento de la productividad de administración, un menor tiempo de recuperación en caso de fallo del sistema y más

agilidad en cuanto al tiempo de respuesta de tecnologías de la información a las necesidades empresariales.

Por otro lado, es un hecho las consecuencias del calentamiento global, en los climas tropicales las altas temperaturas obliga a que los centros de cómputo trabajen con sistemas de enfriamiento las veinticuatro horas del día. Esto implica considerables consumos de energía. Muchas empresas con voluminosas infraestructuras de hardware, están expuestas a invertir en gastos innecesarios por desconocer las ventajas que ofrece la virtualización. Sistemas híbridos con servidores virtualizados, reducirían en gran medida la inversión de recursos económicos en muchas empresas.

Otro aspecto a tener en cuenta, es que las máquinas virtuales pueden ser accedidas desde cualquier lugar con mucha más facilidad que las maquinas físicas, esto facilita el tele trabajo de muchos empleados, pues no necesitarían estar físicamente en la empresa para llevar a cabo sus actividades. En un futuro cercano, la implementación de escritorios virtuales, implicara menos gastos en transporte de personal, menos automóviles circulando en las calles, una menor congestión vehicular que es sinónimo de una menor contaminación ambiental.

Desde el punto de vista tecnológico, el alquiler de servidores virtuales en la Web significa estar siempre a la vanguardia en tecnología. De igual manera las compañías medianas o grandes que necesiten escalar en su infraestructura técnica, lo podrán hacer con más facilidad empleando este tipo de alternativas. La relación costo-beneficio de esta solución es difícil de superar.

El problema para que este panorama idóneo no haya sido tomado en cuenta por muchas empresas, es que existe un paradigma generalizado entre los administradores de sistemas informáticos, puesto que ellos piensan que para las cosas trabajen bien las tienen que ver físicamente funcionando. Se tiene el precepto que no se puede gestionar, ni proteger lo que no se puede ver. Por su misma naturaleza, las máquinas virtuales se pueden mover fácilmente, acarreando problemas de separación y fragmentación de las zonas que se consideran seguras.

El tráfico de red existente entre diferentes máquinas virtuales no atraviesa ninguno de los dispositivos de seguridad perimetral actuales: firewalls, IDS/IPS, analizadores de LOGs, etc. se crean lo denominados "Puntos Ciegos" para la seguridad ya que no se dispone de trazas, registros ni ningún dato acerca del tráfico generado.

Las brechas de seguridad se convierten en una barrera generalizada, que impide que una tecnología que ya existe, no sea considerada formalmente por muchos ingenieros de informática.

De acuerdo a lo comentado anteriormente, el tema a desarrollar gira entorno a una metodología que contribuya a reforzar la seguridad en ambientes virtuales, que es una cuestión crítica para que muchas empresas se puedan sentir seguras con el uso de la virtualización. De igual manera este trabajo tiene como objetivo, desmitificar muchos supuestos de riesgo que supone el uso de máquinas virtuales, de la misma manera está dirigido a los encargados de las Tecnologías de la Información (TI) que se encuentren evaluando soluciones de seguridad para un entorno virtual o mixto.

1.3 PLANTEAMIENTO DEL TRABAJO.

Los ambientes virtuales conllevan riesgos que no son mitigados plenamente con las tradicionales metodologías y arquitecturas de seguridad. El objetivo principal del trabajo es implementar una metodología que permita administrar, analizar y gestionar esos riesgos exclusivos que conlleva la virtualización. Se empleara un piloto experimental para validar los resultados teóricos que se han obtenido al desarrollar la metodología. Demostrar, en lo posible, que los ambientes virtuales pueden trabajar de manera tan segura como los ambientes reales.

El concepto de metodología hace referencia “al camino o al conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. Con frecuencia puede definirse la metodología como el estudio o elección de un método pertinente o adecuadamente aplicable a determinado objeto”. (Wikipedia, 2015)

Bajo este precepto enmarcaremos el trabajo a desarrollar teniendo claros los objetivos a conseguir, objetivos que deberán ser alcanzados por medio de unos procedimientos claros, pertinentes e innovadores los cuales serán validados con un piloto experimental en el que se ponga en marcha una infraestructura típica, con la que un usuario o encargado de un centro de datos, trabaja normalmente en una organización.

La infraestructura a desarrollar contendrá las siguientes características:

- La plataforma será instalada, en una maquina anfitriona, la estructura estará formada por un servidor y tres Máquinas Virtuales. Las VM estarán distribuidos de la siguiente manera: uno para el administrador del sistema, otro para el operador de la aplicación y el último para un operador con menos permisos que el anterior. El entorno virtual estará configurado como muestra la figura 1.

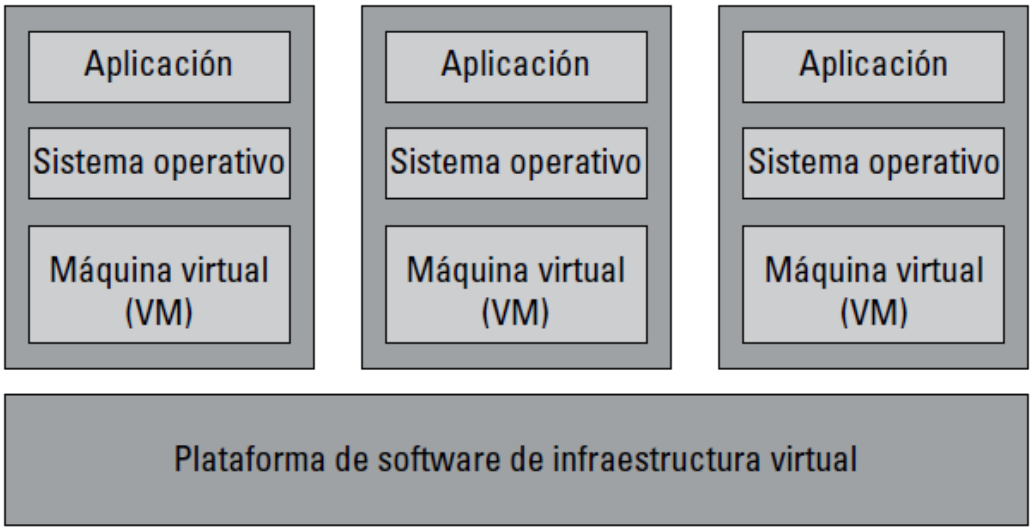

Figura 3. Estructura básica de un entorno virtual.
Fuente. http://www.trendmicro.es/media/br/cloud-virtualisation-security-for-dummies-ebook-es.pdf

- Con la maquina anfitriona se trabajara todo el ecosistema virtual, entre el núcleo de la anfitriona y las VM se tendrá la figura del Hipervisor que estará configurado para gestionar las comunicaciones entre las VM y administrar los recursos del sistema.

- El sistema de virtualización que se va a emplear es el XEN, se escogió este sistema de virtualización por ser open source, funciona con diferentes plataformas de Hardware, se espera trabajar con un Hipervisor tipo uno (Baremetal), de igual manera la selección obedece a que se tiene fácil acceso a los instaladores y que XEN soporta gran variedad de sistemas operativos.

En el año 2003 la Universidad de Cambridge desarrollo un proyecto de investigación cuyo resultado fue, la liberación de la primera versión de XEN. El proyecto estaba liderado por Ian Pratt, quien más tarde creó una empresa de soporte, mantenimiento y capacitación sobre XEN en Enero de 2005.

En la actualidad la empresa es Xensource Inc. Continua con el desarrollo de XEN dedicándose a la programación de aplicaciones adicionales, no libres, para facilitar el uso, instalación y mantenimiento de XEN.

XEN tiene licencia GPL, es código abierto y tanto Xensource como otras empresas importantes en el mercado como son como HP, Sun Microsystems, IBM, AMD, Ontel, RedHat, Novell están involucradas en el mantenimiento y desarrollo de XEN.

Con XEN podemos obtener las siguientes funcionalidades:

- Implementación directa en el hardware: la virtualización de XEN se ejecuta directamente sobre el hardware, en vez de ejecutarse sobre un sistema operativo

- Es el Hipervisor más ligero que se consigue en el medio informático, ocupa tan solo 2MB aproximadamente.

- Una de sus grandes ventajas es que ofrece Virtualización sobre diversos modelos de procesadores INTEL.

- Se pueden conseguir gran variedad de herramientas de seguridad Open Source

- XEN ofrece un gran aislamiento entre máquinas virtuales lo que nos va a permitir parametrizar aún más la gestión de seguridad

- Ofrece soporte para plataformas de 64-bits lo que facilita ejecutar las versiones más recientes de sistemas operativos y productos.

- En XEN los sistemas virtualizados corren directamente sobre el procesador, sin emulación, por lo que obtenemos un rendimiento mucho mayor.

- Las Máquinas virtuales instaladas con XEN pueden dar soporte hasta 8 CPUs virtuales lo que hace posible la instalación incluso de las aplicaciones que requieren un uso

intensivo de CPU y además obtener ventaja de los procesadores actuales que poseen varios núcleos.

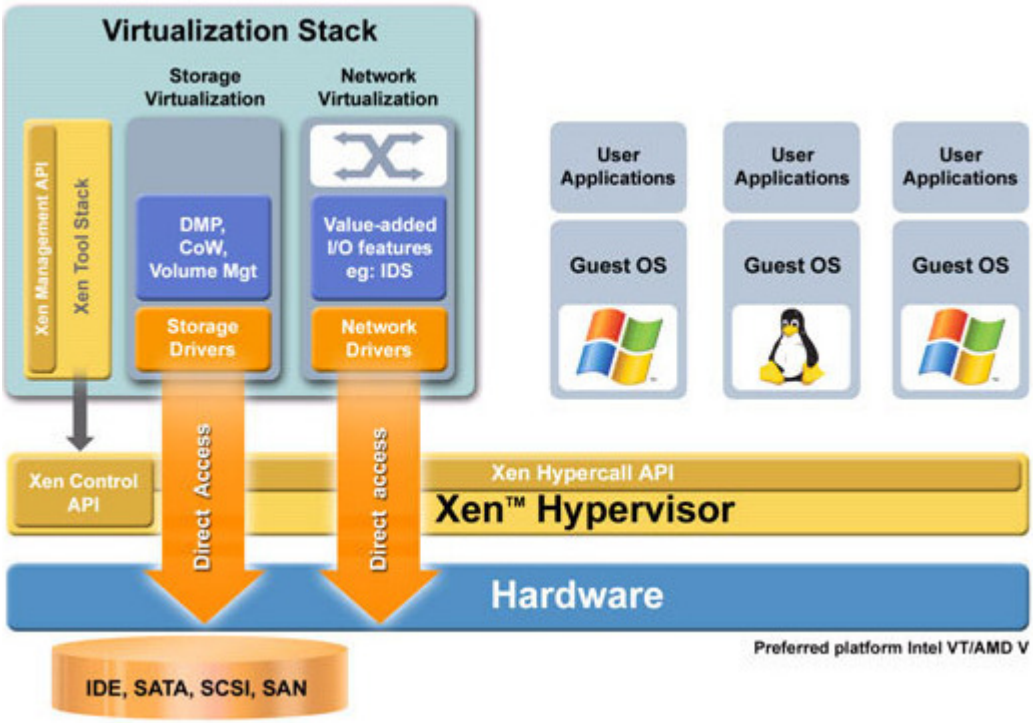

Figura 4. Estructura de trabajo de XEN Hipervisor. Fuente. http://www.opengal.es/xen.html

El sistema debe tener las siguientes funcionalidades para que pueda ser utilizado como experimental y poder poner en práctica la metodología a desarrollar:

- En el ambiente virtual que se va a implementar debe ser posible, para el administrador del mismo, monitorizar, gestionar y proteger los distintos dispositivos que puede contener con las mismas funcionalidades que pueda tener en un ambiente real.

- Los usuarios de la plataforma virtual (Administrador y operarios) podrán acceder ella de forma remota. Esto con el fin de poner a prueba la metodología en cuanto a la gestión de riesgos por acceso remotos.

- El Hipervisor debe ser configurado para que monitorice de forma eficiente las actividades de cada VM. Para conseguir este propósito el Hipervisor debe coordinar las actividades de protección y actualización de software de las VM. De igual manera el tráfico de red debe pasar a través de él y este a su vez reportar al administrador de la plataforma las incidencias que puedan suceder.

- Las plataformas virtuales son susceptibles al consumo excesivo de recursos por replicación de actividades, o por otro lado la inactividad en algunas máquinas virtuales crean brechas de seguridad producto de la no actualización de sistemas operativos y programas antivirus. El sistema debe contar con los mecanismos necesarios para contrarrestar estos y otros problemas de seguridad que conlleva la virtualización.

1.4 ESTRUCTURA DEL TRABAJO

Luego de realizar la introducción sobre el trabajo que se va a llevar a cabo, se presenta la descripción de los distintos capítulos que conforman el presente escrito:

- En el capítulo 2 se presenta el estado del arte en donde afianzamos el tema a desarrollar. El objetivo de este capítulo es ilustrar acerca de la importancia de las tecnologías de virtualización en el mundo empresarial, haciendo una comparativa desde el punto de vista de la seguridad, de los ambientes reales y los ambientes virtuales. Además, se realizara un seguimiento de la forma como ha evolucionado y cuáles son las tendencias actuales de los ambientes virtuales identificando los desarrollos más relevantes hasta el momento.

- El capítulo 3 comprende el objetivo general y los objetivos específicos del trabajo que nos permitirá determinar los resultados concretos que se pretenden alcanzar con el desarrollo de este trabajo.

- El capítulo 4.Corresponde al enunciado de la metodología de gestión de riesgos para ambientes virtuales. Partiendo del marco teórico expuesto analizaremos lo que aporta la norma ISO 27002 con respecto a los 133 controles de gestión de seguridad para sistemas de información. Se buscara identificar metodologías que se puedan aplicar en la seguridad de ambientes virtuales y a partir de aquí plantear una metodología que subsane las brechas de seguridad identificadas.

  De igual manera, en este capítulo se explica la forma como se va aplicar la metodología y de cómo se llevara a cabo el montaje del servidor virtual y las tres VM. Se detallaran las técnicas de control de los dispositivos para prevenir ataques y fallas en la infraestructura. Luego de enunciar la metodología la acoplaremos al estado del arte desarrollado y específicamente con relación al sistema de virtualización XEN y definición de conceptos que van a ser usados en el Piloto experimental como son las capas de virtualización, los tipos de virtualización, la virtualización de máquinas, la virtualización de la red entre otras.

- El capítulo 5 corresponde a la puesta en marcha del piloto experimental, se realizar la instalación del Hipervisor XEN sobre un equipo Debian, por medio del Debian configuraremos las condiciones de disco, el domain0 (Dom0) y el SSH para el acceso remoto de las máquinas virtuales, El Kernel de XEN se instalara sobre el de Debian, de tal manera que a partir de esta instalación tengamos la plataforma de comunicación con el hardware subyacente y poder dar inicio a la creación de la máquinas virtuales (DomU). En el proceso de instalación y configuración del ambiente virtual se pondrá en uso la metodología descrita en el capítulo 4.

- El capítulo 6. trata acerca de las conclusiones que detallan los resultados alcanzadas tras la realización del trabajo. Las pruebas llevadas a cabo sobre el piloto experimental nos van a ayudar a recopilar información, la cual nos permitirá tomar decisiones y a obtener una conclusión sobre los planteamientos iniciales. Para finalizar, se documentara acerca de posibles acciones que pueden ser llevadas a cabo para mejorar la en la infraestructura creada.

2. ESTADO DEL ARTE

2.1 HISTORIA DE LA VIRTUALIZACION

"La virtualización empezó a desarrollarse en la década de 1960 y se utilizó para particionar los mainframes de gran tamaño a fin de mejorar su utilización. En la actualidad, los ordenadores basados en la arquitectura x86(32 bits) tienen que resolver los mismos problemas de rigidez e infrautilización que se planteaban para los mainframes en aquella década. VMware inventó la virtualización para la plataforma x86 en la década de 1990 para abordar los problemas de infrautilización y de otra índole, a lo largo de un proceso que obligó a superar gran cantidad de desafíos. En la actualidad, VMware es líder mundial en virtualización para x86, con más de 400,000 clientes, incluido el 100 % de las empresas de la lista Fortune 100". (Vmware UPN, 2012)

Este es el enfoque histórico que presenta la empresa VMWare que es líder en la implementación de ambientes virtuales. En los años 60 IBM comenzó a implementar diferentes particiones lógicas en un solo equipo, esto con el fin de optimizar los recursos. La primera computadora diseñada específicamente para virtualización fue el mainframe IBM S/360 Modelo 67. Este Sistema Operativo que inicialmente IBM llamo S.O. de Supervisor o VMM (Virtual Machine Monitor) fue evolucionando hasta convertirse en lo que hoy en día conocemos como el Hipervisor.

En los años 70 y 80 la idea de virtualización no era considerada atractiva. Fue hasta 1998 que se funda la empresa VMWare y en 1999 presenta el primer Hipervisor, como solución a los problemas que acarreaba que un solo recurso físico funcionara como múltiples recursos lógicos. Virtualizar es abstraer o en otros términos multiplexar un recurso.

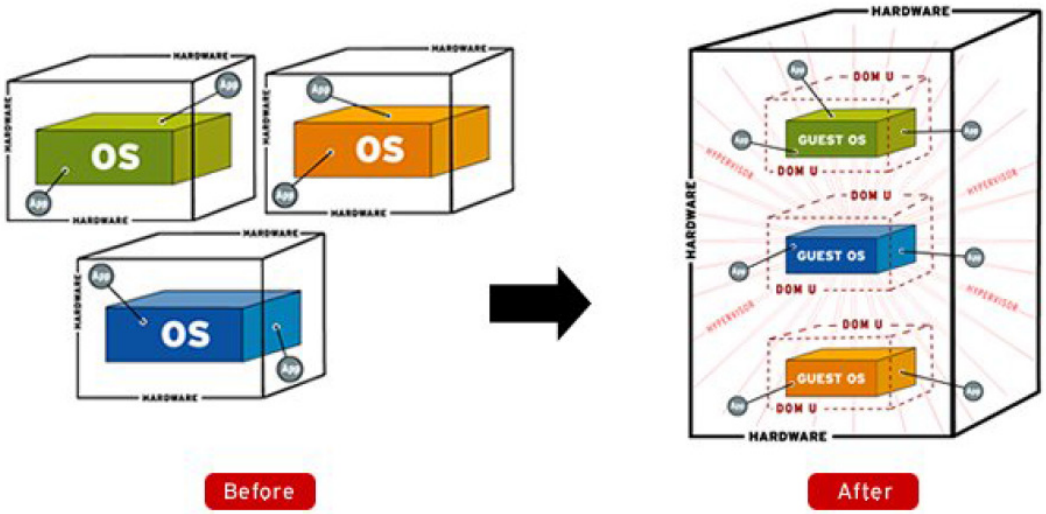

Figura 5. Ilustración del concepto básico del proceso de virtualización. Fuente. http://www.infraestructura.com.co/itasas/index.php/serviciosit/virtualizacion

La virtualización se ha enfocado en gran medida en la virtualización de servidores, que es lo mismo que decir que un servidor físico es particionado en varios servidores virtuales como si fueran recursos físicos independientes. La virtualización se hace posible gracias a la figura del Hipervisor, que es en si el administrador de la virtualización. Este administrador se encuentra entre el software y el hardware, asignando al sistema operativo recursos como procesadores, memoria y unidades de almacenamiento.

2.2. TIPOS DE VIRTUALIZACION

Existen diferentes tipos de virtualización, entre los cuales tenemos:

- **Virtualización de Hardware**

Esta virtualización se conoce como la más completa de lograr. Se hace posible gracias a tecnologías de virtualización como por ejemplo las diseñadas por Intel (Intel-VT) o por AMD (AMD-V) conocidas como *Hardware-Assisted Virtualization.*

Fig. 6. Virtualización por hardware. Fuente http://image.slidesharecdn.com/virtualizacion-130827082218-phpapp01/95/por-qu-la-virtualizacin-11-638.jpg?cb=1377591854

Las máquinas virtuales emulan componentes de hardware, la maquina física donde se realiza la virtualización es conocida como anfitrión, las máquinas virtuales se llaman huéspedes. Por último encontramos una capa en donde ocurre la implantación y puesta en marcha de la máquina anfitrión y está constituida por el Hipervisor.

Este enfoque presenta una gran ventaja y es que pueden emular distintas plataformas de hardware como por ejemplo una arquitectura X86 sobre una Sparc de Sun Microsystems.

La virtualización por hardware puede ser completa o Full Virtualización, en donde cada máquina virtual puede emular sus propios dispositivos como si fueran nativos, esto conlleva en una reducción del rendimiento de las VM. En este tipo de sistema el huésped no sufre ningún tipo de modificación a nivel de su núcleo.

El otro tipo de Virtualización por hardware es el conocido como para virtualización. El sistema operativo se ejecuta como si no estuviera en un entorno virtual. En este caso si existe una modificación del núcleo, los controladores del hardware están integrados en el Hipervisor y su rendimiento se asemeja mucho al de una maquina no virtual.

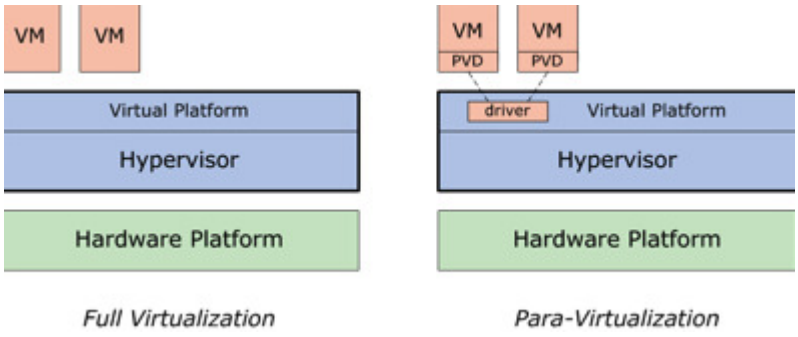

Fig. 7. Diferencias entre Full Virtualización y Para-virtualización. Fuente.http://www.datamation.com/osrc/article.php/3879871/Virtual-Linux-Platform-and-OS-Linux-Virtualization.htm

- **Virtualización a nivel del sistema Operativo**

En este caso los entornos virtuales corren a nivel de un sistema operativo Base. El Hipervisor es reemplazado por este sistema operativo base. Las máquinas virtuales trabajan con sistemas operativos invitados, los procesos se ejecutan independientes y aislados entre ellos. Para que el sistema funcione se hace necesario que el equipo físico disponga de tecnología de virtualización asistida por hardware como por ejemplo Intel-VT o AMD-V.

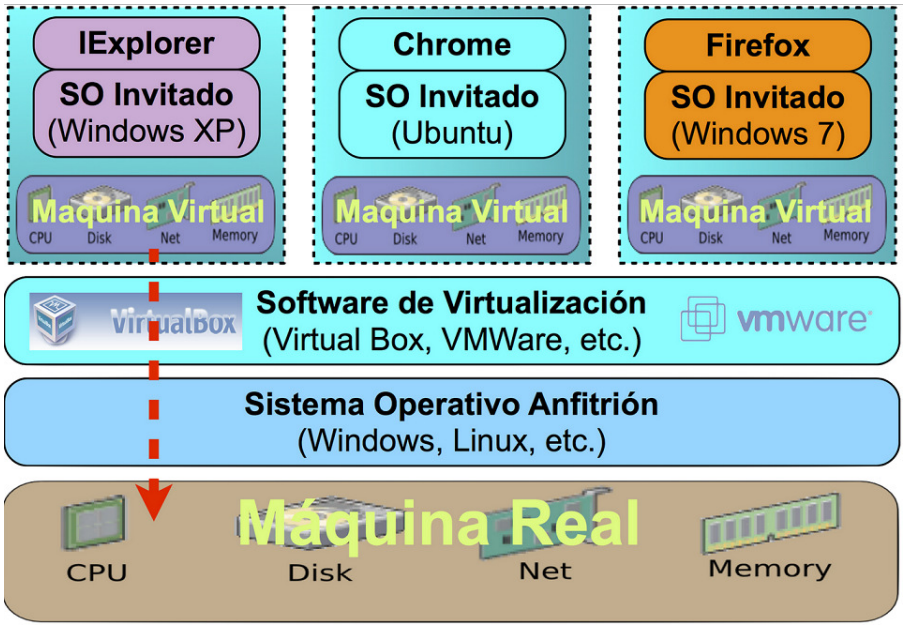

Fig. 8. Virtualización a nivel de sistema operativo. Fuente. http://www.masqueteclas.com/tutorial/virtualizacion-de-sistemas-operativos/

- **Virtualización de aplicaciones.**

La aplicación es ejecutada en el sistema operativo de una forma independiente del mismo. Esta solución es ideal para cuando tenemos varias aplicaciones que son incompatibles entre sí. La virtualización de aplicaciones transforma las aplicaciones en servicios virtualizados, con una administración centralizada y que realmente nunca están instalados, es por eso que no se presentan conflictos con otras aplicaciones.

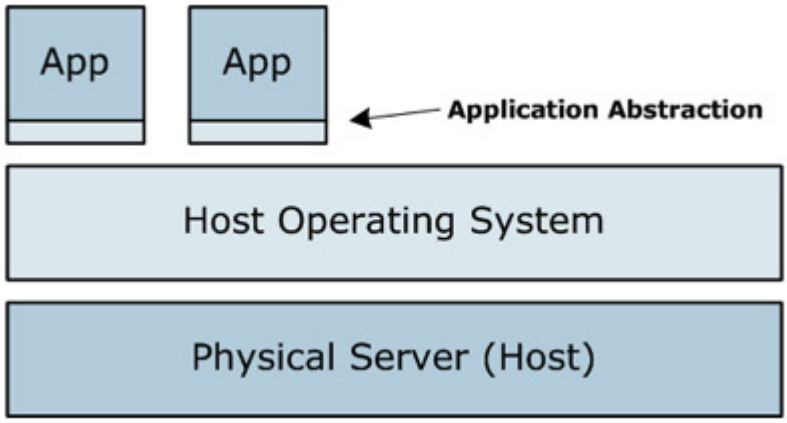

Fig. 9. Virtualización de aplicaciones. Fuente.
http://www.datamation.com/netsys/article.php/3884091/Virtualization.htm

2.3. EL HIPERVISOR

La mayoría de los sistemas de virtualización se apoyan en la figura del Hipervisor. Gracias a él es que múltiples sistemas operativos se puedan ejecutar en una maquina real anfitriona. Los sistemas operativos huéspedes comparten un mismo hardware y creen tener un procesador, memoria y otros recursos de hardware.

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

Los hipervisores también son los encargados de monitorizar las tareas y los recursos que emplean los sistemas operativos invitados. Al utilizar hipervisores es posible conseguir

que múltiples sistemas operativos compitan por el acceso simultáneo a los recursos hardware de una máquina virtual de manera completa y sin conflictos.

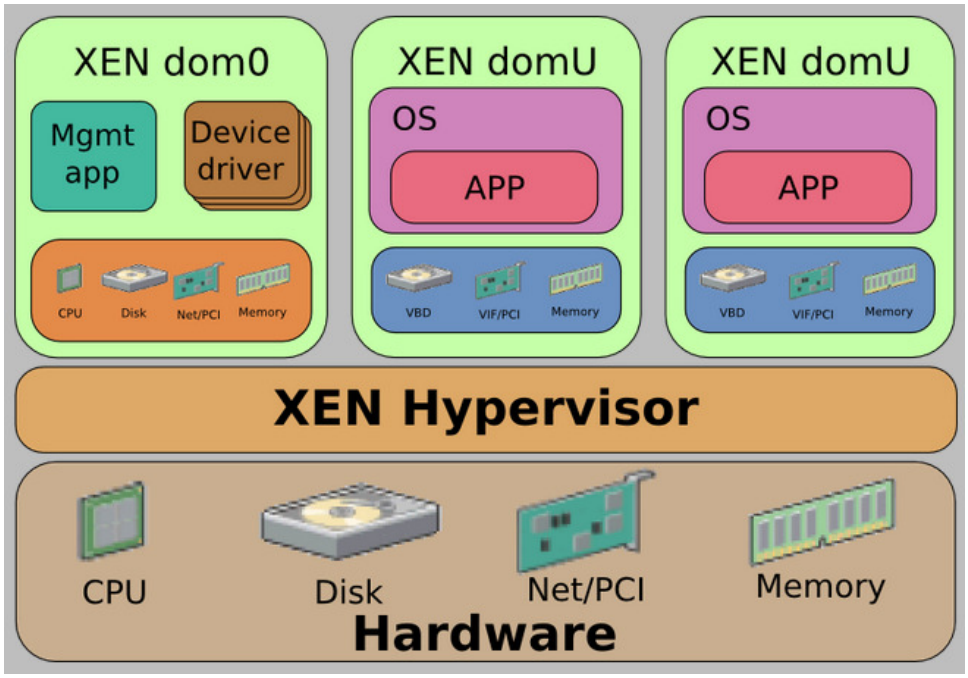

Figura 10. Papel del Hipervisor XEN en un ambiente Virtual.
Fuente. http://linuxprience.blogspot.com/2012/08/1-virtualizacion-con-xen.html
Los hipervisores se clasifican en 2 tipos:

- Hipervisor tipo 1: Bare-metal

También llamado nativo, unhosted o bare metal (sobre el metal desnudo), es un programa que se ejecuta directamente sobre el hardware, para desarrollar una funcionalidad especifica.

Entre los hipervisores del tipo 1 tenemos los siguientes: VMware ESX, Xen (Libre) y Microsoft Hyper-V.

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

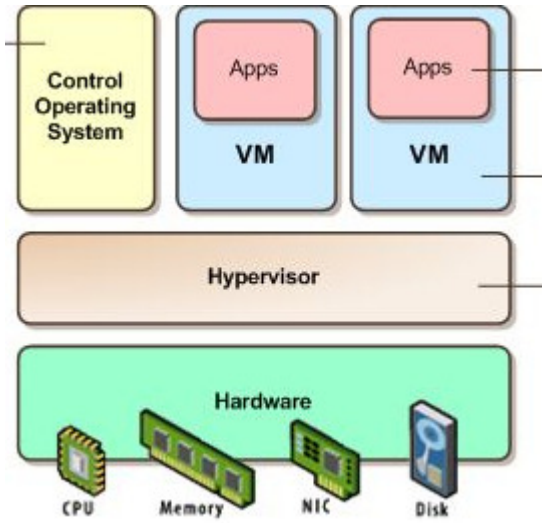

Figura 11.- Hipervisor Tipo 1: Bare metal.
Fuente. http://www.art4software.com/2012/05/virtualizacion-i-introduccion-hypervisor/

- Hipervisor tipo 2: Hosted

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

Figura 12.- Hipervisor Tipo 2: Hosted. Fuente. https://es.wikipedia.org/wiki/Hipervisor

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

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

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

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

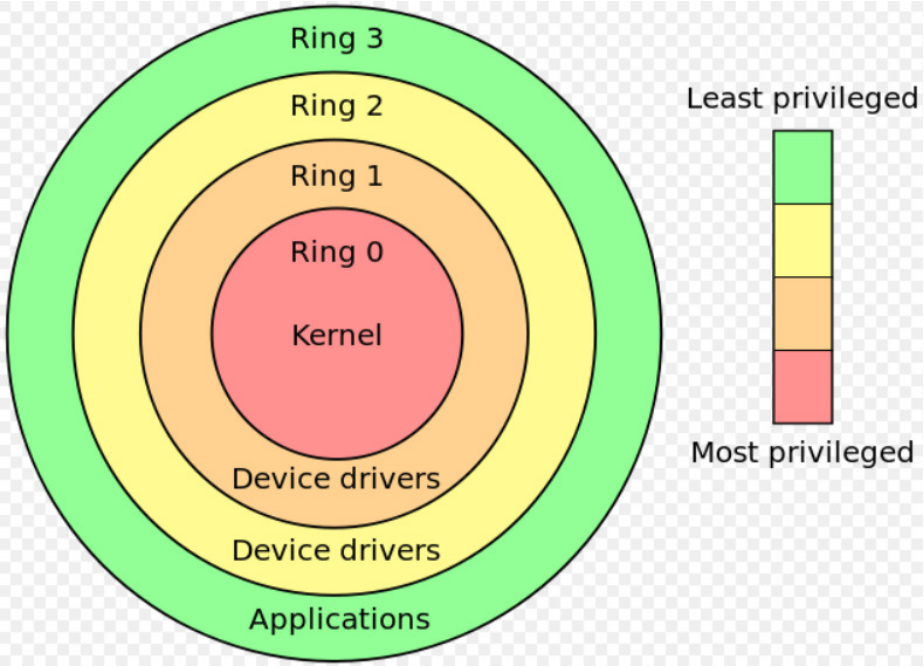

Figura 13. Anillos de privilegio para la arquitectura x86.
Fuente. https://es.wikipedia.org/wiki/Anillo_(seguridad_inform%C3%A1tica)

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

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

La virtualización también puede ser utilizada para combinar diversos recursos en un solo recurso. Un ejemplo de esto puede ser cuando diferentes unidades de almacenamiento son virtualizadas y se convierten en una sola unidad de almacenamiento. A este tipo de virtualización se le conoce como virtualización de recursos.

Estas son algunas ventajas expuestas por la empresa VMWARE con respecto a la virtualización:

- Consolidación de servidores físicos: Unificar varios servidores virtuales en un solo servidor físico.
- Flexibilidad: Instalar, mover, y eliminar recursos de forma rápida, sencilla y centralizada.
- Escalabilidad: El crecimiento fácil y rápido aumentando el número de máquinas virtuales.
- Disponibilidad y balanceo de carga: Varios servidores repartiendo la carga de trabajo y asegurando el servicio.
- Fiabilidad: El fallo de una máquina virtual no afecta al resto de máquinas en el servidor físico.
- Seguridad: Se consigue mediante el aislamiento entre máquinas virtuales.
- Reducción de costes: Menos servidores físicos, menos espacio ocupado en el CPD, menos gastos de electricidad, refrigeración, etc.
- Facilidad y rapidez en la recuperación ante desastres: Rápida creación y clonación de máquinas virtuales.
- Rápida respuesta frente a cambios: Podemos variar la arquitectura o la asignación de recursos muy rápidamente.
- Administración centralizada: Podemos administrar distintos dispositivos de forma centralizada y simplificada.

2.4. COMPARATIVA DESDE EL PUNTO DE VISTA DE LA SEGURIDAD ENTRE UN ENTORNO INFORMATICO REAL Y UNO VIRTUAL

La mayoría de nosotros está acostumbrado a trabajar con ambientes reales, rack de comunicaciones, rack de servidores, componentes y equipos concretos. Los servidores dedicados en las empresas tenían una configuración de hardware y de software específica que estaba allí a la vista de todos.

Cuando nos referimos a una infraestructura de virtualización Cloud, en donde el centro de datos existe en un 100% en la nube, la seguridad física se transforma en algo irrelevante.

A continuación se relacionan los riesgos a los que están expuestos los activos informáticos físicos, cada uno de ellos es un punto a favor de los entornos virtuales, porque cuando no son mixtos ninguna de estas amenazas existen:

- Amenazas naturales:

Los activos informáticos deben ser protegidos de riesgos ambientales como el polvo la humedad y las altas temperaturas. Aquí hay una diferencia importante con las Máquinas virtuales. Lo físico requiere mantenimiento, para prolongar de forma óptima su funcionamiento. De hecho hay que mantener unas condiciones de entorno ideales para el funcionamiento adecuado de los equipos principalmente en lo concerniente a la humedad y la temperatura.

- Accesos no autorizados

En los entornos físicos debe existir una seguridad contra accesos no autorizados, esto conlleva a proteger los activos informáticos de ladrones, actos de sabotaje y en términos generales de personas no autorizadas que pueden ocasionar incidentes. Por obvias razones los entornos virtuales están dimensionalmente aislados de estas amenazas. Esto representa una economía en inversión en seguridad y en pólizas de seguros.

- Variaciones del entorno

Las variaciones de voltajes pueden provocar daños en los sistemas. Estas condiciones deben de mantenerse estables para evitar daños de hardware y en algunos casos de software pues el corte del fluido eléctrico puede dañar programas y archivos.

Ahora bien, analizando la seguridad desde el punto de vista lógico, los ambientes físicos y virtuales comparten muchas amenazas. A continuación relacionamos algunas de ellas:

- Violación al control de acceso y elevación de privilegios

Solo los usuarios autorizados deben de entrar a los sistemas de información y estos usuarios deben de tener los permisos básicos para el trabajo que van a realizar dentro del sistema. Uno de los retos que más llama la atención de los cyber delincuentes es conseguir romper la seguridad en la autenticación e identificación de usuarios. Ambos sistemas son susceptibles a accesos no autorizados el asunto radica en cual es más fácil de atacar un sistema real o uno virtual. Ese es un interrogante que se debe esclarecer con el desarrollo de este trabajo.

- Riesgo de pérdidas de datos.

Los dos sistemas deben de tener mecanismos para evitar que los datos sean borrados intencional o accidentalmente, en los sistemas físicos existen los back up que deben ser realizados periódicamente. De igual manera en los sistemas virtuales existe la figura de *Agent Less* para contrarrestar este tipo de amenaza.

- Riesgo de virus o malware.

De igual manera ambos sistemas son susceptibles de ser infectados con código malicioso, pero el tratamiento que es diferente para ambos casos. Posteriormente se explicara mejor el tratamiento de esta amenaza en ambientes virtuales.

En términos generales los sistemas virtuales pueden ser presa de las mismas amenazas a la lógica que administra, que los entornos físicos. Pero la seguridad en los dos es diferente. Más adelante se determinaran las salvaguardas que deben funcionar de una forma específica, para los entornos virtuales. Por ejemplo en las maquinas físicas los parches y las actualizaciones de programas se pueden aplicar sin ningún problema, en un ambiente virtual las actualizaciones deben ser administradas para no provocar la saturación de los recursos. Si todas las VM se actualizan al mismo tiempo desbordaría la capacidad del sistema.

Otro caso que ilustra más aun la diferencia entre los dos entornos, es cuando ocurre el caso de amenaza por virus o malware. Si ocurre una infección en las VM de un sistema y el antivirus trata de desinfectar a todas al mismo tiempo, colapsaría la capacidad de procesamiento de la maquina anfitriona. La virtualización implica procedimientos de seguridad exclusivos para estos sistemas.

En la figura 4 se muestra la diferencia entre restaurar una maquina física, de una virtual pero así como es más fácil restaurar una máquina virtual, también es más fácil borrarla y hacerla desaparecer. Precisamente para contrarrestar esta amenaza existe la figura del clon virtual, un clon enlazado a la VM nos permitirá remplazar la maquina perdida de manera casi inmediata.

En los ambientes virtuales el back up puede consistir en tener prácticamente una o varias máquinas iguales que nos sirvan de respaldo esta es una ventaja indiscutible en comparación a los ambientes físicos.

Figura 14. La restauración en máquinas reales y virtuales

http://vmwarevenezuela.com/2012/05/27/historia-de-la-virtualizacion/#sthash.MjVbnCLX.dpuf

2.5. LA EVOLUCION DE LOS ENTORNOS VIRTUALES

Raghu Raghuram vice-presidente de VMWARE visualiza de esta manera el proceso de virtualización en el escenario económico mundial:

"La virtualización es definitivamente el primer paso para cloud computing. Las compañías de todo el mundo tienen que pasar por un viaje en el que el primer paso es comenzar a virtualizar la infraestructura que ellos tienen, luego desplegar las aplicaciones de negocios críticas, y luego proporcionar automatización y autoservicios para convertir el centro de datos en una nube privada" (Adrian, G. 2.012)

Es una realidad que el mercado de los servidores virtuales crece a pasos agigantados y supera en creces el de los servidores físicos. Ver figura 5.

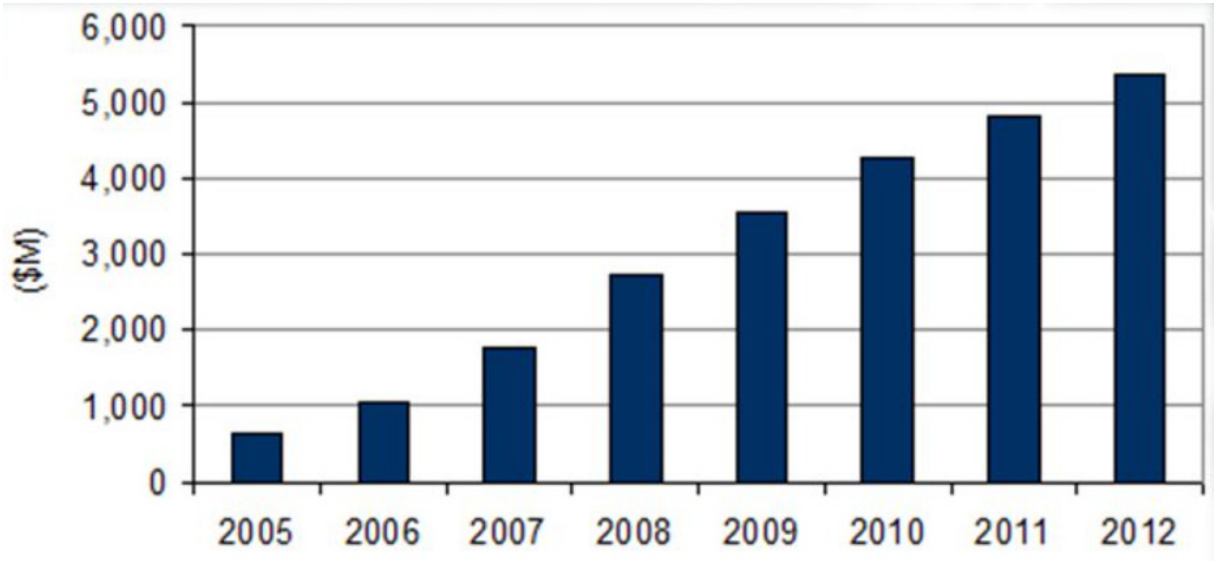

Figura 15. Comercialización de alquiler de servidores virtuales en Millones de Dólares. Fuente. Empresa de consultoría IDC Withe Paper.

El mundo del mercado de los computadores personales viene en decrecimiento, esto debido al auge que han tenido dispositivos como las Tablet y los Smartphone. La virtualización, gracias a las ventajas antes descritas se está convirtiendo en una alternativa más económica, flexible y productiva para diferentes procesos que llevan a cabo las empresas. De ahí la razón de su crecimiento.

2.6. LAS AMENAZAS A LAS QUE ENFRENTAN LOS ENTORNOS VIRTUALES

Son exclusivos de los ambientes virtuales las siguientes amenazas:

- El consumo excesivo de recursos debido a la replicación de las bases de datos de firmas y motores antimalware activos en cada máquina virtual protegida (VM).

- El efecto avalancha que consiste actualizaciones de bases de datos simultáneos o cuando el antimalware realiza simultáneamente procesos de exploración en varias máquinas virtuales, provocando una inundación en el de consumo de recursos. El efecto avalancha puede causar la pérdida drástica del rendimiento en la infraestructura, incluso la denegación del servicio. El asunto es que los intentos de mitigar el problema, mediante la programación de estos procesos se generan "ventanas de vulnerabilidad", esto debido a la activación controlada de actualizaciones y programas antivirus. En

términos generales en sistemas virtuales con muchas máquinas, existirán componentes más vulnerables que otros

- Lagunas de seguridad. En las máquinas virtuales inactivas no se pueden actualizar las bases de datos de los programas antimalware, por lo tanto desde el arranque de la máquina hasta que el proceso de actualización, la máquina virtual es vulnerable a los ataques de virus.

- Una brecha en la seguridad que es evidente, es el tráfico existente entre dos máquinas virtuales que se encuentra instaladas en mismo servidor virtual. Normalmente los administradores de los sistemas informáticos confían en los dispositivos tradicionales de seguridad de red, pero si el tráfico interno entre las máquinas virtuales nunca es visible en la red física.

- Incompatibilidades. Dado que los sistemas operativos estándar no están diseñados para manejar muchas funciones de la virtualización, su uso puede causar inestabilidades e incluso bloqueos del sistema. Este problema se nota mayormente cuando se migran máquinas virtuales o cuando existe un almacenamiento de datos no persistente.

- La rapidez como se implementan las VM pueden producir brechas de seguridad, pues una maquina puede estar lista para su uso en cuestión de minutos, sin estar prepara aun en cuanto a seguridad informática se refiere. En un ambiente virtual deben de existir los mecanismos para permitir la entrada en uso de solamente las VM en las que se hayan aplicado las configuraciones de seguridad pertinentes.

- Los hipervisores son de por si una nueva superficie de ataque que no existe en los sistemas físicos. La seguridad en los hipervisores tiene una problemática y es que al ser sistemas cerrados los firewall y los sistemas de detección de intrusos IDS/IPS no pueden ver el tráfico que circula en él. Esto se constituye en una brecha enorme en la seguridad del entorno virtual.

- En un mismo anfitrión físico pueden existir muchas VM que son externas de nuestro sistema. En un momento dado esas máquinas vecinas pueden traspasar las fronteras impuestas por las directivas de seguridad e invadir y atacar nuestra infraestructura virtual.

Por otro lado si las maquinas foráneas provocan problemas en el anfitrión, el rendimiento de nuestra infraestructura virtual se va ver directamente afectado.

- Las VM orientadas al exterior son puntos vulnerables de entrada para los atacantes. Más riesgoso aún, si nuestro sistema virtual combina maquinas orientadas hacia el interior, con máquinas orientadas hacia el exterior. Ver figura 6.

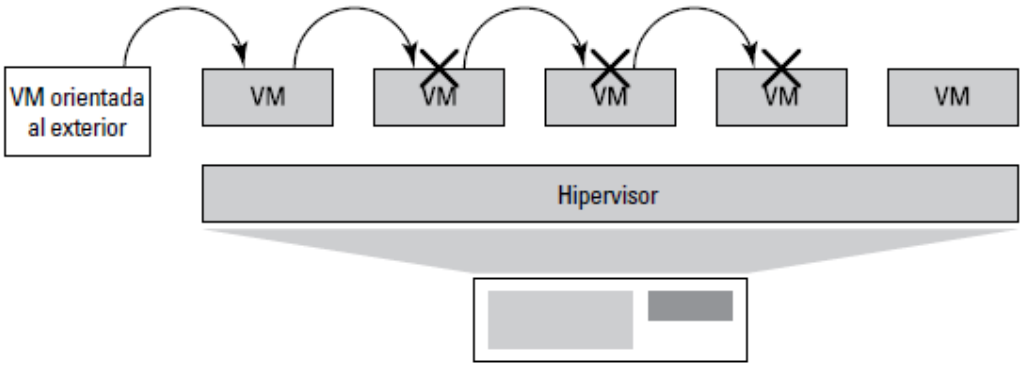

Figura 16. Un atacante puede fácilmente acceder a todo el sistema con la ayuda una VM y del mismo Hipervisor.
Fuente. http://www.trendmicro.es/media/br/cloud-virtualisation-security-for-dummies-ebook-es.pdf

- Las comunicaciones entre VM se realizan a través del Hipervisor. Los Firewalls y los IDS/IPS no pueden tener acceso a este tráfico por lo tanto estos sistemas no pueden ser usados para detectar y prevenir ataques cuando se trata de una red mixta (física y virtual), esta brecha de seguridad compromete la seguridad de muchas VPN por ejemplo.

- Un problema en la seguridad virtual es la persistencia de los datos en la nube. Los proveedores de servicios Cloud manipulan las máquinas virtuales de sus clientes dependiendo de diversos factores. Un VM puede migrar de un sitio a otro sin que no enteremos y los datos almacenados en esa VM pueden persistir en la maquina física anfitriona donde se encontraba. Esto representa una brecha seria en la confidencialidad, como consecuencia del movimiento de los datos almacenados en una infraestructura virtual.

- La mala configuración en un servidor, del anillo (0) que es el sector donde se configuran las instrucciones más privilegiadas, puede afectar el funcionamiento de todas las maquina virtuales. El anillo (0) debe ser desplazado para que este fenómeno de cascada no suceda. El problema es que entre más se distancie el anillo (0) del anillo (0) nativo, menos rendimiento se obtiene por las múltiples capas que deben de ser atravesadas.

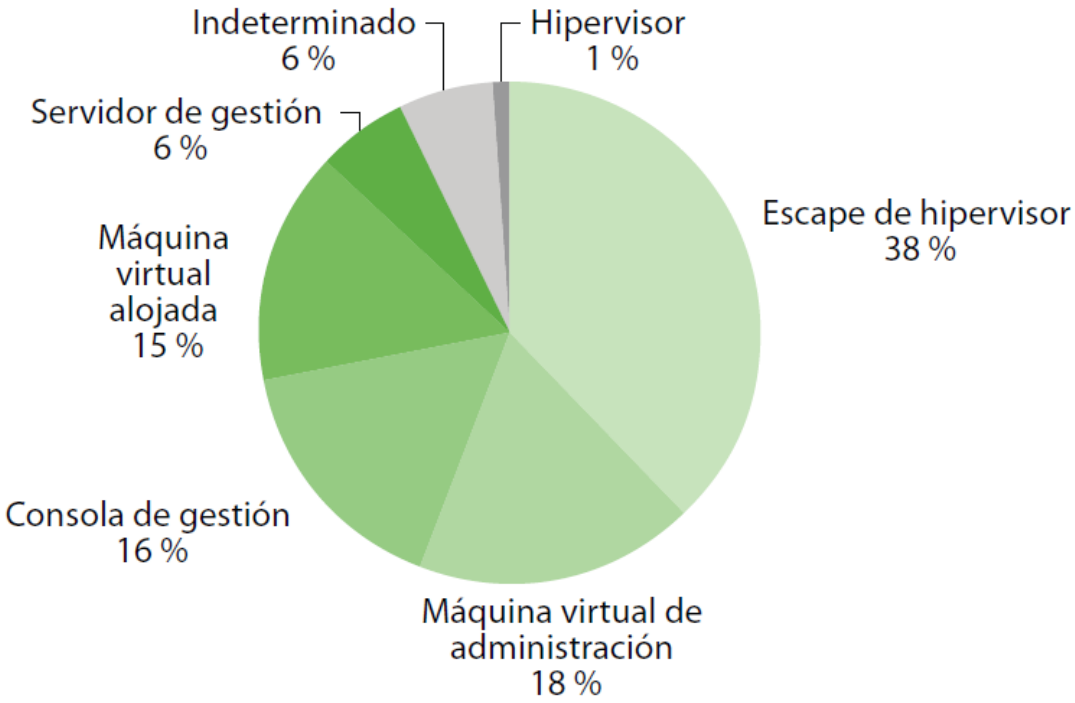

Figura 17. Distribución de las vulnerabilidades en un entorno virtualizado.
Fuente.http://public.dhe.ibm.com/common/ssi/ecm/wg/en/wgl03007usen/WGL03007USEN.PDF

3. OBJETIVOS Y METODOLOGÍA DE TRABAJO

En este capítulo se definen los objetivos que se pretenden alcanzar con el desarrollo de este trabajo, de igual manera se describe la metodología que será llevada a cabo para tal fin. En el capítulo se plantea inicialmente el objetivo general que debe cumplir con las motivaciones planteadas en la introducción de la memoria. Los objetivos específicos definen los mecanismos para gestionar, monitorizar y proteger la infraestructura virtual, buscando implementar las técnicas más efectivas que se pueden utilizar para tal fin.

3.1 OBJETIVO GENERAL

Desarrollar una metodología para ser aplicada en ambientes virtuales y que nos permita gestionar riesgos, administrar de manera segura los recursos y monitorizar las actividades que son llevadas a cabo por los usuarios.

3.2 OBJETIVOS ESPECIFICOS DE LA METODOLOGIA A DEARROLLAR

- Buscar los mecanismos para manejar el excesivo consumo de recursos cuando las actividades se replican en cada máquina virtual. La replicación de actividades (actualizaciones y procesos de exploración de malware simultáneos) pueden producir el efecto avalancha y este se puede traducir en una denegación de servicio por parte de las VM.
- Proponer un sistema de autenticación seguro para los accesos externos que pueda tener el entorno virtual.

- Implementar LOGS seguros a nivel de Hipervisor para separarlos del sistema operativo y así evitar que puedan ser manipulados por atacantes.

- Desarrollar mecanismos de análisis de tráfico entre VMs hacia el interior del entorno virtual.

4. DESARROLLO DE LA METODOLOGIA

De acuerdo con Wikipedia "La metodología (del griego μέθοδος de μετά *metá* 'más allá, después, con', οδως *odós* 'camino' y λογος *logos* 'razón, estudio'),[1] hace referencia al camino o al conjunto de procedimientos racionales utilizados para alcanzar el objetivo o la gama de objetivos que rige una investigación científica, una exposición doctrinal[2] o tareas que requieran habilidades, conocimientos o cuidados específicos. Con frecuencia puede definirse la *metodología* como el estudio o elección de un método pertinente o adecuadamente aplicable a determinado objeto".

Para nuestro caso la metodología estaría enfocada a las acciones destinadas a describir y analizar a fondo los problemas planteados en cuanto a la seguridad de los entornos virtuales y definir unos procedimientos específicos para mitigarlos. Bajo este concepto estará definido el desarrollo de este trabajo.

4.1. METODOLOGIAS PARA LA GESTION DE SEGURIDAD PARA AMBIENTES VIRTUALES

En búsquedas realizadas a través de la Web no existe una metodología de gestión de riesgos que este específicamente destinada a sistemas virtuales. Para sistemas informáticos en general encontramos algunas como Magerit. Octave y Mehari.

4.1.1. MAGERIT

Esta metodología está basada en el análisis del impacto que puede tener la violación de la seguridad en un sistema de información desde el punto de vista de los activos. El proceso busca identificar las amenazas que pueden llegar a afectar al sistema y las vulnerabilidades que pueden ser empleadas por las amenazas identificadas, logrando de esta forma obtener una identificación concreta de las medidas preventivas y correctivas más apropiadas. En la metodología MAGERIT el análisis de riesgos comprende los siguientes aspectos:

1. Los activos, que son los elementos que conforman el sistema de información y que le dan soporte la misión de la Organización

2. Las amenazas, que son hechos que pueden producir un daño a los activos y por ende causan un perjuicio a la empresa.

3. Las salvaguardas, que son las medidas de protección destinadas a mitigar las amenazas que pueden causar un daño a los activos identificados.

Con estos tres aspectos se puede determinar el impacto de lo que podría suceder y el riesgo que probablemente pase.

¿Se puede aplicar esta metodología a los entornos virtuales? Si hablamos de un ambiente hibrido, en donde existen maquinas reales (basadas en hardware) y virtuales, MAGERIT podría funcionar en parte. Pero cuando los activos son intangibles y no son percibidos físicamente el asunto puede complicarse. Para comenzar yo no puedo hacer un inventario de lo que no existe materialmente, no puedo llamar "activo" a lo que no tiene una presencia física y por lo tanto no se puede valorizar. Las VM no tiene un valor económico que se puede cuantificar y no aplicaría cualquier apreciación que queramos hacer al respecto.

En cuanto los activos de información estos dependen de sus características o atributos para poder determinarles un valor y sobre ellos se determinaría las consecuencias que puede provocar la materialización de una amenaza que afecte la disponibilidad de los datos, la confidencialidad y la integridad de los mismos.

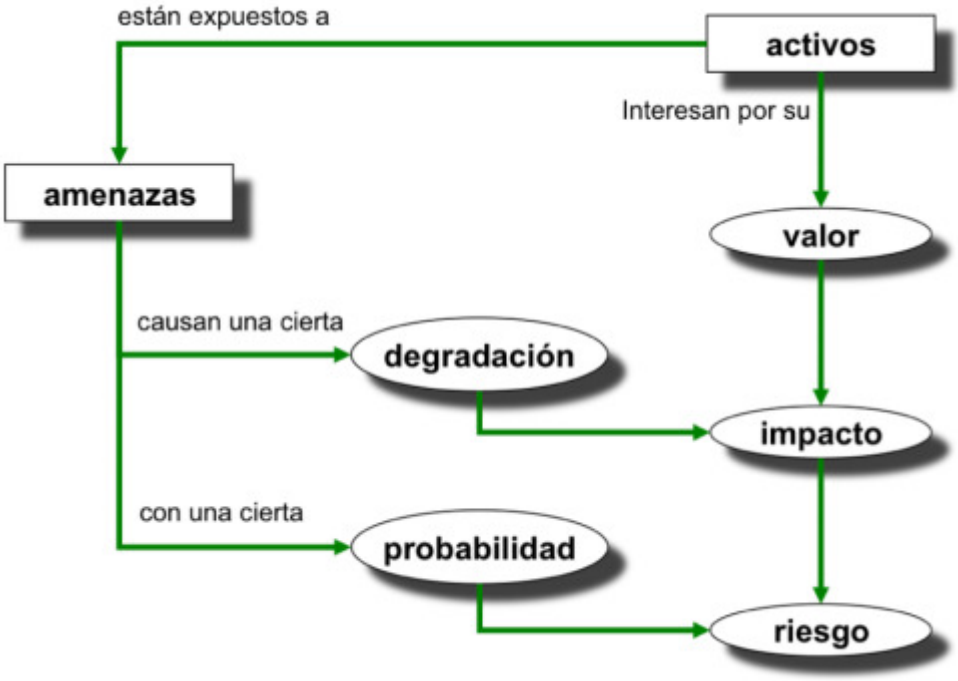

Figura 18. Elementos para el análisis de riesgos potenciales Metodología Magerit.
Fuente. file:///D:/Descargas/2012_Magerit_v3_libro1_m%C3%A9todo_es_NIPO_630-12-171-8.pdf

4.1.2. METODOLOGIA OCTAVE.

Es un framework para el análisis y gestión de riesgos, en sus siglas en inglés Operationally Critical Threat, Asset and Vulnerability Evaluation, esta metodología fue desarrollada por Computer Emergency Response Team (CERT) y tiene como objetivo facilitar la evaluación de riesgos de las tecnologías de la información en una organización.
OCTAVE está compuesta por tres fases:

- Construcción de perfiles de amenazas basadas en activos
- Identificación de vulnerabilidades en la infraestructura.
- Desarrollo de estrategias y planes de seguridad.

En una primera estancia en este modelo, se definen los criterios que permitan conocer la postura de la organización en relación a su propensión a los riesgos. Esta es la base para la evaluación, ya que sin ella no se puede cuantificar el grado en el que la empresa se ve afectada cuando se materializa una amenaza.

En OCTAVE los activos están definidos como los bienes, conocimientos o datos que tienen valor para la organización. Se deben documentar las motivos por la cuales se eligen y además es necesario que exista una descripción detallada de los mismos.

De igual manera, se debe designar un responsable para cada uno de estos activos de información, el custodio asignado deberá definir los requisitos de seguridad que van a ser implementados para salvaguardar la confidencialidad, integridad y disponibilidad, de acuerdo a su criterio y experiencia.

Los activos deben estar acompañados por un perfil que los encargados del desarrollo del modelo consideren como crítico, de esta manera se tiene una base para identificar amenazas y riesgos en pasos subsecuentes. Esta actividad es imprescindible para corroborar que los activos se definen de forma precisa y consistente, así como sus requisitos de seguridad, para determinar las herramientas de protección a aplicar.

El principal problema de los modelos de evaluación de este tipo, es que el análisis de riesgo gira entorno a una identificación y valorización objetiva de los activos puesto que a partir de aquí es que comienza el desarrollo de la metodología.

4.1.3. MEHARI

Este modelo es conocido como un método de análisis de riesgo armonizado. En un comienzo su enfoque era el de apoyar a los responsables de la seguridad de los sistemas de información, en las tareas de gestión de riesgos. Un aspecto importante de MEHARI es que se encuentra en permanente evolución para satisfacer la naturaleza cambiante del entorno de la organización, esto facilita su implementación en ambientes como los virtuales que se caracterizan por ser cambiantes y fácilmente renovables.

Esta metodología nos provee de una serie de herramientas especialmente diseñadas para la gestión de los riesgos, en ella están incluidas una serie de pasos a seguir y que cada una de ellos tiene un objetivo específico:

- Desarrollo de planes de seguridad.
- Implementación de políticas o normas de seguridad, las cuales estarán reunidas bajo el término “marco de referencia de seguridad”
- Relación de la situación detallada del estado de la seguridad
- Evaluación y gestión del riesgo
- Incluir la seguridad en la gestión de proyectos de desarrollo
- Sensibilizar al personal de la organización sobre la seguridad a través de sesiones de formación
- Gestión operativa de la seguridad por medio de la monitorización de las acciones ejecutadas.

Con MEHARI se espera conseguir la madurez en términos de seguridad informática a nivel empresarial y organizacional, de igual manera se espera que contribuya a mejorar la toma de decisiones por parte de las directivas y se acreciente una cultura tecnocrática donde las normas están definidas y se deben de cumplir.

A nivel general MEHARI se adapta a muchos contextos y es coherente con los cambios constantes en las tecnologías de la información, que de por si están en constante evolución.

4.2. APLICACIÓN DE LA NORMA ISO 27001 EN ENTORNOS VIRTULES

La mayoría de las metodologías existentes basan sus riesgos y controles en la norma 27001 asumiendo en ocasiones, únicamente los riesgos descritos en esta norma. En el anexo A de la norma se describen 133 controles, que en una gestión de riesgos son los mínimos que se deberán aplicar, o por lo menos justificar su no aplicación.

La evaluación de riesgos en ambientes virtuales determina que se necesitaría la creación de nuevos controles para cubrir los agujeros de seguridad claramente identificados. Los controles que la norma ISO 27001 propone en el anexo A quedan agrupados de la siguiente forma:

- **A.5 Políticas de seguridad.**

Las políticas de seguridad de este grupo están divididas en dos partes:

- Política de seguridad a nivel estratégico de la organización: Es la mayor línea conductora y proviene de la alta dirección. Determina las principales líneas a seguir y el grado de compromiso de la dirección con ellas.
- Plan de Seguridad táctico: en este plan se define el cómo se va a hacer. En este caso se especifica un nivel más profundo de detalle, para dar comienzo al conjunto de acciones que se deben de cumplir.

En un ambiente CLOUD COMPUTING donde un servidor es como edificio de muchos apartamentos con múltiples huéspedes es difícil tener una política de seguridad unificada. Estas políticas más que todo, deben de ser establecidas por el proveedor del servicio, políticas que deben de estar enfocadas a la protección de máquinas virtuales, administración de usuarios y protección de datos.

- **A.6 Organización de la información de seguridad.**

En este apartado se encuentra enumerados los controles referentes a la confidencialidad de la información los compromisos de la Dirección con respecto al tratamiento de la información y los responsables de dicha seguridad.

En teoría por medio de la virtualización, podemos contar con espacios libres de riesgos, donde resguardar aquella información sensible para la organización. Por supuesto, deben de existir unas políticas claras de autenticación para poder acceder en forma privada a la cuenta virtual de almacenamiento.

De una u otra forma esto facilita aplicar los controles descritos en el apartado A.6, con respecto a la seguridad de la información, con el almacenamiento virtual se tiene la posibilidad de compartir solo la información que sea de interés difundir o presentar a otros. Además existe la posibilidad de dividir los archivos en carpetas públicas o privadas. En aquellos archivos de acceso público tendremos la

posibilidad de colocar determinados archivos que luego, por medio de un link que facilitemos, cualquier persona podrá realizar la descargar en su equipo.

- **A.7 Administración de recursos.**

La gestión de activos de este apartado, se consideraría para los entornos virtuales, como un caso especial pues se tratan de activos intangibles que en teoría no se pueden inventariar ni etiquetar, como si se puede hacer con los recursos físicos.

El control A7 está basado en dos aspectos: en que deben de existir unas responsables de un inventario de los recursos y de los activos informáticos. El segundo aspecto es que es necesario existía una calificación, identificación y tratamiento de la información. Este control es considerado meramente procedimental y aporta muy poco a la seguridad de los sistemas de información

- **A.8 Seguridad de los recursos humanos.**

La seguridad de los recursos humanos es un asunto crítico, como ya veremos más adelante en las arquitecturas ZERO-TRUST, la contratación de personal nuevo en la organización o el ascenso de los empleados implican indudablemente nuevos accesos a los sistemas de información y a los recursos de los entornos virtuales. En este aspecto es definitivo, que se realicen las respectivas acciones preventivas que conlleven a mitigar los riesgos derivados del mal uso de la información y de los recursos virtuales.

Este riesgo crítico implica, que la contratación del personal este acompañada por la debida comprobación de todos sus antecedentes, en algunos países es posible acceder a antecedentes disciplinarios, fiscales y judiciales. Incluir igualmente un riguroso estudio del contenido del currículum, las certificaciones académicas y profesionales.

Un momento crucial en la seguridad de los recursos virtuales es cuando un empleado finaliza su relación con la empresa, es imprescindible supervisar la gestión de su salida hasta la completa retirada de privilegios, permisos y accesos. Es fácil borrar máquinas, discos y recursos virtuales, prácticamente con unos pocos comandos se puede hacer desaparecer un volumen de almacenamiento que contenga todas las VM y servidores virtuales.

Para este caso específico debería existir una persona que sea responsable de supervisar la finalización de labores en los puestos de trabajo. Visto de otra forma si no se trata del despido de un empleado sino de un cambio de puesto de trabajo, existe la necesidad de verificar los

accesos que no sean necesarios, cambiar las cuentas y contraseñas para garantizar que exista una renovación y actualización total, referente al acceso a los recursos con los que ahora se va a trabajar.

- **A.9 Seguridad física y del entorno.**

La tendencia y la evolución de los ambientes virtuales giran en torno a la consolidación del CLOUD COMPUTING la cual está definida como:

"En este tipo de computación todo lo que puede ofrecer un sistema informático se ofrece como servicio, es un paradigma en el que la información se almacena de manera permanente en servidores de Internet y se envía a cachés temporales de cliente, lo que incluye equipos de escritorio, centros de ocio, portátiles, etc." [3]

La seguridad física se convierte en algo irrelevante pues el usuario está accediendo a servicios de virtualización, quizás en un ambiente hibrido este punto de la norma pueda ser relevante.

- **A.10 Administración de las comunicaciones y operaciones.**

Uno de los principales retos que debe superar una empresa que esté planeando la virtualización de sus operaciones es mantener la disponibilidad del servicio sobre todo si estamos haciendo referencia a conexiones remotas. Las comunicaciones entre los usuarios y el entorno virtual deben funcionar de manera ininterrumpida, los administradores deben garantizar que se pueda tener acceso a los servicios y datos cada vez que necesite sin que existan retrasos.

La consolidación de servicios virtuales, exige de la existencia de interfaces cada vez más rápidas. Cada vez es mayor la cantidad de datos, que fluyen entre los extremos de las comunicaciones. Para que todo funcione como es debido, se requiere de una infraestructura de transmisión de datos dimensionada para proporcionar un ancho de banda adecuado. De igual manera deben de existir mecanismos que brinden protección en cuanto a la confidencialidad e integridad de la información que se transmite.

- **A.11 Control de accesos**

La organización debe tener unas políticas claras al respecto, los usuarios del sistema y en nuestro caso del ambiente virtual, deben tener clara su responsabilidad con su cuenta de

usuario para acceder a los servicios o máquinas virtuales. Este acceso debe ser de carácter personal e intransferible, debe quedar clara la prohibición de compartir su acceso con otras personas.

En caso de que un usuario sea retirado de la empresa, cambie de funciones o se reubique en otra área administrativa, los administradores del entorno deben actuar de manera inmediata en cuanto a los ajustes correspondientes a las claves y controles de acceso a los recursos.

- **A.12 Adquisición de sistemas de información, desarrollo y mantenimiento.**

Una de las principales ventajas de la virtualización es la escalabilidad, la capacidad de cómputo de los sistemas de la empresa pude crecer sin problemas, pudiendo tener una infraestructura que pueda trabajar en el "peor de los casos" o en otras palabras conseguir manejar a futuro, mayores cargas de trabajo.

En este aspecto la adquisición de sistemas de información y su desarrollo se convierte con la virtualización en una tarea fácil de conseguir. Se habla por ejemplo en Cloud Computing de una escalabilidad elástica, que consiste en migrar cargas de trabajo de manera temporal a la nube, esto es en otras palabras ampliar los servicios Cloud cuando se requiera, si por ejemplo una empresa tiene más carga computacional en determinadas épocas del año (Navidad, vacaciones, época de elecciones de gobierno) no tendrá que comprar servidores nuevos para la ocasión sino que solo tendrá que ampliar la capacidad el servicio para suplir la necesidad temporal.

- **A.13 Administración de los incidentes de seguridad.**

Este es otro punto a favor de la virtualización, mecanismos como la clonación de máquinas virtuales y los Snapshot permiten tener respaldos de seguridad constantes, que nos permitirán mitigar accidentes en los que puedan estar involucradas pérdidas de información o en el peor de los casos la eliminación accidental o provocada de VMs.

- **A.14 Administración de la continuidad de negocio A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)**

En la actualidad el licenciamiento de Máquinas Virtuales está envuelta en un mar de confusión. Se habla de que el host o el hardware que realiza la virtualización es quien debe poseer la licencia. Esta es una explicación dada por Microsoft al respecto:

"Los sistemas operativos Windows se licencian por dispositivo. Dado que una máquina virtual no lo es, tenemos que licenciar el dispositivo en el que corre dicha máquina virtual, o el dispositivo desde el que se accede a ella".

"Generalmente se adquieren equipos a través de un fabricante determinado con sus licencias OEM de Windows, y se usa la licencia de actualización para plataformarlos con la imagen corporativa deseada. Y dado que las versiones OEM van asociadas al equipo, tampoco pueden utilizarse para instalar la máquina virtual".

Estos conceptos abren muchas brechas en la legalidad del software puesto que si lo se licencia es un equipo y las VM en teoría no los son, entonces ¿cómo puedo legalizar el software en entornos virtuales? Microsoft trata de resolver el dilema vendiendo suscripciones para maquinas virtualizadas para su Hipervisor Hiper-V y es llamado VDI Suite, esto no resuelve el problema en otros hipervisores como XEN, VMwrare o KVM.

Otro tema del cual queda mucho que definir en la actualidad es el tema de las auditorias. Si hablamos de un proveedor de servicios en la nube ¿Cómo poder verificar el cumplimiento por parte del proveedor Cloud de requerimientos en materia de seguridad? ¿Qué estándares se deben seguir en dichas verificaciones? Y lo que resulta más importante ¿Cómo conseguir que el proveedor sea revisado?

La organización de profesionales de seguridad informática ISACA reconoce que no existen estándares específicos para los servicios Cloud, por lo que por ahora no queda más que utilizar los que son empleados para los sistemas de información basados en recursos físicos y aquí cabe recordar que la virtualización implica riesgos que son exclusivos de ella.

Hasta aquí hemos hecho un breve comparativo de los catorce grupos de control y su posible aplicación en los entornos virtuales.

4.3. LA NORMA ISO 27018

La ISO/IEC 27018 de agosto del año 2014, es la primera norma internacional sobre seguridad en la nube y su particularidad es que trata cuestiones específicamente relacionadas con los

servicios de virtualización, esto es algo que hasta el momento no existía. Esta norma principalmente se refiere a la protección del derecho a la privacidad de la información de los usuarios y obliga a los proveedores de servicios CLOUD a informar sobre el tratamiento que le dan a la información almacenada de los clientes. La norma 27018 se enfoca en fortalecer la privacidad, mediante la incorporación de sistemas de protección, que salvaguarde la información sensible que se encuentra almacenada en los servidores que dan soporte a este servicio.

La responsabilidad de la seguridad de servicios Cloud recae sobre el proveedor de los mismos, la Norma ISO 27018 describe los requerimientos necesarios para garantizar que los servicios en la nube puedan ofrecer los controles adecuados para garantizar la seguridad de información.

Empresas como Microsoft ya han adoptado la norma para aplicarla en servicios de almacenamiento virtual en la nube, Algunos de los productos que han adoptado este estándar son Microsoft Office 365, Microsoft Azure, Microsoft Intune y Microsoft Dynamics CRM.

Los aspectos más relevantes del estándar ISO/IEC 27018 son los siguientes:

- Consentimiento: los proveedores de servicios no accederán a los datos personales para temas de publicidad o marketing a menos que el usuario lo requiera.

- Control: los usuarios deben especificar cómo se usará la información que le ha proporcionado a la empresa.

- Transparencia: los proveedores de servicios informarán a sus clientes sobre dónde están sus datos y si utilizan otras empresas a modo de externalización de servicios.

- Comunicación: los proveedores deben mantener un registro claro sobre cualquier incidente para posteriormente comunicárselo al cliente en cuestión.

- Auditoría externa sobre el cumplimiento de la normativa ISO/IEC 27018.

4.4. MODELO ZERO-TRUST DE FORRESTER

Este modelo nace a partir de la premisa de que los incidentes de seguridad en los entornos virtuales son desastrosos y que por lo regular los profesionales de informática de hoy en día, conocen las ventajas de la virtualización, pero lamentablemente desconocen sus riegos.

En febrero del año 2011 en la empresa japonesa Shionogi, el administrador del área informática Jason Cornish, fue despedido por la empresa, en venganza por lo sucedido utilizó una cuenta de usuario para acceder a la red de la empresa. Una vez conectado, utilizó una aplicación del software VMware VSphere para eliminar 88 servidores virtuales. Según el reporte de las autoridades:

"los servidores eliminados almacenaban la mayor parte de la infraestructura informática americana de Shionogi, incluidos el correo electrónico de la empresa y los servidores de BlackBerry, su sistema de seguimiento de pedidos y su software de gestión financiera. El ataque paralizó las operaciones de Shionogi durante días, provocando que los empleados de la empresa no pudieran enviar los productos, recibir pagos ni comunicarse por correo electrónico" (Holland, 2012).

Forrester el creador del modelo ZERO-TRUST se dio cuenta de la ineficacia de las soluciones tradicionales de seguridad para proteger los entornos virtuales. Por ejemplo, utilizan dispositivos de seguridad de red diseñados para proteger entornos físicos y que no son eficaces proteger las cargas de trabajo virtuales.

Con la virtualización existe una visión limitada del tráfico interno, existente entre las máquinas virtuales. Viendo el funcionamiento del entorno desde el punto de vista de una arquitectura de red, la virtualización conlleva a que existan múltiples puntos ciegos dentro del sistema, y muchos encargados de la seguridad informática no planificado implementar las herramientas necesarias para vigilar la comunicación interna entre máquinas virtuales.

El modelo Zero Trust de seguridad de la información de Forrester ya no existe una red interna de confianza y de manera evidente, las redes externas son de muy poca confianza. En este modelo, completamente todo tráfico de red es poco fiable.

El modelo ZERO-TRUST está basado en los siguientes aspectos:

- Los usuarios deben tener un acceso seguro a los recursos del entorno independientemente del lugar en que se encuentren. Los usuarios con mayores privilegios deberán hacer uso de una autentificación robusta para acceder al entorno y administrarlo.

- Adoptar una estrategia de mínimos privilegios e imponer un estricto control de acceso. Se debe eliminar los accesos como administrador en donde sea posible y establecer un sistema de gestión único para administrar el entorno virtual.

- Registrar todo el tráfico para que sea posible llevar a cabo de manera eficaz acciones de respuesta y recuperación. En caso de que exista una amenaza interna accidental o intencionada, se debe disponer de las herramientas adecuadas para detectar rápidamente infracciones de políticas o actividades sospechosas. Las funciones de auditoría y registro son necesarias para poder tener un alto grado de regulación de las actividades dentro del entorno.

4.5. METODODLOGIA ACRD PARA EL CONTROL DE RIESGOS DE SEGURIDAD EN AMBENTES VIRTUALES.

Durante el desarrollo de este trabajo hemos descrito los ambientes virtuales, sus componentes, la forma como interactúan entre si y los riesgos de seguridad que acarrea el uso de la virtualización.

Antes de dar inicio al planteamiento de la metodología, sea hecho un análisis de las metodologías, modelos y estándares existentes, que son usados indistintamente en entornos físicos y virtuales. ZERO-TRUST es un modelo que mitiga algunas brechas en la seguridad pero no todas. En este campo de la seguridad informática existe aún mucho por hacer, sorprende que solo hasta agosto del 2.014 la ISO lanza la norma ISO/IEC 27018 para estandarizar y auditar servicios Cloud Computing, con esto se puede concluir que las tecnologías de virtualización están avanzando más rápido que la mitigación de los riesgos.

ACRD significa Aislar, Controlar, Re autenticar y Detectar. A continuación se describirá cada uno de los aspectos de la metodología.

4.5.1. AISLAR.

Un problema identificado en la virtualización, es la existencia de varias VM en un mismo anfitrión físico. Ya sea que se trate de servicios Cloud o entornos virtuales o híbridos, en un

momento dado un atacante que adquiera el control de una VM puede atacar las máquinas vecinas traspasando las fronteras impuestas por las directivas de seguridad e invadir y vulnerar toda la infraestructura virtual.

Por otro lado las VMs o servidores virtuales orientados hacia conexiones externas, son puntos vulnerables de entrada para los atacantes. El asunto se torna más riesgoso aún, si nuestro sistema virtual combina maquinas orientadas hacia el interior, con máquinas orientadas hacia el exterior. Para mitigar este agujero en la seguridad la metodología ACRD plantea el aislamiento de las VM de tal manera que en su instalación se desarrollen fronteras entre ellas que minimicen el impacto producto de un ataque al entorno virtual.

El aislamiento de máquinas virtuales lo podemos obtener mediante la instalación de las VM en particiones o volúmenes diferentes, esta acción dificultaría que un atacante recopilara información del sistema ya que solo podría tener información de la VM vulnerada y del directorio raíz donde esta se encuentra. Las demás maquinas estarían asiladas por encontrarse en volúmenes de disco diferente. En caso de un ataque por Malware o antivirus tenemos la opción de no solo eliminar la máquina virtual sino también todo el Volumen Lógico que la contiene.

Otra acción que nos puede ayudar a mitigar esta vulnerabilidad es ubicar la maquina Dom0, las maquinas DomU internas y las DomU con acceso externo en segmentos de red diferentes.

4.5.2. CONTROLAR.

Los recursos del computador anfitrión deben ser distribuidos y limitados para cada VM. El rendimiento de una VM no debería afectar el rendimiento de otra máquina virtual. Una de las vulnerabilidades encontradas, es el consumo excesivo de recursos debido a la replicación de las bases de datos de firmas de antivirus y motores antimalware activos en cada máquina virtual protegida (VM).

El control de recursos también nos permitirá mitigar el efecto avalancha que ocurre cuando se activan simultáneamente actualizaciones en las VMs o cuando el antimalware realiza simultáneamente procesos de exploración en varias máquinas virtuales, provocando una inundación en el de consumo de recursos.

Cada VM debe tener asignados recursos fijos para su funcionamiento y de esta manera evitar que el efecto avalancha ocasione la perdida drástica del rendimiento en la infraestructura virtual, esta vulnerabilidad puede acarrear incluso fallas como la denegación del servicio.

4.5.3. REAUTENTICAR (Doble factor de autenticación).

La autenticación es prácticamente la primera línea de defensa en un entorno virtual, solo los usuarios autorizados deben tener acceso. En muchos casos como por ejemplo en Cloud Computing el acceso es remoto, en este caso podemos estar hablando de que un acceso podría darse a través de una red Wi-Fi insegura y esto podría poner en riesgo la seguridad de todas las VMs.

La metodología presentada recomienda dos factores de autenticación para que el proceso sea aún más seguro. Se debe combinar por ejemplo la clave y una tarjeta magnética, o la clave y un Pin lo importante es que exista un doble factor de autenticación.

4.5.4. DETECTAR

Una vulnerabilidad importante es que las comunicaciones entre VM se realizan a través del Hipervisor. Elementos de control y detección como los Firewalls y los IDS/IPS no pueden tener acceso a este tráfico, por lo que deben de existir mecanismos de detección de trafico dentro de del entorno virtual. Este control de detección de trafica la existencia de reportes como los siguientes:

- Horarios de accesos al entorno virtual.
- Registro de tráfico entre maquina virtuales.
- Flujo de datos valorizado entre VM.
- Maquinas conectadas y accesos externos.
- Reporte de host activos y tiempo de actividad.
- Análisis de protocolos y rendimiento de comunicación.
- Alertas por detección de tráfico malicioso y accesos no permitidos.

Con esta información podemos tener un control general del tráfico y de los sucesos que ocurren hacia el interior del entorno virtual.

5. IMPLEMENTACION DEL PILOTO EXPERIMENTAL

En el capítulo 5 se explica de forma detallada la implementación del piloto experimental, donde se aplicara la metodología ACRD y así poder sacar conclusiones con respecto a la efectividad de misma.

5.1. DESARROLLO ENTORNO VIRTUAL

A continuación se explicara la composición del piloto experimental sobre el cual aplicaremos la metodología.

- Establecer un entorno virtual con un Hipervisor Dom(0) y tres máquinas virtuales Dom(U).
- Configurar durante la instalación del entorno las características deseadas para poner en práctica el aislamiento entre VMs plateado por la metodología la metodología.
- Implementar una capa de protección extra en el momento de la autenticación de entrada al entorno virtual.
- Instalar un sistema de detección de intrusos hacia el interior del entorno que nos permita supervisar el tráfico entre VMs y los eventos que ocurran en el Hipervisor.

5.2. INSTALACION DEL HIPERVISOR

Para el piloto experimental utilizaremos el monitor de máquina virtual XEN Versión 4.4. Como ya habíamos anotado anteriormente, es un Hipervisor distribuido bajo licencia GPL de GNU. Por ser un software libre distribución, tenemos la facilidad de usar este Hipervisor en el entorno virtual para el desarrollo de nuestro trabajo. Con Xen podemos ejecutar varios sistemas operativos en un mismo sistema anfitrión y conseguir que el aislamiento entre los recursos en cada sistema operativo sea absoluto. El objetivo para la sustentación de la metodología que vamos a aplicar es que cada uno de estos sistemas operativos resida por separado en cada máquina virtual.

El piloto experimental se encontrara instalado en un equipo con las siguientes características

Procesador Intel Core I7 3.6 Ghz Modelo 4790 con 8 Mb de cache, cuatro nucleos y 8 hilos. Este procesador nos ofrece tecnología de virtualización (VT-x), cuenta además con una memoria ram de 8 Gb y un Disco Duro real de 160 Gb.

El computador anfitrión contendrá las imágenes de estas máquinas virtuales, las imágenes corresponden al sistema de ficheros sobre el que reposaran los datos del sistema operativo que será ejecutado, además de los datos de usuario y de sistema.

Vamos a requerir de un sistema operativo básico, sobre lo cual vamos a crear la capa de virtualización con Xen, y después implementar las tres máquinas virtuales del piloto experimental. Inicialmente realizamos la instalación del DOM 0 o Domain 0 en donde tendremos los controladores de hardware así como también se tendra el conjunto de herramientas para el control de las Máquinas Virtuales (MV). Para la instalación del DOM 0 seleccionamos Debian en su versión 8 también llamada Jessie. A nivel de pruebas la versión Jessie es considerada estable, soporta arquitecturas de 64 bits y contiene paquetes más actualizados que la Etch.

Durante la instalación de Debian se ha configurado una partición para las máquinas virtuales en un volumen LVM en un espacio de disco de 150 GB. La partición configurada como LVM para volúmenes lógicos nos permitirá manejar el espacio de las VM de una forma más flexible, de igual forma podemos configurar grupo de volúmenes para el Hipervisor XEN.

En la instalación también se definieron dos volúmenes lógicos: Uno primario llamado *root*, en un espacio de 8 GB y será la raíz del sistema de archivos del servidor. El segundo volumen será utilizado como de intercambio (SWAP), en un espacio 2 GB y constituirá la partición swap del servidor. Este volumen Swap es utilizado por el sistema como memoria virtual, cuando la memoria real se agota, el sistema copia parte del contenido de esta directamente en el espacio de memoria de intercambio a fin de poder realizar otras tareas.

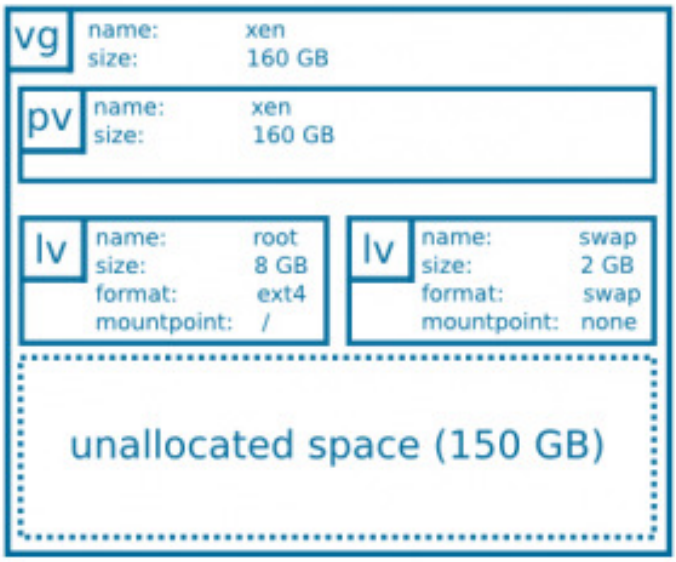

Figura No 19. Distribución del disco duro para el Piloto experimental.
Fuente. http://otzarri.net/manuales/servidor-xen-en-debian-con-lvm

Los pasos a seguir para la instalación del Hipervisor XEN son los siguientes:

1. Actualización del Debian. La versión Xen 4.4 requiere que el sistema operativo este es su última actualización. Para ello digitamos, en el terminal de Linux los siguientes comandos:

```
apt-get update
```

Seguido de la instrucción:

```
apt-get dist-upgrade.
```

2. Instalamos los paquetes *stunnel* y *xcp/xe* con el comando **apt-get install xen 4.4.** Mediante estos paquetes podemos tener la ejecución remota de comandos *xe* en el Hipervisor, que más tarde emplearemos en la implementación de la metodología ACRD.

3. Previo a la instalación del Xen instalamos las siguientes herramientas que nos van a ayudar a monitorizar procesos dentro del sistema:

- Iotop : monitorización de entrada y salida de datos en los discos duros. La interfaz de iotop nos permite ver el uso de I/O de procesos individuales. Esta herramienta nos permitirá saber que procesos se están copiando el disco duro. Inicialmente habilitamos en el Kernel

las opciones CONFIG_TASK_DELAY_ACT, CONFIG_TASK_IO_ACCOUNTING, CONFIG_TASKTAST y CONFIG_VM_EVENT_COUNTERS. Obtenemos la herramienta mediante el comando apt-get install iotop

- Iftop: esta herramienta nos permite visualizar el tráfico de red del Hipervisor como el uso del ancho de banda actual, nos permitirá auditar los procesos que están utilizando el ancho de banda y hacia donde se dirigen ya sea en IPv4 o en IPv6. Esta herramienta es ideal para saber que procesos están ocupando nuestro entorno virtual y así poder identificar posibles ataques DoS. La herramienta también nos permite tomar estadísticas de consumo de ancho de banda una vez creemos las VPN. Esta herramienta la obtenemos mediante el comando: `apt-get install iftop`

- Htop – Esta herramienta nos va a permitir listar las tareas realizadas por cada usuario del entorno virtual permitiéndonos visualizar el consumo de recursos de cada máquina virtual. Obtenemos la herramienta mediante el comando: `apt-get install htop.`

4. Realizamos la instalación de los paquetes de Xen, del Hipervisor Xen y laS herramientas Xen para la implementación de Bridges. Esto lo hacemos mediante el siguiente comando:

```
apt-get install xen-4.0 bridge-utils
```

5. Instalamos el paquete de xen-tools de Debian que es una serie de scripts que nos permiten crear de manera fácil una configuración completa de un invitado de Xen. Mediante el siguiente comando obtenemos el paquete Xen-tools:

```
apt-get install xen-tools
```

Debemos indicar la ruta donde se guardarán las imágenes de las ISO para la instalación de los DomU y habilitar la contraseña de súper usuario en la construcción de las imágenes. Para ello editamos el archivo:

```
/etc/xen-tools/xen-tools.conf
```

Debemos des comentar las líneas:

```
dir = /home/xen/
passwd = 1
```

5.3 GESTION DE GRUPOS Y VOLUMENES

La metodología propuesta ACRD nos sugiere el aislamiento de máquinas mediante la creación de un sistema de volúmenes que nos permita crear las máquinas virtuales en volúmenes de disco diferentes, de igual manera se requiere separar las máquinas virtuales ubicándolas en segmentos de red diferentes dependiendo por ejemplo si los accesos a estas VM son externos o internos.

La implementación para la administración de Volúmenes lógicos es llamada LVM (Logical Volumen Manager) con LVM podemos realizar las siguientes acciones:

1. Cambio de tamaño de grupos de volúmenes.
2. Cambio de tamaño de volúmenes lógicos.
3. Instantáneas de lectura y escritura (a partir de LVM2).
4. RAID0 de volúmenes lógicos.

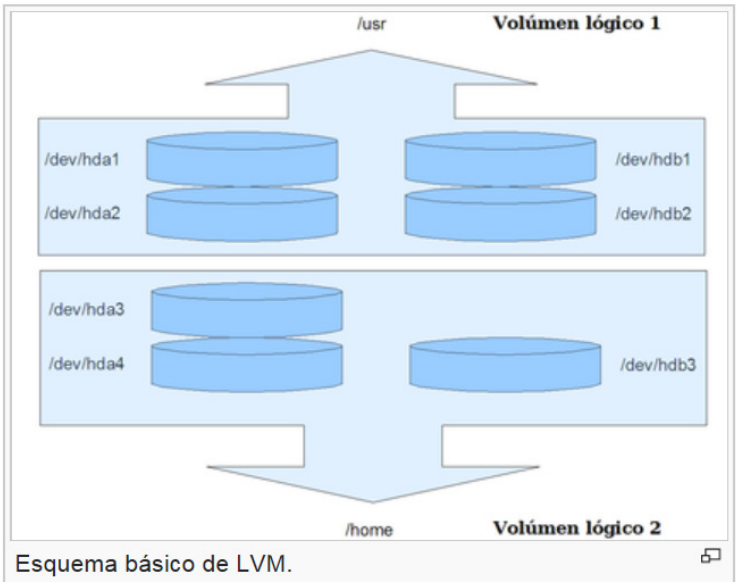

Fig. No 20 Esquema básico del sistema de volúmenes lógicos en Linux.
Fuente. https://es.wikipedia.org/wiki/Logical_Volume_Manager.

LVM funciona a tres niveles: Volúmenes físicos, volúmenes lógicos y grupos de volúmenes. Inicialmente debemos instalar la herramienta LVM2 mediante el siguiente comando:

```
apt-get install lvm2
```

Con esta herramienta manejaremos los volúmenes físicos los cuales serán utilizados con las letras PV, los **volúmenes** Lógicos identificados con la LG y los grupos de Volúmenes identificados con las letras VG.

Con el comando **lvmdiskscan** verificamos con que dispositivos contamos para la creación de los volúmenes. La partición que creamos como LVM, en la instalación de Debian es la que aparece como SDB6 y sobre ella creamos un volumen físico con la siguiente instrucción.

```
pvcreate /dev/sdb6
```

Creamos un grupo de volumenes llamado VolGroup01

```
Vgcreate VolGroup01/dev/sdb6
```

Creamos un volumen logico en VolGroup01:

```
Vgcreate VolGroup01 /dev/sdb6
```

Ahora creamos cuatro volúmenes lógicos para las cuatro máquinas virtuales que vamos a instalar en el piloto experimental.

A cada volumen le asignaremos 20 Gigas de espacio y para cada volumen digitamos los siguientes comandos:

```
Lvcreate  -L 20G VolGroup01 -n vol01
Lvcreate  -L 20G VolGroup01 -n vol02
Lvcreate  -L 20G VolGroup01 -n vol03
Lvcreate  -L 20G VolGroup01 -n vol04
```

Con los comandos pvdisplay, vgdisplay y lvdisplay verificamos que todo está correctamente configurado. El objetivo es tener cuatro volúmenes lógicos independientes para cada máquina virtual y tener una distribución con VMs aisladas como muestra la siguiente figura:

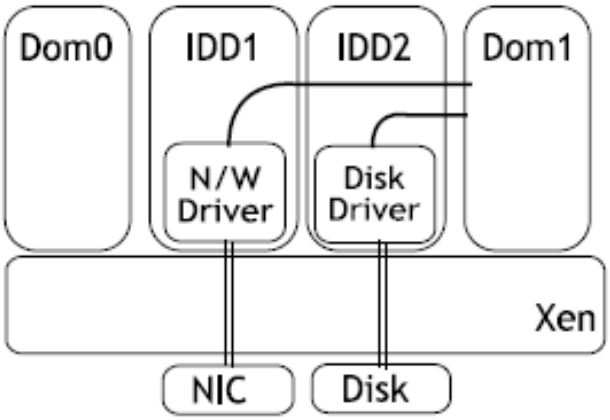

Fig No. 21. Modelo en donde las entradas y salidas de las VM en discos y redes diferentes. http://web.mit.edu/rhel-doc/3/rhel-sag-es-3/ch-lvm-intro.html

Fig.22. Captura de pantalla de los cuatro volúmenes creados.

5. 4. CREACION DE MAQUINAS VIRTUALES

Configuramos un volumen de 40 Gb. para guardar las imágenes de los sistemas operativos de las máquinas virtuales que vamos a crear mediante la siguiente instrucción:

```
Lvcreate  -L 40G VolGroup01 -n vol05
```

Necesitamos tener cuatro imágenes ISO para los diferentes sistemas operativos que vamos a instalar: Windows Server 2008, Windows 7 Pro, Ubuntu y Linux Mint.

Copiamos las cuatro imágenes ISO asignándole a cada uno 10 GB, mediante las siguientes instrucciones:

Para Windows Server 2008:

```
#dd if=/dev/zero of=/var/xen/domains/WindowsServer2008/disk.img bs=1024k
count=10000
```

Para Windows 7 Pro.

```
#dd if=/dev/zero of=/var/xen/domains/Windows7Pro/disk.img bs=1024k
count=10000
```

Para Ubuntu.

```
#dd if=/dev/zero of=/var/xen/domains/Ubuntu/disk.img bs=1024k
count=10000
```

Para Linux Mint:

```
#dd if=/dev/zero of=/var/xen/domains/linux-mint/disk.img bs=1024k
count=10000
```

Creamos los archivos de configuración para las cuatro imágenes.

```
#vim /etc/xen/WindowsServer2008.cfg
#vim /etc/xen/Windows7Pro.cfg
#vim /etc/xen/Ubuntu.cfg
 #vim /etc/xen/linux-mint.cfg
```

Colocamos lo siguiente en cada archivo.

```
kernel = "/usr/lib/xen-4.4/boot/hvmloader"
builder='hvm'
memory = 1024
name = "WindowsServer2008" (Para cada sistema operativo cambia el name)
dhcp= 'dhcp'
vif= [ 'type=ioemu, bridge=eth0' ]
disk = [ 'file:/root/WindowsServer2008.iso,xvdc:cdrom,r',
'file:/srv/xen/domains/WindowsServer2008/disk.img,xvda,w' ] (Esta línea
cambia para cada sistema operativo)
device_model = '/usr/lib/xen-3.2-1/bin/qemu-dm'
# boot on floppy (a), hard disk (c) or CD-ROM (d)
```

```
# default: hard disk, cd-rom, floppy
boot="dc"
sdl=0
vnc=1
vnclisten="0.0.0.0"
vncconsole=1
stdvga=0
serial='pty'
on_poweroff = 'destroy'
on_reboot = 'restart'
on_crash  = 'restart'
```

Luego creamos cada una de las máquinas virtuales:

```
#xl create /etc/xen/VMWindowsServer2008.cfg
#xl create /etc/xen/VMWindows7Pro.cfg
#xl create /etc/xen/VMUbuntu.cfg
#xl create /etc/xen/VMlinux-mint.cfg
```

Se realiza la instalación de cada sistema a partir de la imagen ISO previamente configurada, corremos las cuatro máquinas virtuales con el comando xl créate y con el comando xl list verificamos el funcionamiento de las máquinas virtuales.

Eliminamos las líneas que contienen las imágenes ISO luego de haber hecho la configuración del sistema, para que se reinicie la instalación.

La línea que se debe eliminar de cada uno de los archivos de configuración es la siguiente:

```
file:/root/WindowsServer2008.iso,xvdc:cdrom,r
file:/root/Windows7.iso,xvdc:cdrom,r
file:/root/Ubuntu.iso,xvdc:cdrom,r
file:/root/linux-mint-debian.iso,xvdc:cdrom,r
```

Con el comando xl list vemos las máquinas virtuales creadas y su configuración.

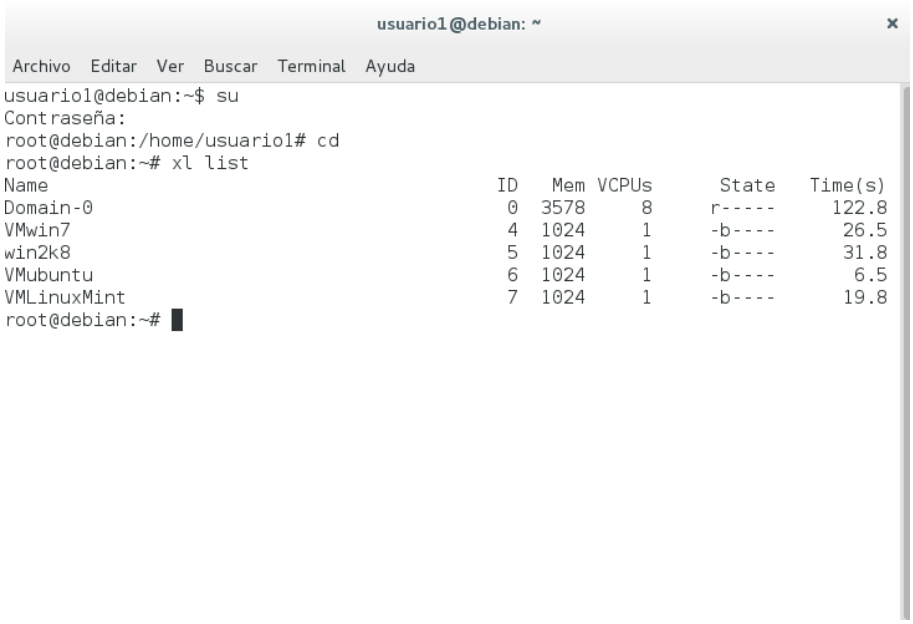

Fig. 23. Listado Máquinas virtuales creadas.

Realizamos una prueba adicional poniendo a correr las máquinas virtuales, luego con el comando **xentop** visualizamos el rendimiento de las VM.

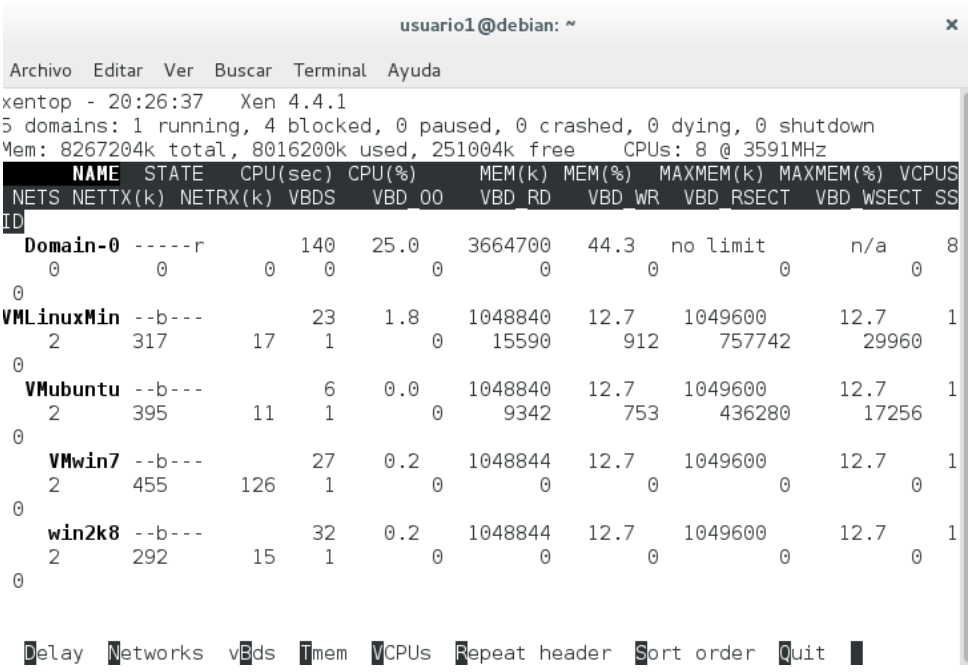

Fig. 24. Listado con rendimiento de las VM

Con esto finalizamos la instalación de nuestro entorno virtual.

5.5. APLICACIÓN DE LA METODOLOGIA ACRD

A continuación vamos aplicar la metodología en un entorno virtual creado en XEN y compuesto de la siguiente forma:

- El entorno virtual está compuesto por el DOM 0 que es el Hipervisor X por cuatro DOMU que son las cuatro máquinas virtuales VM.

- Cuatro máquinas virtuales conectadas en red con los siguientes sistemas operativos Windows Server 2008, Windows 7 Pro, Ubuntu y Linux-Mint.

- Las maquinas Windows Server 2008, Windows 7 Profesional y Linux-Mint serán accedidas internamente. La máquina Ubuntu será accedida de forma remota.

Sobre este piloto experimental se deberán mitigar las brechas de seguridad expuestas durante el desarrollo de este trabajo, para ello aplicaremos la metodología ACRD para aislar las maquinas entre sí, aplicando un aislamiento de la red a la maquina Vmubuntu que va a tener acceso remoto y Dom0 que es el Hipervisor. Para Vmubuntu configuraremos el doble factor de autenticación y emplearemos una herramienta para para monitorizar el tráfico de red interno.

5.5.1. AISLAR LAS VM

El aislamiento de máquinas virtuales entre sí, es la primera parte de la metodología ACRD. En la instalación del Kernel donde íbamos a instalar el Hipervisor XEN, creamos una partición LMV para luego allí crear cuatro volúmenes (Vol01, Vol02, Vol03 y Vol04). Hasta aquí tendríamos cuatro VMs funcionando en volúmenes diferentes. Esto nos permitirá:

- Administrar las capacidades o propiedades de disco (lectura – Escritura) de acuerdo a las necesidades de cada Usuario.
- Clonar, mover, migrar o eliminar máquinas virtuales sin que se afecte el funcionamiento del entorno.

Posterior a esto debemos aplicar la metodología en la configuración de la red de tal manera que tengamos segmentos de red aislados mediante Bridges virtuales.

La siguiente información corresponde a la configuración de red de cada máquina virtual:

Nombre	Sistema operativo	Núcleos	Ram	Espacio Disco	Dirección ip
VMmint	Linux-Mint	1	1 Gb	20 Gb	192.168.0.5
Vmwin7	Windows 7 Pro	1	1 Gb	20 Gb	192.168.0.6
Vmubuntu	Ubuntu	1	1 Gb	20 Gb	192.168.0.7
Vmwin2K8	Windows server 2008	1	1 Gb	20 Gb	192.168.08

Tabla No 1. Información máquinas virtuales.

La configuración inicial de red con el que el inicia Kernel Xen es la siguiente:

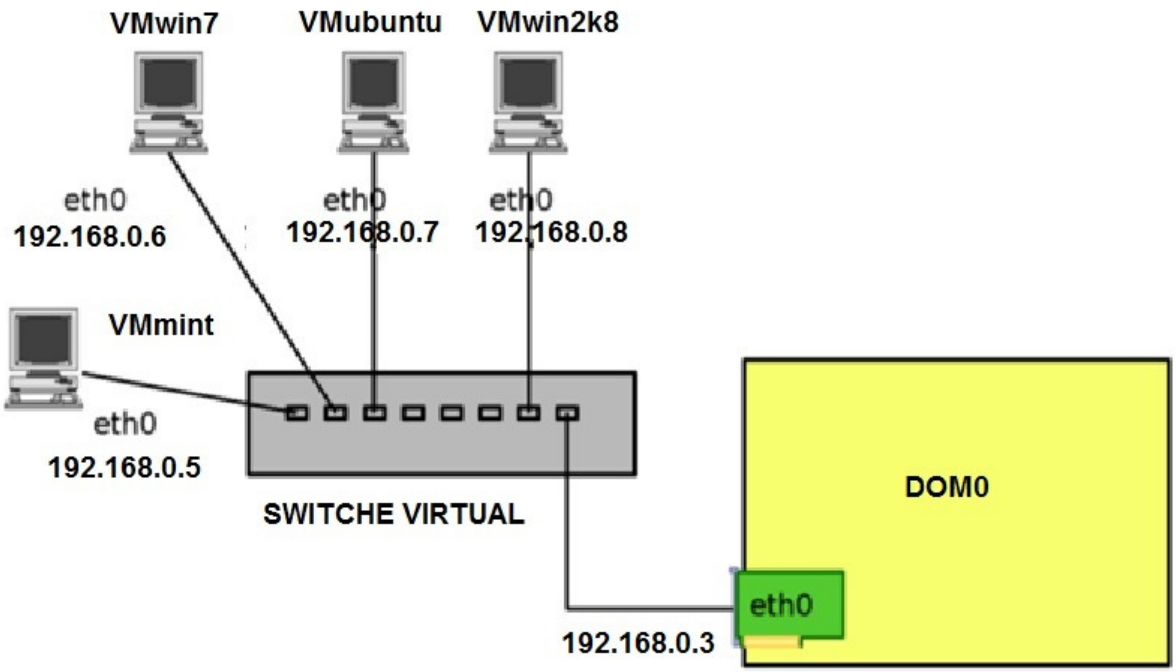

Figura 25. Configuración inicial de red en el Entorno Virtual.

En el esquema tenemos las cuatro máquinas virtuales conectadas a un switche virtual. Para configurar los tramos requeridos y aplicar el aislamiento que propone la metodología utilizaremos la configuración del entorno virtual en modo Bridge.

El objetivo que buscamos es aislar la maquina Dom0 de las maquinas DomU. De igual manera separar las DomU que tienen acceso interno y de la DomU con acceso externo (La que hemos llamado VMubuntu).

Inicialmente configuramos el entorno de red en el servidor Xen en modo bridge creamos un archivo llamado xend-config-sxp en el directorio xen y lo editamos con las siguientes líneas:

```
network-script network-bridge

vif-script vif-bridge
```

Reiniciamos el hipervisor para que se reconfigure la red. Cuando reiniciamos el sistema se ejecuta el siguiente script /etc/xen/scripts/network-bridge de tal manera que en el entorno tenemos un nuevo Bridge llamado br0, la interface Eth0 es desactivada y copiada a la red virtual Veth0 y renombrada como Peth0 y la interface Veth0 es renombrada como Eth0.
El entorno virtual quedaría configurado de la siguiente manera:

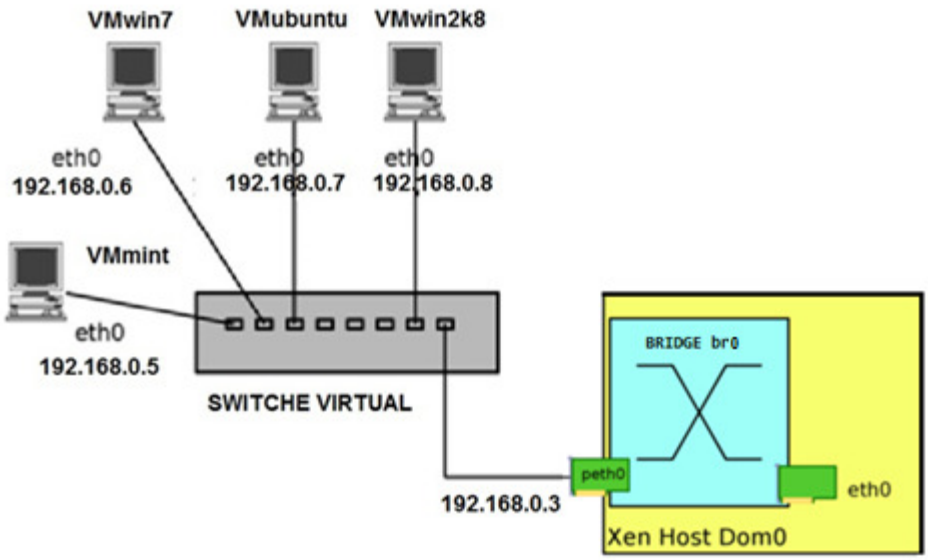

Figura 26. Subred con Birdge br0.

Como podemos ver hemos puesto a Dom0 en una red diferente a las maquinas DomU. El fichero interfaces queda modificado con el bridge que hemos creado br0.

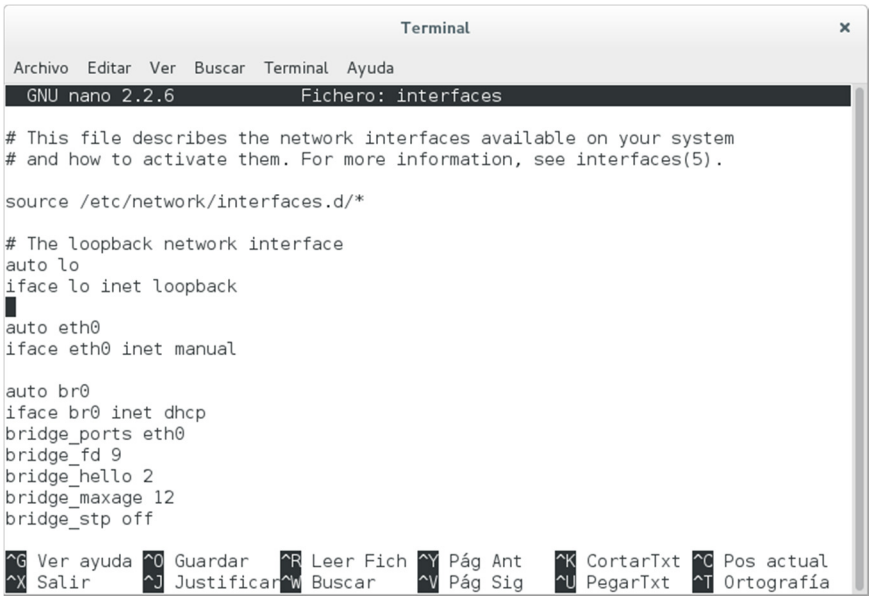

Figura 27. Configuración fichero interfaces.

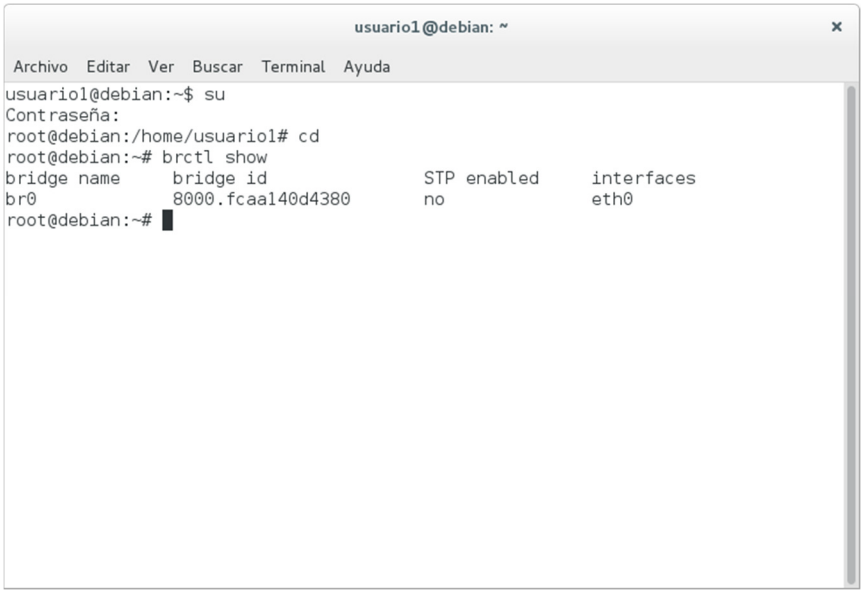

Figura 28 Uso el comando brctl para verificar el bridge creado.

Para darle más seguridad a nuestro entorno virtual debemos separar la DomU No 3 que es la que va a ser accedida remotamente del resto de VMs.

Para Vmubuntu (DomU No3) creamos un script en la siguiente ruta:

`/etc/xen/scripts/multi-network-bridge`

Este script debe tener el siguiente contenido:

```
/etc/xen/scripts/network-bridge "$@" netdev=eth1 bridge=br1
```

Configuramos la interfaz de red eth1 en modo manual en el archivo interfaces agregando las lineas:

```
# Interfaz fisica para bridge br1
auto eth1
iface eth1 inet manual
```

Una vez configurado el bridge, se lo asignamos a la maquina DomU3, accedemos al fichero de configuración de la VMubuntu y cambiamos la línea del vif asignándole al bridge br1 la dirección mac de la maquina VMubuntu :

```
vif = ["mac=00:16:3e:22:5f:98  ,bridge=br1" ]
```

Reiniciamos el sistema y verificamos que la VMubuntu está separada del resto de las DomU y de la Dom0

Ahora tenemos una estructura de la siguiente forma:

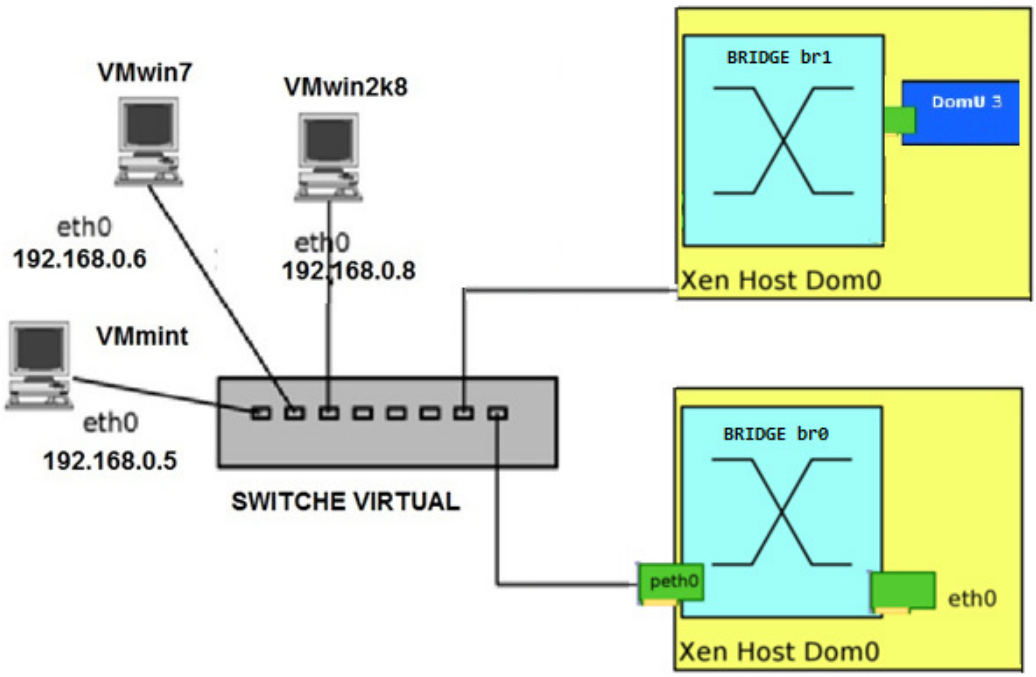

Figura 29 Configuración de red del entorno virtual.

5.5.2. CONTROL DE LOS RECURSOS EN LAS VM

Esta es una parte importante de la metodología. La configuración específica de cada máquina virtual debe quedar limitada a determinados recursos del sistema anfitrión, para ello editaremos el fichero /etc/xen-tools/xen-tools.cfg que es el lugar donde se guarda la configuración de las máquinas virtuales. El fichero lo editamos de la siguiente forma:

```
dir = /var/xen-gests          #donde se almacenan las máquinas virtuales
size = 20 Gb                  #tamaño del disco para cada máquina virtual.
memory = 1gb                  #cuanta memoria queremos utilizar
fs = ext3                     #tipo de sistema de ficheros
dist = etch                   #distribución de GNU/Linux
mirror = http://ftp.es.debian.org/debian/ #mirror
arch = amd 64                 #arquitectura de la pc
gateway = 192.168.1.1         #puerta de enlace
netmask = 255.255.255.0       #mascara de subred
kernel = /boot/vmlinuz-3.16.0.4      #el kernel que instalamos
```

Con este procedimiento nos aseguramos que cada VM solo tendrá 20 Gb de disco y utilizara un Giga byte de memoria ram.

Xen por defecto asigna un núcleo a cada máquina virtual, pero de acuerdo a la metodología ACRD debemos limitar todos los recursos (Disco duro, memoria y CPU) para evitar el efecto avalancha. En ese mismo orden de ideas debemos asegurar que cada VM solo use un núcleo, asignándole manualmente un Cores a cada VM mediante el siguiente comando:

```
Xe vm-param-set VCPUs-at-startup=1 uuid="uuid"
```

Mediante el procedimiento anteriormente descrito estamos limitando los recursos del computador anfitrión mitigando de esta forma el consumo excesivo de los mismos, cuando por ejemplo se dé el caso que se activen simultáneamente actualizaciones evitaremos le efecto avalancha dentro de nuestro entorno virtual.

5.5.3. ACCESO CON DOBLE FACTOR DE AUTENTICACION

De acuerdo a la metodología debemos tener un doble factor de autenticación sobre todo en las máquinas que son accedidas de forma remota. En nuestro piloto experimental tenemos la

maquina VMubuntu que es accedida de manera externa al entorno y sobre ella aplicaremos este control descrito en la metodología.

La metodología ACRD sostiene que es un método inseguro la autenticación tradicional que normalmente utilizamos. El empleo de usuario y contraseña debe ser reforzado en los entornos virtuales con una medida extra de seguridad.

Son tres factores que se pueden utilizar para validar usuarios:

- Algo que el usuario sabe, como una contraseña.
- Algo que el usuario tiene, como un token o una clave pública.
- Algo que el usuario es como el uso de huellas dactilares, iris, etc.

Para el piloto experimental, sobre el cual, aplicaremos la metodología ACRD utilizaremos un canal SSH para el acceso remoto a la maquina Vmubuntu (DomU3). Emplearemos en esta VM un sistema con doble factor de autenticación, que consistirá en la validación de usuarios con una contraseña y con una clave pública.

Inicialmente instalamos SSH en la maquina VMubuntu que vamos a acceder remotamente, con el comando

```
sudo apt-get install ssh
```

Como usuario Root creamos un usuario para hacer la prueba de conexión con nombre y contraseña.

```
sudo adduser testuser
```

Activamos el uso de clave pública en el fichero etc/ssh/sshd_conf agregando las siguientes tres líneas al script:

```
RSAAuthentication yes
PubKeyAuthentication yes
AuthorizedKeysFile      %h/.ssh/authorized_keys
```

En el escritorio remoto el cual va a ser un PC con Linux Mint editmos el fichero etc/ssh/ssh_conf y agregamos la línea

```
FowardAgent     yes
```

Esta línea nos permite activar un agente de claves para no tener que escribir cada vez que accedamos una clave de paso.

5.5.4. DETECCION DE TRAICO ENTRE LAS VM

La metodología ACDR para la gestión de riesgos en ambientes virtuales, requiere de un cuarto control que es el de la detección de tráfico entre VMs. Una vulnerabilidad importante que se plantea con la virtualización es que las comunicaciones entre VM se realizan a través del Hipervisor. Elementos de control y detección que se instalen en las redes como los Firewalls y los IDS/IPS no pueden tener acceso a este tráfico, por lo que se hace necesario la detección de trafico dentro de del entorno virtual.

Para la detección del tráfico entre máquinas virtuales utilizaremos la herramienta Ntopng. Esta aplicación es la última versión de la herramienta Ntop. Con Ntopgn podemos tener las siguientes funcionalidades:

- Detección de tráfico entre VMs utilizando multiples criterios como dirección IP. Protocolos, puertos.
- Muestra tráfico de red IPV4 e IPV6 en VMs activas.
- Producir informes a largo plazo sobre varios parámetros de red tales como rendimiento, protocolos de aplicación
- Top X conversadores / oyentes, top AS, aplicaciones L7 superiores.
- Para cada segmento de red realiza un informe de flujo de la comunicación / latencia de las aplicaciones / RTT, estadísticas TCP (retransmisiones, paquetes OOO, paquetes perdidos), y estadísticas de bytes por paquete.
- Mostrar la distribución del tráfico IP entre los diferentes protocolos.
- Analizar el tráfico IP y ordenarla según la fuente / destino.
- Mostrar matriz tráfico IP de subred (quién habla a quién?)
- Informe del uso de protocolos IP ordenados según tipo de protocolo.

Ntopng nos provee de los controles y la monitorización que se requiere para una detección eficiente entre VMs. Para poder poner en funcionamiento Ntopng debemos instalar previamente en el Hipervisor XEN los siguientes paquetes:

rrdtool
rrdtool-devel
init-system-helpers

libc0.1
libc6
libgcc1
libgeoip1
libhiredis0.10
libhiredis0.13
libjson-c2
libluajit-5.1-2
libndpi1a
libpcap0.8
librrd4
libsqlite3-0
libstdc++6
libzmq3
webmin
libpcap-dev
libglib2.0-dev
libgeoip-dev
redis-server
wget
libxml2-dev
build-essential
subversion

Luego con el programa de instalación apt-get en nuestro caso iniciamos la instalación de Ntopng.

```
Apt-get install ntpng ntopng-data nbox.
```

Creamos el directorio raíz

```
mkdir -p /etc/ntopng
```

Dentro del directorio ntopng necesitamos crear dos archivos el primero ntopng.start

```
nano /etc/ntopng/ntopng.start
```

A este archivo agregamos las siguientes líneas indicando la red que va a ser monitoreada:

```
--local-networks “192.168.0.0/24"
--interface 1
```

El segundo archi que vamos a crear es ntopng.conf:

```
nano /etc/ntopng/ntopng.conf
```

A este archivo agregamos las siguientes líneas

```
-G=/var/run/ntopng.pid
```

De esta forma terminamos la instalación de la herramienta Ntopng para detección de tráfico entre VMs. Con esto tenemos listo el piloto experimental para aplicar en el la metodología ACDR

5.5.5. PRUEBAS Y VALIDACION DE RESULTADOS

El entorno virtual sobre el cual vamos aplicar la metodología ACDR tiene la configuración y las herramientas necesarias para realizar para validar la efectividad de la metodología. Vamos a ir demostrando cada uno de los aspectos de dicha metodología.

5.5.5.1. PRUEBA DE AISLAMIENTO Y CONTROL DE RECURSOS

Se demostrara que las maquinas se encuentran aisladas entre sí y sus recursos controlados como medida de seguridad, para tal fin se instalaron las VMs en volúmenes diferentes y las más críticas en sectores de red diferentes. Esto con el fin de mitigar las siguientes amenazas y vulnerabilidades:

- Invasión del entorno virtual mediante ataque a maquinas que son accedidas de forma remota.
- Efecto avalancha por consumo de recursos por parte de una o varias VMs

Paso 1.

Verificamos la actividad de las maquinas sin estar inicializadas con el gestor de máquinas virtuales instalado en Xen. Verificamos la inactividad de las mismas.

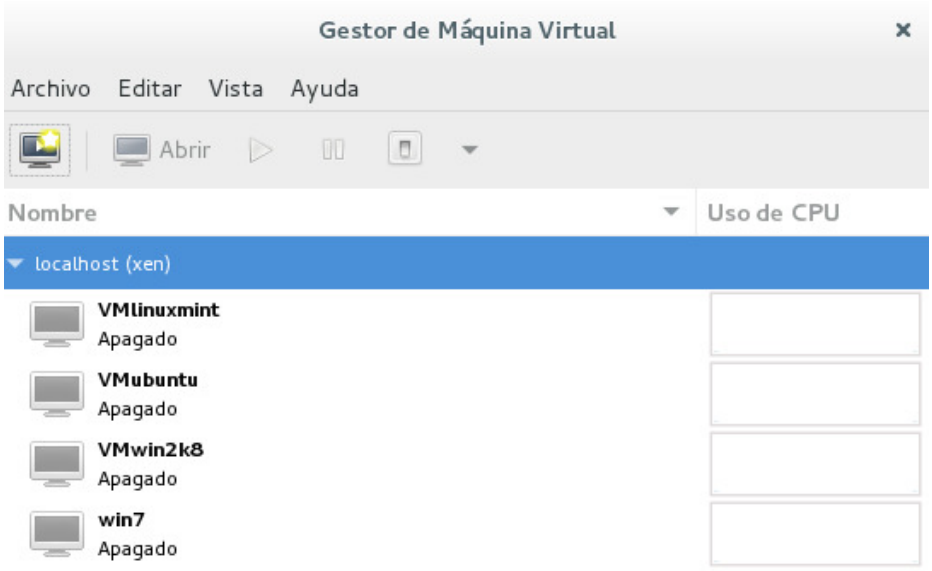

Figura 30. Máquinas virtuales apagadas.

Paso 2.

Encendemos las cuatro máquinas virtuales y podremos observar en la figura la actividad normal en cada una de ellas.

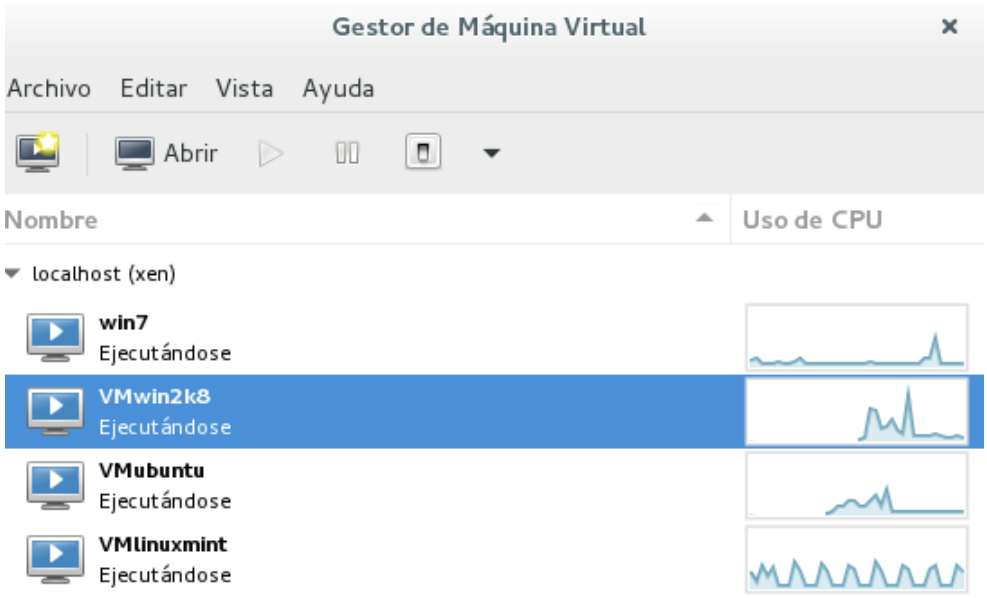

Figura 31. Reporte de actividad en cada VM.

Las VM en actividad normal, ejecución de aplicaciones, transferencia de archivos presenta el siguiente uso de los recursos.

Nombre	Uso de la CPU	Uso memoria Ram	Espacio Disco
VMmint	12%	12.7 %	8.9 Gb
Vmwin7	18%	22.8 %	8.6 Gb
Vmubuntu	11%	19.3 %	9.3 Gb
Vmwin2K8	8%	23.2 %	9.02 Gb

Tabla No 2. Consumo de recursos de las VM en actividad normal.

Paso 3.

Vamos a intentar producir un efecto avalancha saturando los recursos de la Vmubuntu y observaremos si afecta el funcionamiento de las otras máquinas virtuales. Para tal fin iniciaremos la descarga de un archivo por internet, realizamos un análisis con el antivirus Bitdefender, realizamos una actualización del Ubuntu. Con esto conseguimos llevar al limite la máquina virtual

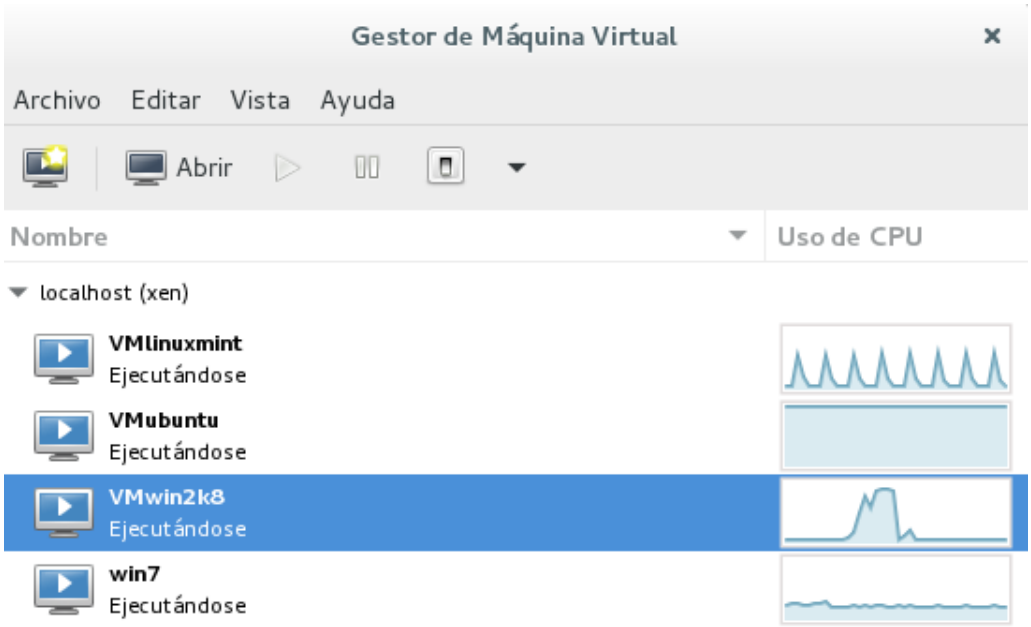

Figura 32. Saturación maquina VMubuntu.

Observemos ahora los indicadores

Nombre	Uso de la CPU	Uso memoria Ram	Espacio Disco
VMmint	15%	12.7 %	8.9 Gb
Vmwin7	23%	22.8 %	8.6 Gb
Vmubuntu	98%	89.9 %	9.3 Gb
Vmwin2K8	1%	16.3 %	9.02 Gb

Tabla No 3. Maquina VMubuntu saturada.

VALIDACION DE RESULTADOS.

Como podemos observar las VMs del entorno no se ven afectadas en su rendimiento por la saturación de procesos de la maquina Ubuntu. Hemos Seguido saturando la maquina Ubuntu hasta que la llevamos a un punto de bloqueo y las VM continúan su funcionamiento normal. Lo que si observamos, fue que el gestor de máquinas virtuales quedo inactivo luego de que la Vmubuntu dejo de funcionar. Apagamos la máquina virtual Vmubuntu, el gestor que es usado para reportes volvió a la normalidad. Lo más relevante de los resultados es que el entorno no se vio afectado y que el resto de VMs continuaron funcionando normalmente y con sus recursos (CPU y Ram) a niveles habituales.

5.5.5.2. PRUEBA DE CONTROL DE ACCESO A MAQUINAS VIRTUALES

Dentro del entorno virtual tenemos una máquina que configuramos para que pueda ser accedida remotamente, instalamos en ella los servicios para el uso de un canal SSH. La máquina fue ubicada en una subred aparte del resto de VMs por medio de un bridge Br1, el bridge se comunica por el puerto Peth1. Al verificar la dirección Ip está a cambiado a 192.168.122.98.

Paso1.

Desde una maquina por fuera del entorno y con el sistema operativo Linux Mint instalado, intentamos acceder por medio de un canal SSH a la maquina VMubuntu. Aun si digitamos la contraseña de acceso nos da un error de clave pública y pasword.

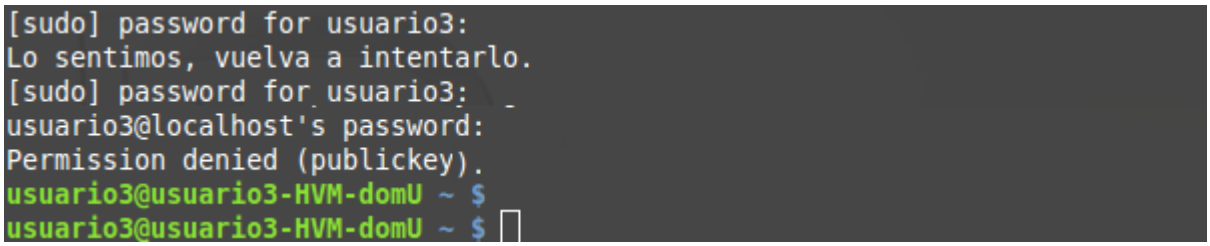

Figura 33. Acceso denegado por falta de clave pública.

Paso2.

Para que el acceso remoto funcione debemos realizar la instalación de clave pública. En el escritorio remoto creamos un usuario para el acceso testuser2 y generamos una clave pública que utiliza el sistema criptográfico de clave pública RSA con el siguiente comando:

ssh-keygen –t rsa

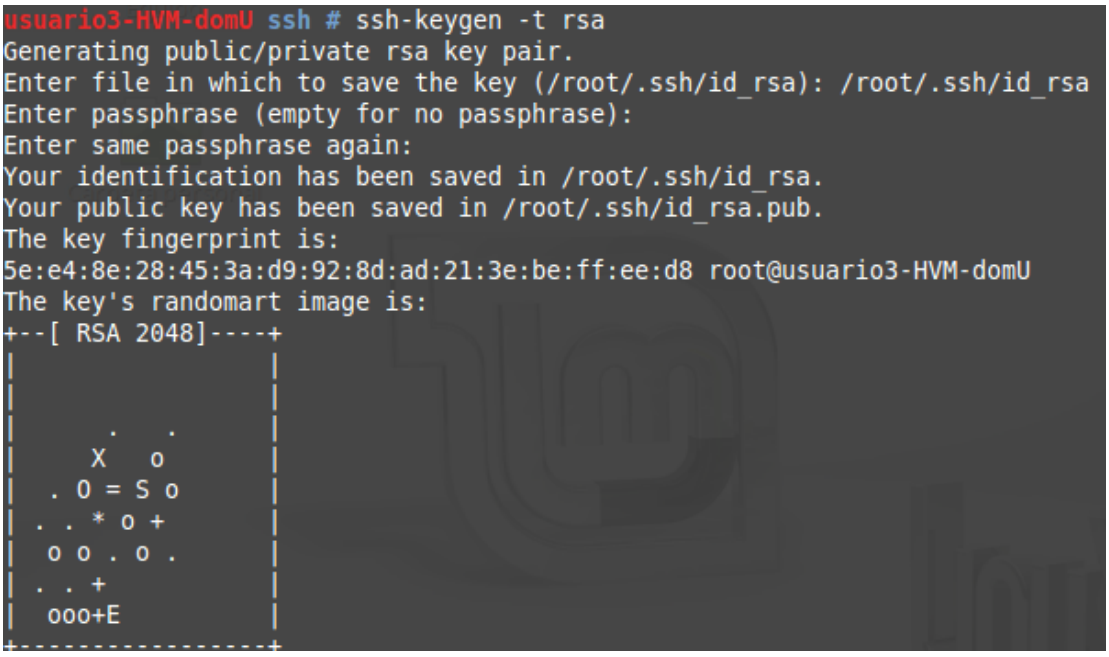

Figura 34. Generación de clave pública en el escritorio remoto.

Paso 3.

Escribimos la ruta donde vamos a guardar la clave pública generada y el digitamos una llave de paso que debe tener como mínimo 5 caracteres, esta clave pública la copiamos en VMubuntu en la siguiente ruta /home/testuser/.ssh/id_rsa.pub.

Lo que nos queda por hacer es añadir la llave pública generada en la maquina VMubuntu a una lista de llaves públicas autorizadas con el siguiente comando:

cat id-rsa.pub authorized keys

Para garantizar aún más la seguridad del sistema, cambiamos los permisos para que excepto el usuario autorizado, pueda leer o modificar el fichero de claves públicas.

chmod go –rwx authorized_keys rsa_pub

Paso 4.

Con este procedimiento cada vez que el equipo remoto quiera acceder a la VMubuntu del entorno el usuario deberá colocar la contraseña y digitar el código de la clave pública y de esta forma tenemos configurado el doble factor de autenticación en la VM que es accedida remotamente.

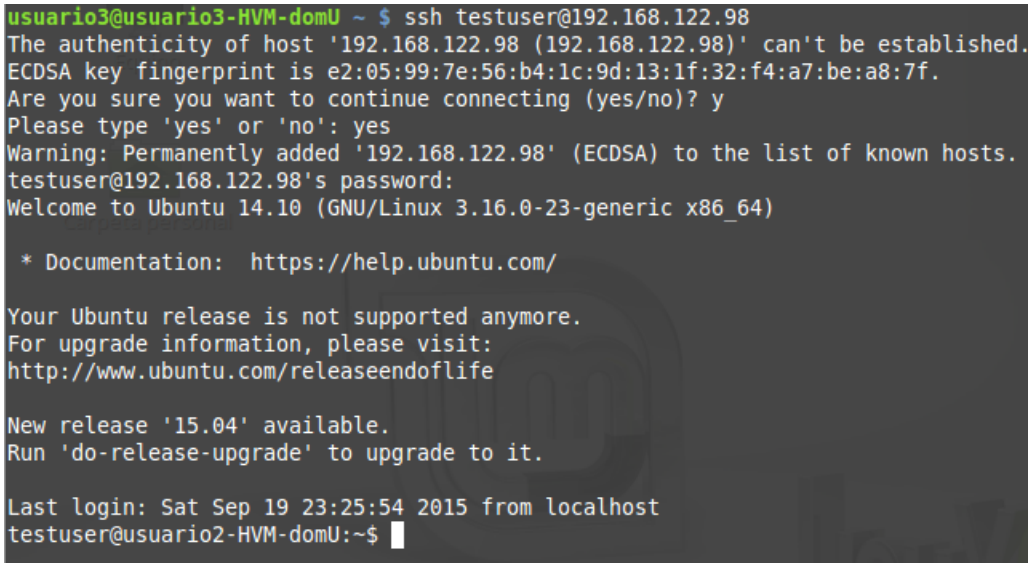

Figura 35. Verificación de acceso luego de configurar la clave pública.

VALIDACION DE RESULTADOS

Como podemos observar solo cuando se genera una clave pública y se agrega a la lista de claves públicas validas (archivo .ssh) es que podemos tener acceso a la VMubuntu. Se intentó acceder al resto de máquinas virtuales pero genera un error en la coneccion con lo que garantizamos que el entorno virtual está protegido y solo la Vmubuntu tiene acceso remoto, pero con doble factor de autenticación.

```
usuario3-HVM-domU usuario3 # ssh user1@192.168.0.5
ssh: connect to host 192.168.0.5 port 22: Connection refused
usuario3-HVM-domU usuario3 #
```

Figura 36. Acceso remoto denegado, a otra Vm del entorno virtual

5.5.5.3. PRUEBA DE DETECCION DE TRÁFICO EN EL ENTORNO VIRTUAL

El tráfico entre las máquinas virtuales es una brecha de en a seguridad que presentan este tipo de entornos, se deben de utilizar herramientas específicas que funcionen con la virtualización. La metodología ACDR plantea un cuarto control que es la detección de tráfico para ello utilizaremos la aplicación Ntopng.

Paso 1.

La herramienta corre a través de un navegador compatible con html o Ajax. En la maquina Hipervisor Xen tenemos el navegador Iceweasel que el navegador por defecto de Debian. Abrimos el navegador y en la ventanilla de direcciones digitamos http://localhost:3000. Nos pide usuario y contraseña que por defecto es admin y admin. Antes de arrancar el analizador de trafico encendimos las máquinas virtuales y realizamos una coneccion SSH entre una maquina externa la entorno (sistema operativo Linuxmint, dirección Ip 192.168.0.2) y la VMubuntu (dirección IP 192.168.122.98)

Paso 2.

Usamos el navegador de cada máquina para acceder a diferentes páginas Web y determinar ese tráfico. El primer reporte que obtuvimos es el de flujo de tráfico de VMs.

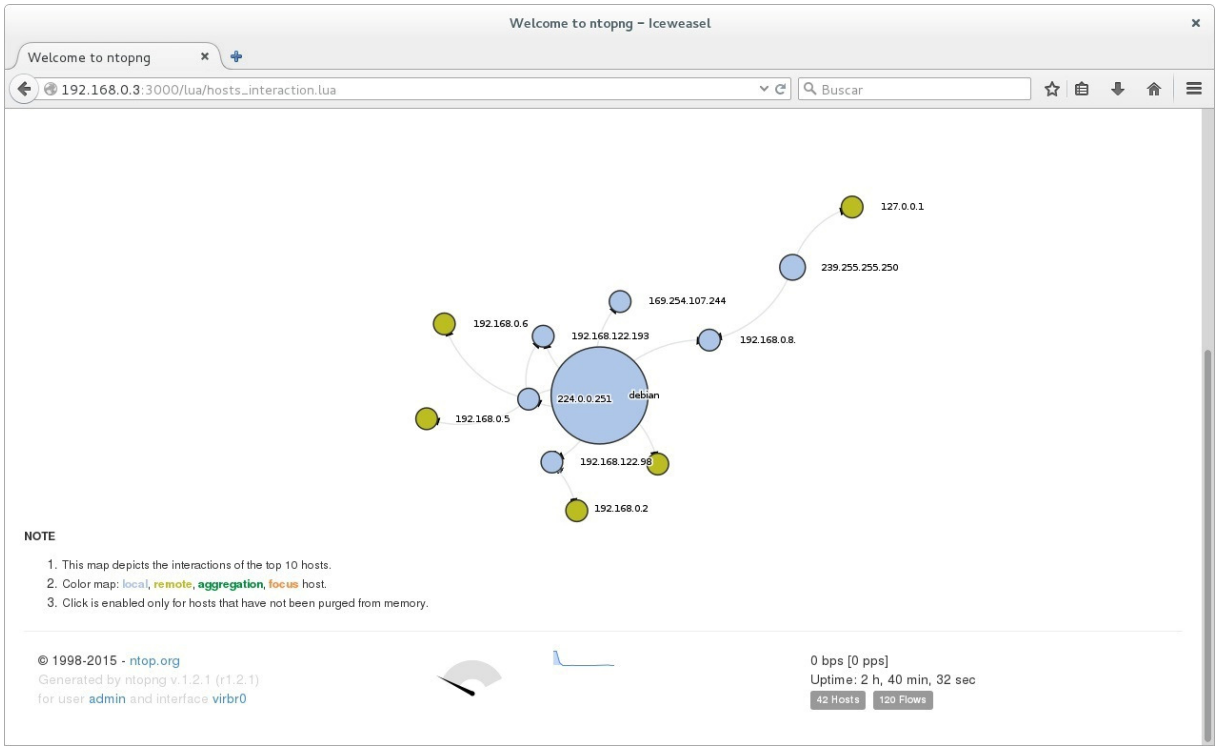

Figura 37. Flujo de tráfico de las Máquinas Virtuales

En la figura podemos observar cada máquina virtual con un círculo azul, en cada máquina tenemos acceso a internet círculos verdes, hicimos ping entre las maquinas Vmwin7 y Vmlinuxmint (Ips 192.168.0.5 y192.168.0.6) en el informe tenemos una línea que las conecta. La máquina Vmubutu (Ip 192.168.122.98) está conectada a una maquina externa por medio de un canal SSH. Esa máquina externa está identificada con un círculo verde y con la dirección IP 192.168.0.2.

Paso 2.

Requerimos de un informe detallado de cada Máquina virtual, el host al que está conectado el tiempo de conexión, los datos transmitidos y las posibles alertas que pudieran generar ese tráfico

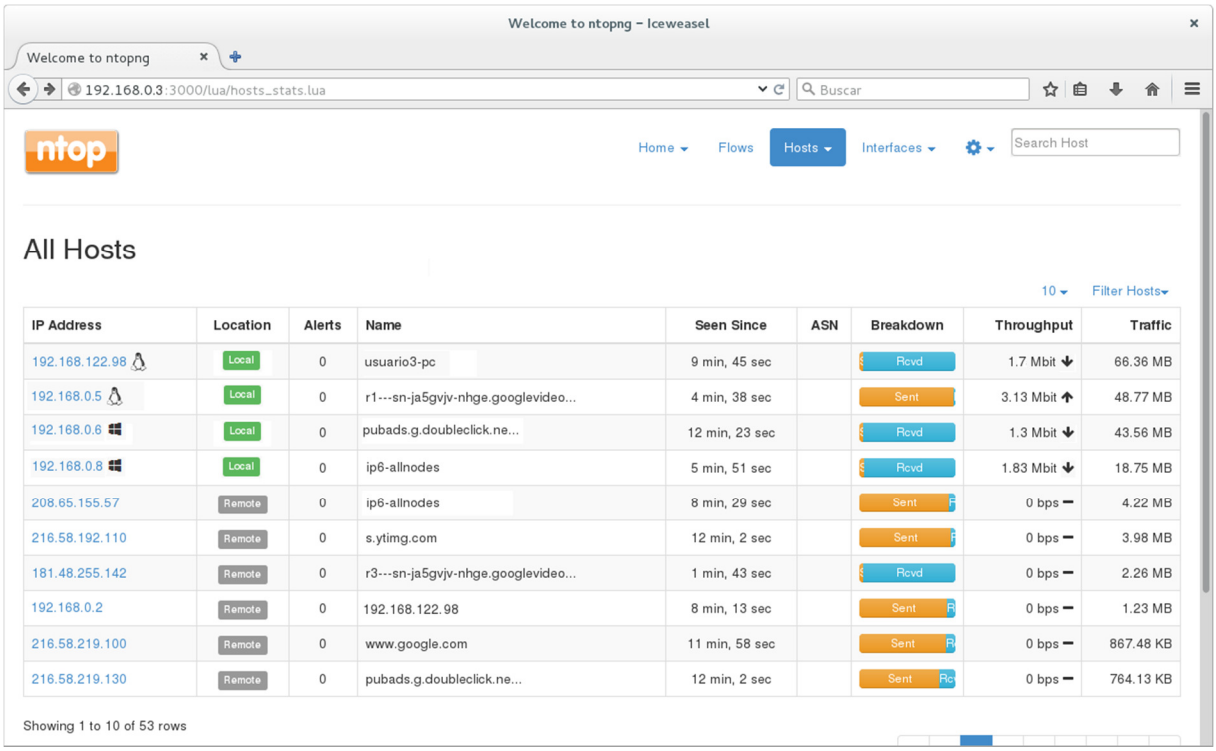

Figura 38. Reporte análisis de trafico Máquinas virtuales.

En el reporte podemos ver las cuatro máquinas de nuestro entorno virtual. Observamos en primera instancia la Vmubuntu (Ip 192.168.122.98) conectada al usuario tres y más abajo vemos el mismo usuario como host remoto (Ip 192.168.0.2) conectado a la maquina VMubuntu. Vemos las otras máquinas realizando procesos en la web de subida de archivos (Maquina VMlinuxmint) y descarga de archivos en las dos máquinas. No se observan alertas producto de tráfico malicioso, las últimas dos columnas nos indican el volumen de trabajo o de información que fluye a través del sistema.

VALIDACION DE RESULTADOS.

Con la herramienta Ntopng obtenemos la información de tráfico hacia el interior del entorno. Al ser instalada en el Hipervisor y configurada específicamente para red virtual del piloto experimental, pudimos obtener los resultados de acorde al control descrito en la metodología ACDR. Pudimos tener un reporte de las conexiones entre VMs el tráfico de adentro y hacia afuera del entorno. De igual manera se llevó a cabo la detección del acceso remoto del que era objeto una de las máquinas virtuales.

6. CONCLUSIONES Y TRABAJO FUTURO

6. 1. CONCLUSIONES

Durante el desarrollo este trabajo se ha definido y aplicado una metodología cuyo objetivo principal es proporcionar la gestión de seguridad en ambientes virtuales. La virtualización es una tecnología en pleno crecimiento, pero que de acuerdo a lo que hemos estudiado aún falta por desarrollar sistemas de seguridad que la hagan más confiable.

La metodología ACRD contribuye a subsanar falencias en la seguridad, mediante una interrelación de procedimientos que se aplican para mitigar vulnerabilidades específicas de los ambientes virtuales. Se ha conseguido el objetivo propuesto al comienzo del proyecto, puesto que se ha obtenido para cada brecha en la seguridad un procedimiento determinado que nos ayuda a separar cada Host de sus vecinos, a controlar recursos que pueden ser agotados cuando existe un mal manejo de las máquinas virtuales, hemos proporcionado además controles de autenticación robustos para los accesos remotos y puesto en marcha un sistema de detección de tráfico entre las máquinas virtuales que nos permite tener una visión de lo que sucede hacia el interior del sistema.

Este trabajo de Fin de Master nos permitió conocer y estudiar conceptos fundamentales relacionados con la virtualización de recursos informáticos, este conocimiento fue necesario para el posterior planteamiento de la metodología. Se llevó a cabo un recuento histórico de cómo surgieron las tecnologías de virtualización y como han llegado a ser una de las soluciones más utilizadas en la implementación de sistemas de información por aspectos tan relevantes como economía, funcionalidad y aporte a la conservación del medio ambiente

Los resultados de la evaluación realizada, con la puesta en marcha del piloto experimental, nos ofrece una visión de cómo podemos aplicar la metodología propuesta y nos aporta múltiples e interesantes conclusiones. Podemos afirmar que se ha conseguido un cumplimiento global para los aspectos de seguridad planteados y que corresponden a la mitigación de vulnerabilidades específicas de los ambientes virtuales.

6.2. TRABAJO FUTURO

Para una aproximación de cara hacia el futuro se plantean una serie de propuestas como posibles mejoras técnicas con respecto a la metodología definida, como se describe a continuación:

- Inclusión de más aspectos de seguridad complementarios como clonado de VMs y sistemas de snapshot.
- Aumentar el abanico de seguridad propuesto con una VM Ossim trabajando dentro del entorno.
- Desarrollar mecanismos de autenticación alternativos como el uso de lectores biométricos o tokens.
- Profundizar acerca del licenciamiento de máquinas virtuales pues en la actualidad existen muchos vacíos al respecto.

La metodología ACRD puede ser aplicada en controles de seguridad de la información en la Cloud Computing, pero aún falta profundizar más acerca de implementación de la metodología en este tipo de ambientes virtuales. También se debe relacionar aún más la metodología con el nuevo estándar ISO/IEC 27018 de agosto del año 2014, que es específica para servicios en la nube.

7. GLOSARIO, TERMINOS Y ACRONIMOS

API:

Application Programming Interface

Applience Virtual:

Se trata de una Máquina Virtual (VM a partir de ahora) que se encuentra alojada en algún sitio de internet, con un formato comprimido llamado OVF (Open Virtualization Format).

Cloud Computing:

Tecnología que permite ofertar servicios de cómputo y almacenamiento de forma remota, a través de una red.

Dom 0:

Dom0 es el dominio inicial en el Hipervisor Xen durante su arranque. Dom0 es una abreviatura de "Dominio 0" (a veces escrito como "dominio cero" o el "dominio del host"). Dom0 es un dominio privilegiado que empieza primero y gestiona los dominios sin privilegios de los DomU.

DomU:

Un DomU es la contrapartida de Dom0; es un dominio sin privilegios por defecto y no tiene acceso directo al hardware. Se debe ejecutar un Frontend Driver para que el hardware multiplexado se pueda compartir con otros dominios.

Hipervisor:

Capa intermedia entre el hardware del equipo donde se instala y los diferentes entornos virtuales que pueden correr sobre él.

Hipervisor Nativo:

Es él se ejecuta directamente sobre el hardware o máquina Host (bare-metal) y es el que se encarga de controlar todos los accesos al hardware

Hipervisor Hosted:

Hipervisor que se ejecuta sobre un sistema operativo.

Hipervisor Hibrido:

En este modelo tanto el sistema operativo anfitrión como el Hipervisor interactúan directamente con el hardware físico.

Imagen ISO:

Una imagen ISO es un archivo informático donde se almacena una copia o imagen exacta de un sistema de archivos o ficheros de un disco óptico, normalmente un disco compacto (CD) o un disco versátil digital (DVD).

Network:

Objeto Xen que representa un switch ethernet virtual. Puede haber más de uno en cada host Xen.

Para virtualización:

Es una técnica de programación informática que permite virtualizar por software sistemas operativos. El programa paravirtualizador presenta una interfaz de manejo de máquinas virtuales. Cada máquina virtual se comporta como un computador independiente, por lo que permite usar un sistema operativo o varios por computador emulado.

PIF:

Objeto que representa una interfaz de red física de un host en XenServer. También representa una agrupación lógica (bond) de varias interfaces físicas.

SNAPSHOT:

En informática es una copia instantánea de volumen es una instantánea del estado de un sistema en un momento determinado. El término fue acuñado como una analogía a la de la fotografía. Puede referirse a una copia real del estado de un sistema o de una capacidad que ofrecen los sistemas de copia de seguridad.

TIC:

Tecnologías de la Información y la Comunicación

VIF:

Objeto que representa una interfaz de red virtual de una máquina virtual en XenServer. Es lo que va a detectar la máquina virtual dispositivo de interfaz de red.

VLAN:

Una VLAN, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.1 Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

8. REFERENCIAS BIBLIOGRAFICAS

Archlinux. (2.015). Xen. Recuperado de https://wiki.archlinux.org/index.php/Xen_(Espa%C3%B1ol)

Barry, D. (2.009). Cloud Computing: las pruebas de la nube. Recuperado de https://technet.microsoft.com/es-es/magazine/hh395480.aspx

Capacity. (2.012). ¿Qué es la virtualización y cuáles son sus beneficios?. Recuperado de http://blog.capacityacademy.com/2012/08/07/que-es-la-virtualizacion-y-cuales-son-sus-beneficios/

Cerda, C. (2012). Tips para hacer eficiente a tu empresa. Recuperado de http://www.cnnexpansion.com/opinion/2012/12/17/tips-para-hacer-eficiente-a-tu-empresa.

Clusif. (2.007). Mehari. Recuperado de http://www.clusif.fr/fr/production/ouvrages/pdf/MEHARI-2007-Introduccion.pdf

Davis, M. (2.011). ¿Cómo controlar la seguridad de la virtualización? Recuperado de http://www.informationweek.com.mx/analysis/como-controlar-la-seguridad-de-la-virtualizacion/

DMTF. (2.009). Open Virtualization Format Specification. Recuperado de http://www.dmtf.org/sites/default/files/standards/documents/DSP0243_1.0.0.pdf

Echaiz, J., Ardhengi, J. (2.008). Seguridad en Entornos Virtuales. Recuperado de http://sedici.unlp.edu.ar/bitstream/handle/10915/19828/Documento_completo.pdf?sequence

El Magazine de la Virtualización & Cloud Computing. (2.004).¿Qué es el Hypervisor? Recuperado de http://www.virtualizacion.com/hypervisor/

Estréllate y Arde. (2.007). Máquina virtual Xen. Recuperado de http://www.estrellateyarde.org/virtualizacion/maquina-virtual-xen

Garcia, M. (2.015) Comandos básicos para Xen. Recuperado de http://www.nettix.com.pe/manuales/virtualizacion/181-comandos-basicos-para-xen

Hofman, J. (2.012). Virtualización: Virtualización en y más allá de la nube. Recuperado de https://technet.microsoft.com/es-es/magazine/hh855066.aspx

Isaca. (2.015). Presentan la primera norma ISO sobre seguridad en la nube - ISO 27018. Recuperado de http://www.isaca.org/chapters8/Montevideo/NewsandAnnouncements/Pages/Page2.aspx

Jones, T. (2.010). Virtualization. Recuperado de http://www.datamation.com/netsys/article.php/3884091/Virtualization.htm

Moreno, P. (2.011). Centos 5: Virtualizando Windows con Xen 4.x. Recuperado de http://pheriko.blogspot.com/2011/10/centos-5-virtualizando-windows-7-con.html

Normas ISO. (2.015). Análisis de la Norma ISO / IEC 27018 2014 Requisitos para la protección de la información de identificación personal (PII) en sistemas cloud. Recuperado de http://www.normas-iso.com/2015/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-persona

Ortega, L. (2.008). Instalar Windows en una VM Xen. Recuperado de https://ortegaga.wordpress.com/2008/02/17/instalar-windows-en-una-vm-xen/

Ramírez, M. (2.012). Protección coordinada: seguridad adaptada a la dinámica actual del CPD. Recuperado de http://www.datacenterdynamics.es/focus/archive/2012/11/protecci%C3%B3n-coordinada-seguridad-adaptada-la-din%C3%A1mica-actual-del-cpd

Red Hat. (2.015). Gestión del Administrador de volumen lógico. Recuperado de https://access.redhat.com/documentation/es-ES/Red_Hat_Enterprise_Linux/6/html-single/Logical_Volume_Manager_Administration/index.html#PV_label

RFFP. (2.009). LVM: Ventajas sobre el particionado tradicional. Recuperado de https://modulado.wordpress.com/2009/01/07/lvm-ventajas-sobre-el-particionado-tradicional/

rm-rf.es. (2.009). Usar múltiples interfaces de red en virtualización Xen. Recuperado de

http://rm-rf.es/usar-multiples-interfaces-red-virtualizacion-xen/

Rodríguez, J. (2.015). Seis mitos de la protección de ambientes virtuales. Recuperado de http://www.b-secure.co/blog/mitos-de-la-proteccion-de-ambientes-virtuales.

Rozalem, R. (2.014) Cinco claves de seguridad para entornos virtualizados. Recuperado de http://www.siliconnews.es/2014/07/16/cinco-claves-de-la-seguridad-para-entornos-virtualizados/

Segu-Info. (2.009). Seguridad Lógica - Identificación y Autentificación. Recuperado de http://www.segu-info.com.ar/logica/identificacion.htm

Wiki.Debian. (2.012). Xen. Recuperado de https://wiki.debian.org/es/Xen

Wikipedia. (2.015). Computacion en la nube. Recuperado de https://es.wikipedia.org/wiki/Computaci%C3%B3n_en_la_nube

Wikipedia. (2.015). Hipervisor. Recuperado de http://es.wikipedia.org/wiki/Hipervisor

Wikipedia. (2.015). Metodología. Recuperado de https://es.wikipedia.org/wiki/Metodolog%C3%ADa

Wiki.Xen. (2.012). Xen Overview. Recuperado de http://wiki.xen.org/wiki/Xen_Overview/es

Wiki.Xen. (2.014). XL. Recuperado de http://wiki.xen.org/wiki/XL

Xennetap, (2.009) Copias de seguridad en máquinas virtuales Xen. Recuperado de http://xennetapp.blogspot.com/2009/10/copias-de-seguridad-de-maquinas.html.