Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

La Seguridad Informática en infraestructuras tecnológicas virtuales

Autor:
Pablo Roberto Sandoval Barrantes

Tutor de Trabajo Final:
Dr. Juan Pedro Hecht

Año de presentación: 2019
Cohorte: 2018

Declaración Jurada

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Pablo Roberto Sandoval Barrantes
DNI: 95853656, Pasaporte Costarricense: 401940201

Resumen

La presente investigación indaga las infraestructuras tecnológicas virtuales convergentes y servicios en la nube, comprende sus orígenes y componentes claves, para posteriormente generar una visión sólida que permita hacer un análisis crítico y profesional de la seguridad informática entorno a este tipo de plataformas tecnológicas de actualidad, lo anterior a la luz de la bibliografía existente y el aporte profesional del autor.

El interés radica en como durante la última década la tecnología de virtualización ha evolucionado dando pasos gigantescos en comparación a sus inicios documentados en los años sesenta, y si nos ubicamos cronológicamente a finales de los años noventa nos encontramos con la virtualización básica de equipos servidores de producción y la complejidad de estos para interconectarse a través de redes físicas, costoso almacenamiento y limitado procesamiento computacional, lo que hizo que este tipo de herramientas informáticas no estuvieran al alcance de todos y no eran viables de fabricar en ese entonces.

Ahora bien, en los últimos años ocurrió un salto tecnológico importante tanto en costos como en avance de procesamiento computacional, las organizaciones tuvieron acceso a equipos tecnológicos eficientes, las redes se globalizaron y tomaron relevancia, por lo que se generó un atractivo mercado para las empresas fabricantes. Lo anterior dio origen a las recientes infraestructuras convergentes e hiperconvergentes y servicios en la nube informática, esto aliviano la complejidad operativa y administrativa de las compañías, agregó un valor real al negocio y establecieron el rumbo o futuro próximo en este tema tecnológico.

Por lo anterior, esta investigación determina los orígenes, componentes, y estado actual de las infraestructuras tecnológicas virtuales, profundiza sus aspectos elementales, y entrega conclusiones valiosas relacionadas a la seguridad informática en este tipo de entornos virtuales modernos, incentivando nuevas investigaciones alrededor de esta temática.

Palabras claves: Infraestructura tecnológica, convergencia tecnológica, virtualización tecnológica, nube tecnológica, seguridad informática.

Índice de contenidos

Índice de figuras

Índice de tablas

Agradecimientos

A Dios, mi esposa, mis padres, familia, y amigos, que en todo momento me brindaron el apoyo incondicional para cumplir la meta propuesta.

A la Universidad Estatal a Distancia (UNED) en la República de Costa Rica, Institución Benemérita de la Patria que me patrocinó durante toda la carrera y además confió en mi persona la gran responsabilidad de especializarme en seguridad informática en la República Argentina.

A todo el personal del Acuerdo de Mejoramiento Institucional (AMI), a la Unidad Coordinadora del Proyecto Institucional (UCPI) y su Directora Heidy Rosales Sánchez quien con un gran equipo de trabajo han realizado una admirable labor con las iniciativas que fortalecerán el modelo de educación a distancia en la UNED.

Al Consejo de Becas Institucional (COBI), por su labor en seguimiento durante el proceso de beca.

A todo el personal de la Dirección de Tecnología de Información y Comunicaciones (DTIC), liderados por el Mag. Francisco Durán Montoya, que me abrieron las puertas para ser parte del equipo, y han depositado su confianza en este proceso.

A la Unidad de Infraestructura Tecnológica (UIT), liderados por el Mag. Rolando Rojas Coto, quienes me han brindado palabras de aliento y acompañamiento durante este proceso.

A todo el personal administrativo y docente de la Carrera de Especialización en Seguridad Informática de la Universidad de Buenos Aires, que durante todo el proceso me acompañaron, me instruyeron, me guiaron, y me brindaron todo el apoyo que necesité.

Al Dr. Juan Pedro Hecht, coordinador académico de la Carrera de Especialización en Seguridad Informática de la Universidad de Buenos Aires, por su compromiso como tutor, su trayectoria científica, y su entrega a la carrera.

A la República Argentina, a todas sus personas que me brindaron calor humano durante mi estadía en la Ciudad de Buenos Aires, y que se convirtieron en mi familia argentina, me hicieron parte de esta gran Nación.

Nómina de abreviaturas

BCP: *Business Continuity Plan* o Plan de Continuidad del Negocio

BIA: *Business Impact Analysis* o Análisis de Impacto al Negocio

CERT: *Computer Emergency Response Team* o Equipo de Respuesta ante Emergencias Informáticas

CIFS: *Common Internet File System* o Sistema de archivos de Internet

CN: Continuidad del Negocio

CPU: *Central Processing Unit* o Unidad Central de Procesamiento

CSIRT: *Computer Security Incident Response Team* o Equipo de Respuesta ante Incidencias de Seguridad Informáticas

CVE: *Common Vulnerabilities and Exposures* o Vulnerabilidades de Seguridad Conocidas

DDoS: *Distributed Denial of Service* o Ataque de Denegación de Servicio

DHCP: *Dynamic Host Configuration Protocol* o Protocolo de Configuración Dinámica de Host

DMZ: *Demilitarized Zone* o Zona desmilitarizada

DNS: *Domain Name System* o Sistema de Nombre de Dominios

DRP: *Disaster Recovery Plan* o Plan para la Recuperación de Desastres

FC: *Fibre Channel* o Canal de Fibra

FCoE: *Fibre Channel over Ethernet* o Canal de Fibra sobre red Ethernet

HCI: *Hyper-Converged Infrastructure* o Infraestructura Hiperconvergente

IA: Inteligencia Artificial

IBM: *International Business Machines Corporation*

IDS: *Intrusion Detection System* o Sistema de Detección de Intrusiones

IoT: *Internet of Things* o Internet de las cosas

IPS: *Intrusion Prevention Systems* o Sistema de Prevención de Intrusiones

iSCSI: Internet SCSI

ISF: *Information Security Forum* o Foro de Seguridad de la Información

KVM: *Kernel-based Virtual Machine* o Máquina virtual basada en el núcleo

Modelo OSI: *Open System Interconnection* o Modelo de Interconexión de Sistemas Abiertos

NFS: *Network File System* o Sistema de Archivos en Red

NIC: *Network Interface Card* o Tarjeta de Interfaz de Red

NIST: *National Institute of Standards and Technology* o Instituto Nacional de Estándares y Tecnología

PDCA: Círculo de Deming, (Planificar-Hacer-Verificar-Actuar)

RAM: *Random Access Memory* o Memoria de Acceso Aleatorio

SCSI: *Small Computer System Interface* o Pequeña interfaz de sistema de cómputo

SDDC: *Software-defined data center* o Centro de Datos Definido por Software

SGSI: Sistema de Gestión de la Seguridad de la Información

SIEM: *Security Information and Event Management* o Sistema de Gestión de Información y Eventos de Seguridad

SLA: *Service Level Agreement* o Acuerdo de Nivel de Servicio

SMB: *Server Message Block* o bloque de mensajes de servidor

TIA: *Telecommunications Industry Association* o Asociación de la Industria de Telecomunicaciones

VDI: *Virtual Desktop Infrastructure* o Infraestructura de Escritorio Virtual

VLAN: *Virtual Local Area Network* o Red de Área Local Virtual

VM: *Virtual Machine* o Máquina Virtual

VMWare: *VMware Corporation*

vNIC: *Virtual Network Interface Card* o Tarjeta de Interfaz de Red Virtual

VoIP: *Voice over IP* o Voz Sobre IP/Voz Sobre Internet

VPN: *Virtual Private Network* o Red Privada Virtual

Introducción

A partir de la importancia que representa el uso de la virtualización de infraestructura computacional en las organizaciones actuales, resulta necesario investigar el creciente fenómeno de la seguridad informática implícita en este tipo de plataforma tecnológica, esto mediante la indagación del contenido de la virtualización tecnológica y el estudio de cómo se comporta la seguridad informática alrededor de este tipo de infraestructura.

Sin embargo, al ser un tema que viene incursionando y desarrollándose continuamente en las distintas compañías de nuestra sociedad, parece ser que se están dejando de lado algunos factores claves de seguridad informática, lo cual es la proyección y fundamento para este trabajo escrito. Si bien existen diversos métodos de seguridad informática aplicados a la infraestructura, algunos de estos corresponden a recomendaciones de cada fabricante, o en otros casos son pautas empíricas heredadas de las anteriores formas de virtualización de equipos computacionales.

Por lo anterior, es que el presente texto pretende evidenciar aspectos generales tanto de los antecedentes así como de la realidad actual en virtualización, esto para entregar posteriormente una serie de claves a considerar en esta materia, logrando que desde la bibliografía existente del tema y sumado a la experiencia profesional del autor, se pueda reorganizar de una manera más crítica y profesional el fondo referente a la seguridad informática alrededor de esta tecnología, permitiendo llegar a conclusiones útiles para la posterior gestión de la seguridad informática en este campo de estudio en auge.

Objetivo general

El objetivo general de esta propuesta consiste en evidenciar la realidad de la seguridad informática en infraestructuras tecnológicas virtuales convergentes y servicios en la nube.

Objetivos específicos:

Determinar los principales aspectos que dieron origen a la infraestructura tecnológica virtual convergente y servicios en la nube.

Establecer los principales procesos y componentes que sustentan el esquema moderno de infraestructura convergente, hiperconvergente y servicios en la nube.

Comprender la seguridad informática de la infraestructura convergente, hiperconvergente y servicios en la nube implementados en organizaciones actuales.

Alcance

El alcance de este documento es analizar el antecedente que origina a la tecnología de virtualización, establecer los procesos de actualidad en esta temática siempre dentro del esquema moderno de infraestructura convergente, hiperconvergente y servicios en la nube, para finalmente obtener conclusiones de la seguridad informática que acontece alrededor de estos equipos y servicios implementados en las organizaciones actuales.

Metodología:

Para lograr la propuesta del presente documento, se trabajó en una primera etapa de indagación y selección de fuentes bibliográficas, que cubrieran aspectos relacionados al antecedente histórico de la virtualización tecnológica, etapa histórica experimental, evolución de esta tecnología a la producción empresarial, y en una segunda etapa se analizan las áreas y componentes propios del tema, en concordancia con la bibliografía que sustenta el tema de estudio. Finalmente se desarrolla el contenido del documento para poder llegar a plasmar los hallazgos y realidades del fenómeno de la seguridad informática entorno a la infraestructura tecnológica virtual en la actualidad, obteniendo conclusiones importantes para su comprensión.

Capítulo 1: Origen y evolución de la infraestructura tecnológica virtual y los servicios en la nube.

Nuestra sociedad se interrelaciona constantemente con el mundo tecnológico, y claro está que ese entorno informático es soportado por importantes recursos virtuales, pero muchas veces desconocemos cual fue el motivo u origen de este tipo de tecnología y su desarrollo hasta la actualidad, por lo que el presente capítulo constituye un breve repaso de la infraestructura tecnológica virtual, así como su origen y adaptación en el tiempo hasta nuestros días.

1.1 Inicio de la virtualización

Para comprender la tecnología de virtualización moderna es necesario volver la mirada a su primera etapa en la década de 1960, cuando dominaban los enormes equipos de cómputo, los cuales eran económicamente costosos de adquirir y mantener, básicamente se utilizaban a nivel empresarial en funciones muy específicas, y esto representó el dominio de la computación centralizada mediante el concepto de *Mainframes*[1].

El primer equipo relacionado a la virtualización en aparecer en escena fue la computadora System/360 del fabricante IBM, lanzada en abril de 1964, podía llegar a fabricarse hasta con dos procesadores y 2 megabytes de memoria RAM (poder computacional impensable para su época, pero ínfimos si se compara al poder computacional de un celular de gama baja hoy día), la cual con el sistema operativo CP/CMS y su versión CP-40 /CMS permitió definir la arquitectura de máquina virtual, incluso utilizado hasta la década de 1970, permitía asignar a los usuarios una porción de procesamiento de manera que tuviese un System/360 virtual independiente para su labor. Pero el contexto descrito para esa época (principalmente costo y tamaño) impidió que la virtualización se desarrollará, y solamente representó un esfuerzo experimental, sin auge, finalmente fue puesto en el olvido por algunos años.

[1] En castellano Unidades Centrales, consiste en computadoras potentes, costosas, y de gran tamaño, de uso empresarial para el procesamiento de gran cantidad de datos.

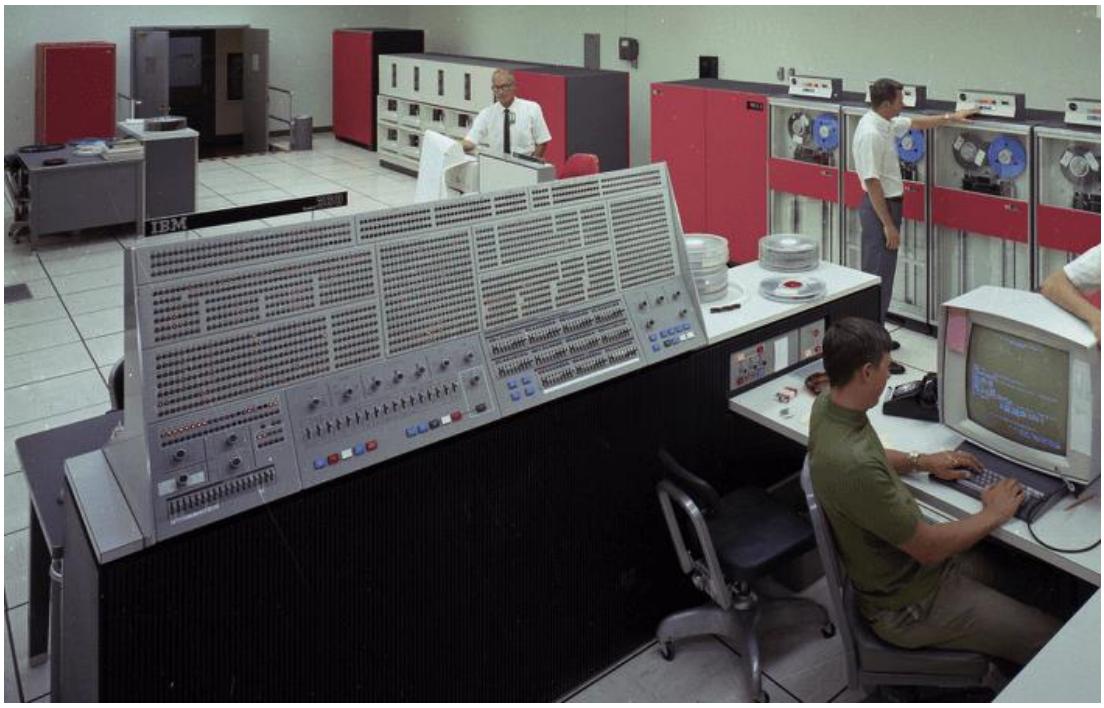

Ilustración 1 Computadora IBM System/360, primer equipo en ser utilizado para virtualización en la década de 1960.

Fuente: http://www.righto.com/2019/04/iconic-consoles-of-ibm-system360.html [1]

1.2 Evolución de la virtualización

El continuo avance tecnológico que se generó en las décadas posteriores hizo que el objetivo tecnológico se centrará en desarrollar computadores más pequeños en capacidad de procesamiento y tamaño, pero que además se consiguieran más económicas, ampliando el mercado y utilizando sistemas operativos abiertos, por lo que el uso de las computadoras ya no solo era un interés empresarial, sino que empezó a darse la utilización de los primeros computadores personales con interfaces gráficas más amigables al usuario, lo cual generó la necesidad de interconectar distintos sectores de la sociedad, aumentó el uso de Internet y finalmente demandó nuevos y diversos servicios tecnológicos.

Lo anterior propicio para fines de la década de 1990 un contexto tecnológico basado en el procesamiento distribuido de la información, y esto a su vez generó dos aspectos fundamentales que darían un nuevo impulso a la virtualización: en primera instancia se debía resolver la gran y creciente complejidad administrativa que demandaba la implementación y mantenimiento de estos equipos, y por otra parte se debía revisar la

subutilización que se daba con estos costosos recursos tecnológicos. Cada equipo requería una atención operativa particular, y además en muchas ocasiones su objetivo o función era brindar un servicio para el cual estaba sobredimensionado en recursos.

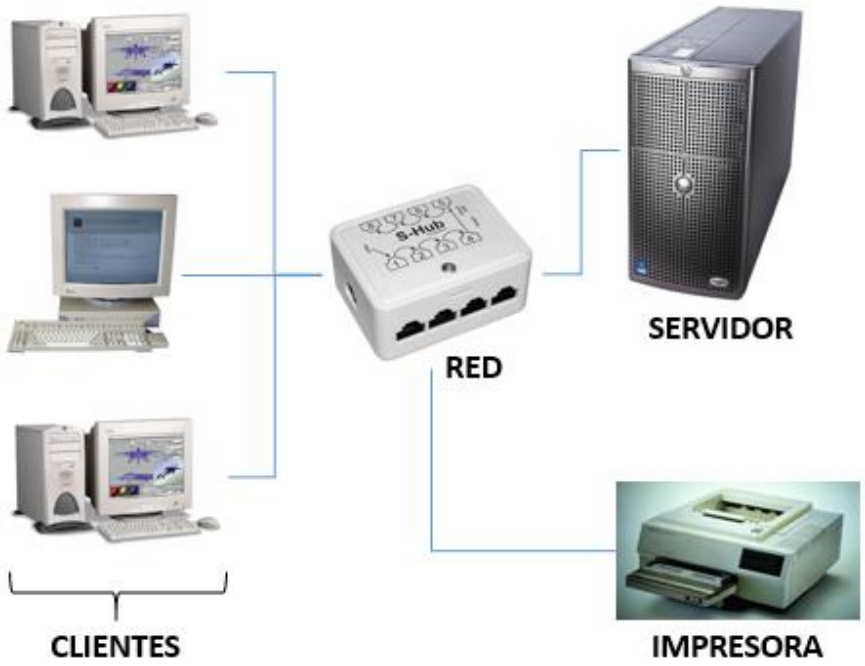

Ilustración 2: Esquema básico de procesamiento distribuido ampliamente utilizado desde la década del 2000, esquema cliente-servidor soportado en una red de computadores.

Fuente: Elaboración propia.

Es entonces que para 1998 la empresa tecnológica VMWare presentó la patente denominada **Sistema y método para la virtualización de sistemas de cómputo**, dicha patente se fundamentaba en poder utilizar una arquitectura para virtualización de equipos sobre una plataforma física de cómputo x86 [2], fue llevada a cabo en el año 1999 con la solución **VMWare Workstation**, la cual consistía en un software capaz de crear equipos virtuales, y permitía que estos utilicen los recursos y periféricos de un anfitrión con sistema operativo Windows, Linux, o Mac. En los primeros años esta solución de VMWare se posicionó como una herramienta para desarrollo y pruebas, pero marcó un hito que revolucionaría la tecnología virtual rápidamente.

[2] Se llama x86 a la compatibilidad de microprocesadores con arquitecturas Intel e IBM.

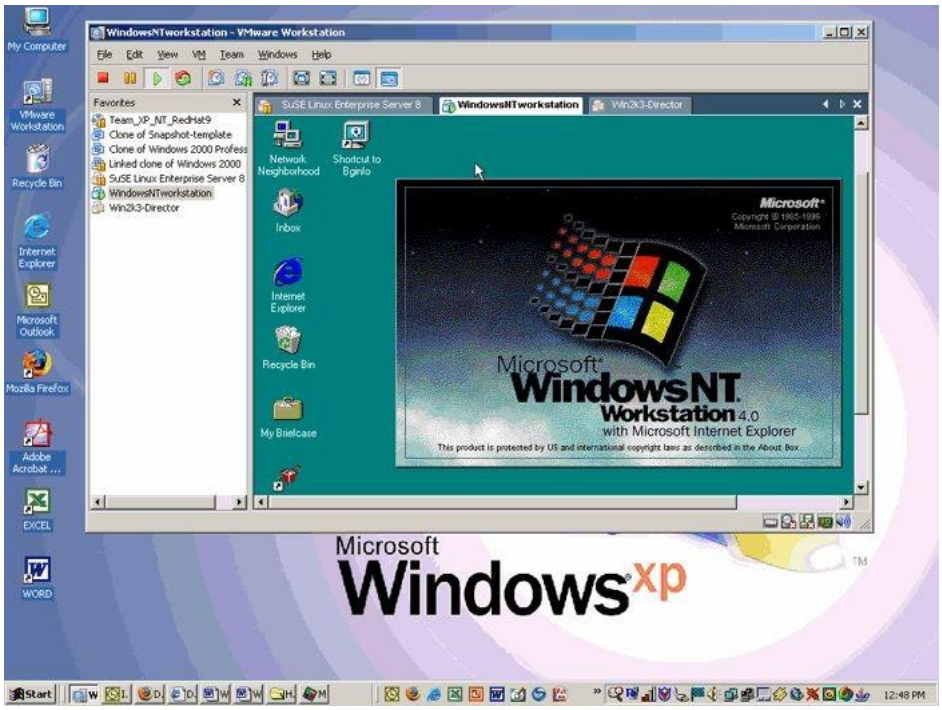

Ilustración 3: VMWare Workstation, software sobre sistema operativo Windows XP, emulando otro sistema Windows Server NT, ambos funcionales y compartiendo recursos de un mismo equipo físico.

Fuente: http://grabii.blogspot.com/2010/02/vmware-workstation-7-virtual-machine.html [2]

1.3 El hipervisor y la Infraestructura Virtual

Para el año 2006 VMWare avanzó en su producto y lanza el concepto de *Virtual Infrastructure*[3] de manera que introduce el concepto de **hipervisor**, lo cual marca el inicio de lo que actualmente se llama **Infraestructura Virtual**. Entonces como lo definen “Marchionni y Formoso [3] el llamado hipervisor es un componente de software que permite que varios sistemas operativos puedan acceder a un equipo en forma concurrente, como si cada uno de ellos fuera el dueño coordinando el acceso y uso de sus recursos”. Este punto en la historia de la virtualización representó un antes y un después de lo que conocemos, porque desde el procesamiento centralizado hasta el esquema de procesamiento distribuido a finales de siglo, ocurrió una evolución del hardware, pero es hasta que se da esta concepción del hipervisor que se marca un hito fundamental que desencadenó un acelerado desarrollo del cómputo virtual hasta nuestros días.

[3] Traducido como Infraestructura Virtual, permite que varios sistemas virtuales funcionen eficientemente sobre un mismo equipo físico, optimiza recurso y mejora costos.

Ilustración 4: Introducción del hipervisor como orquestador de la virtualización, dando origen al concepto de infraestructura virtual.

Fuente: Elaboración propia.

1.4 Virtualización y procesamiento en la nube tecnológica

Para la década del año 2010 rápidamente se consolidó la infraestructura virtual, pasó a ser algo más que un tema técnico de la informática y sus costos operativos adjuntos, sino que “Marchionni y Formoso [3] mencionan como La infraestructura pasa de ser un costo asociado a los requerimientos del negocio a ser un centro de recursos optimizados para asegurar un nivel de servicio sustentable. El próximo paso nos muestra la manera de transformar la infraestructura como un servicio para el negocio, que puede ser automatizado para que la empresa y sus necesidades puedan abastecerse de él”, es así como podemos ver el cómo se concibe un nuevo concepto en el mundo de la virtualización hasta nuestros días, esto es el procesamiento en la nube.

Claro está que vivimos en la era de los servicios en la nube, lo cual como bien lo describen “Marchionni y Formoso [3] La nube (cloud) no es un producto o una herramienta, ni siquiera una solución, es un concepto que engloba muchos componentes y solo algunos son software y hardware, y hasta talvez sean los menos importantes. Este concepto está asociado a la transformación del centro de datos. Permite que toda la infraestructura más las aplicaciones de una empresa funcionen como un servicio”, el cual consumimos sin necesidad de ser experto en temas técnicos, lo obviamos como al servicio de electrificación o agua de nuestro domicilio, por los cuales

pagamos y consumimos en un período determinado y con las condiciones acordadas con el proveedor, incluso algunos de manera gratuita.

Ilustración 5: Abstracción de la concepción de la nube informática como servicios tecnológicos al alcance del usuario y accedidos a través de Internet.

Fuente: https://www.areatecnologia.com [4]

1.5 La noción actual de la virtualización

El fundamento histórico del concepto sumado a la realidad de nuestros días nos brinda una percepción de lo que es la virtualización, pero resulta importante considerar algunas definiciones, como las dadas por los actuales fabricantes líderes en esta tecnología.

Como concepto base, el fabricante VMWare indica en su sitio en Internet que

> La virtualización es el proceso de crear una representación basada en software (o virtual), en lugar de una física. La virtualización se puede aplicar a servidores, aplicaciones, almacenamiento y redes, y es la manera más eficaz de reducir los costos de TI y aumentar la eficiencia y la agilidad de los negocios de cualquier tamaño [5].

Por su parte el reconocido desarrollador de tecnología Microsoft expresa sobre la virtualización lo siguiente:

> Permite a las organizaciones particionar un equipo o servidor físico en varias máquinas virtuales. Cada máquina virtual puede interactuar de forma independiente y ejecutar sistemas operativos o aplicaciones

> diferentes mientras comparten los recursos de una sola máquina host. Al crear varios recursos a partir de un único equipo o servidor, la virtualización mejora la escalabilidad y las cargas de trabajo, al tiempo que permite usar menos servidores y reducir el consumo de energía, los costos de infraestructura y el mantenimiento [6].

Así mismo la notoria empresa tecnológica Red Hat adopta el concepto y además recalca que:

> El software llamado hipervisor se conecta directamente con el hardware y permite dividir un sistema en entornos separados, distintos y seguros, conocidos como máquinas virtuales (VM). Estas VM dependen de la capacidad del hipervisor de separar los recursos de la máquina del hardware y distribuirlos adecuadamente [7]

De las definiciones anteriores queda claro que la virtualización en esencia es utilizar software para representar o simular hardware en un entorno no físico, pero la alta demanda de esta forma de implementar infraestructura tecnológica en las organizaciones, han incentivado que los fabricantes caractericen a la virtualización con otros aspectos relacionados a las ventajas esperadas para el negocio y sus necesidades, como costos, eficiencia, escalabilidad, entre otros, provocando además que se concentren cuatro categorías como lo son la virtualización del escritorio, la red, aplicaciones y almacenamiento. El uso que se le da a las cuatro categorías, y las distintas combinaciones entre estas, genera la base para crear infraestructuras virtuales empresariales, robustas y convergentes.

Ahora bien, después de discurrir por la historia y alcanzar el concepto moderno de virtualización, surgen algunas interrogantes como: ¿Cuánto evolucionó la tecnología virtual en la última década? ¿Qué conceptos y tecnologías se acuñaron? ¿Por qué se volvió tan importante la virtualización para el mundo tecnológico globalizado en que vivimos? ¿Qué papel desempeñan las redes en todo esto? ¿Qué sucede con nuestra información? y principalmente ¿En qué punto la seguridad informática se convirtió en tema de interés para todo esto? Son las incógnitas que nos invitan a meditar si realmente la seguridad informática se contempló durante el desarrollo histórico de la infraestructura virtual o si debemos indagar la situación actual

debido a que desconocemos ciertos aspectos claves que afectan el entorno en el que vivimos.

Si bien este capítulo constituye un breve repaso histórico del como la virtualización avanzó diversas etapas para llegar a lo que hoy día es, aún resulta necesario profundizar los más recientes aspectos técnicos que nos permitan comprender lo que es la infraestructura virtual que soporta la mayoría de plataformas tecnológicas alrededor del mundo, y es por eso que el próximo capítulo se centrará en revisar aspecto técnicos generales, modelos y tipos de virtualización que dominan las plataformas tecnológicas modernas, con el fin de obtener un panorama completo del área de estudio que motiva este trabajo.

Capítulo 2: Infraestructura convergente, hiperconvergente y servicios en la nube

Nuestra realidad tecnológica se fundamenta en un mundo interconectado que es soportado por servicios en la nube informática, esto lo observamos en cada momento que accedemos a nuestro correo electrónico, o visitamos una página web, hasta la forma en que almacenamos nuestro trabajo diario en un medio colaborativo en la Internet, todo eso y mucho más lo hacemos accediendo desde nuestro teléfono celular o computadora portátil, y en la mayoría de los casos ni siquiera nos percatamos en donde se almacenan los datos, de donde viene la información que consultamos, o que tan seguras sean nuestras acciones en este universo digital.

Como se señaló previamente, la nube tecnológica representa un servicio que consumimos sin importar los detalles técnicos que la originan, sin embargo, detrás de este tipo de plataformas existe todo un ecosistema tecnológico complejo que se entrelaza mediante diversos equipos físicos, virtuales, software, normas técnicas y toda una serie de componentes que finalmente nos entregan un servicio veraz para nuestras labores personales o profesionales.

El presente capítulo reúne conceptos principales relacionados a componentes de la infraestructura virtual más utilizada en las organizaciones modernas, sus características primordiales, esto con el fin de llegar a comprender los conceptos de convergencia y servicios en la nube, que servirán de base para profundizar en el tema de la seguridad informática que los envuelve, esto en los consecuentes capítulos.

2.1 Componentes de la virtualización

Si bien existen diversos y complejos conceptos que conforman las plataformas tecnológicas físicas y virtuales, con características técnicas, funcionales, o incluso propias del negocio, a continuación, se detallan de una manera práctica los conceptos claves que nos servirán para comprender la naturaleza de la infraestructura virtual utilizada en propósitos generales de una organización:

2.1.1 Máquina Virtual

Como se mencionó anteriormente, fue la empresa VMWare quién acuño hace más de una década y media el término de infraestructura virtual, lo que desencadenó un amplio desarrollo en software para crear y utilizar lo que actualmente llamamos máquina virtual o comúnmente abreviado a VM por sus siglas en inglés (Virtual Machine), consiste en “un contenedor de software bien aislado que incluye un sistema operativo y una aplicación. Cada máquina virtual autónoma es completamente independiente. Si se instalan varias máquinas virtuales en un mismo ordenador, es posible ejecutar varios sistemas operativos y aplicaciones en un solo servidor físico o host [5]”. En poco tiempo el concepto fue ampliamente utilizado por otros fabricantes de software para generar plataformas similares que pudiesen emular diversos sistemas operativos en máquinas virtuales sobre hardware de arquitectura x86, ampliamente utilizados en nuestros días.

En la industria tecnológica actual existe software disponible para que los usuarios con conocimientos básicos en informática puedan experimentar con este tipo de tecnología, sin embargo, en el segmento empresarial existe una constante actualización en este tipo de software con el fin de adaptar los equipos virtuales a las nuevas exigencias del mercado, buscando adaptar el medio virtual a la realidad física del equipo anfitrión, optimizando recursos y ampliando capacidades, principalmente en compatibilidad con dispositivos periféricos recientes, por ejemplo simular nuevas versiones de puerto USB, o nuevos estándares en protocolos de red, entre otros.

Por lo anterior es que la máquina virtual se presenta como uno de los componentes más fundamentales del engranaje operativo de la infraestructura virtual, es donde las aplicaciones procesan, acceden al almacenamiento, e interactúan en red, de manera que se comportan en idénticas condiciones a un equipo físico con procesador, memoria RAM, disco duro, tarjeta de red y las características necesarias para proveer los servicios propios de un computador convencional.

2.1.2 Almacenamiento virtual

Otro componente fundamental de la virtualización, y quizás el más crucial para muchas organizaciones, es el almacenamiento, el cual en primera

instancia es el espacio en discos físicos donde se almacenarán las máquinas virtuales y los datos necesarios para el funcionamiento correcto de las mismas, pero en el detalle de su configuración se muestra como el medio de almacenamiento en red o disco duro de la máquina virtual, accedido virtual o físicamente por un subsistema de almacenamiento y protocolos como NFS, CIFS, SMB, iSCSI, Fibre Channel (FC), FCoE, u otros que no se profundizarán en este texto por la amplitud técnica y su estrecha relación a la necesidad de cada empresa, pero para efectos generales de este documento son protocolos que permiten a las máquinas virtuales y a otros equipos del entorno acceder al almacenamiento en un formato compatible y eficiente, incluso de manera simultánea en algunos casos.

Si bien la selección y configuración del almacenamiento más adecuado siempre resulta particular para la necesidad de cada organización, el punto relevante a trabajar es la centralización del mismo, específicamente en la capacidad de tener una plataforma de almacenamiento versátil, que alcance los aspectos técnicos suficientes para lograr solventar la necesidad del negocio, como: velocidad, acceso físico y geográfico, tamaño del almacenamiento, escalabilidad, capacidad de recuperación ante fallos, funciones de acceso, escritura y lectura a los datos en simultaneó.

También es relevante considerar que las plataformas virtuales admiten la posibilidad de utilizar almacenamiento descentralizado utilizando los discos duros físicos de los equipos anfitriones, esto es una práctica más común en ambientes experimentales o de pruebas y desarrollo, contrario a la realidad de la infraestructura virtual que centra gran parte de su éxito en un eficiente almacenamiento centralizado.

2.1.3 Servidores virtuales y procesamiento

En cuanto al aspecto del procesamiento, este concepto está estrechamente ligado al equipo servidor, que en su concepto más fundamental es un software aplicativo que responde a una o más peticiones de otro software cliente (solicitud web, consulta a una base de datos, petitoria DHCP, DNS, descargar o subir archivos, por considerar algunos ejemplos de uso frecuente), pero en términos de infraestructura también se suele acuñar el concepto de servidor a la combinación del equipo físico que realiza

procesamiento computacional y al software o aplicación alojado en él para brindar el servicio.

Por lo anterior, es que las máquinas virtuales toman relevancia en cuanto a función de servidor, pues existen equipos físicos robustos fabricados con características de seguridad y rendimiento específico para procesar peticiones a nivel empresarial (como servir 24 horas, altas prestaciones de CPU y memoria RAM, rápida escritura y lectura en disco, desempeño eficiente de red y recursos en general, entre otros), pero bajo un esquema de procesamiento distribuido, se elevan costos y genera subutilización de espacio físico, energía y recursos en segundo plano, u otras consideraciones propias de la regla del negocio. Entonces el uso de múltiples máquinas virtuales que se puedan crear sobre un servidor físico o un arreglo de varios de ellos, permiten tener una plataforma de servidores virtuales que finalmente pueden brindar múltiples servicios a numerosos clientes, de forma que un equipo físico pasa a ser una plataforma de hardware eficiente y la máquina virtual toma el rol de servidor para atender las consultas.

2.1.4 Sistemas Operativos

En cuanto al software que consume los recursos de un equipo de cómputo, sin importar si es hardware físico o una máquina virtual, este se aprovisiona con características específicas que dan sentido a la función o rol del dispositivo, lo cual para efectos del tema abordado lo podemos ver como el sistema operativo para servidor o para cliente, donde el primero incluye funciones para recibir peticiones, optimizar recursos para sus funciones internas computacionales, y brindar respuestas optimas al cliente que origina las consultas, mientras que el segundo se puede mostrar como un sistema operativo con funciones óptimas para la experiencia del usuario final que utiliza un computador o quizás otro equipo servidor pero que en este caso genera las peticiones.

La evolución histórica y la variedad de los sistemas operativos es amplia, soportados por diversos fabricantes y para distintos objetivos funcionales, pero en su mayoría las versiones más actuales son compatibles con su implementación en infraestructura virtual, principalmente las versiones para equipos dedicados a ofrecer transacciones como servidor.

Tabla 1 Estadísticas de sistemas operativos más utilizados en el 2018 como cliente y sus fabricantes.

Sistema Operativo	Porcentaje de utilización global	Fabricante
Android	36.5%	Google Inc.
Windows	35.99%	Microsoft Corporation.
iOS	13.99%	Apple Inc.
OS X	6.37%	Apple Inc.
Unknown	4.78%	NA
Linux	0.79%	Comunidad Open Source.

Fuente: Elaboración propia con información obtenida de http://gs.statcounter.com

La tabla anterior nos muestra la preferencia de sistemas operativos utilizados por los usuarios durante el año 2018, esto principalmente para funciones tipo cliente/usuario final. Se observa una preferencia por los sistemas móviles actuales.

Tabla 2 Estadísticas de sistemas operativos más utilizados en el 2017 como servidor y sus fabricantes.

Sistema Operativo	Porcentaje de utilización global	Fabricante
Unix / Linux	69.4%	Comunidad Open Source Red Hat Enterprise (Privativo) Otros.
Windows	30.6%	Microsoft Corporation.
Mac OS	0.1%	Apple Inc.

Fuente: Elaboración propia con información obtenida de https://w3techs.com

Por otra parte, la tabla anterior nos muestra la preferencia de sistemas operativos utilizados por las organizaciones en el año 2017, esto para funciones tipo servidor, en procesos empresariales.

2.1.5 Red virtual

Como es común en el campo de la informática moderna, un computador necesita estar conectado a una red para ser realmente funcional, comúnmente responde a una red empresarial privada o en otros casos a una red pública como Internet, de manera que el equipo realiza un gran número de transacciones a través de los dispositivos de comunicación.

Cuando a la red física le agregamos la propiedad de ser virtual, la esencia funcional de red se mantiene, pero las características cambian, las redes virtuales “son independientes del medio físico [8]”. Lo anterior nos ilustra una característica fundamental, pues si tomamos como referencia a las redes virtuales de uso común en el ambiente empresarial como lo son VLAN y VPN, indiferentemente de su objetivo funcional, podemos abstraer que son medios lógicos que funcionan sobre una plataforma física, pero sin embargo dentro de una infraestructura virtual funcionan de manera transparente para la comunicación entre los equipos de la misma red.

Aunque en términos generales la VLAN (Virtual LAN) constituye una red lógica que comparte un medio físico, o en el caso de la VPN (Red Privada Virtual) que se encarga de extender una red privada sobre una red pública no segura como la Internet, ambos ejemplos son variantes que surgieron como respuesta a necesidades que el medio físico no brindaba nativamente en su momento, pero es hasta que se concibió la infraestructura virtual que se obtiene la virtualización completa de la red en un ambiente de este tipo, pues al crear las máquinas virtuales se les provee uno o varios dispositivos adaptadores de red totalmente virtuales (vNIC), con idénticas características funcionales a las de un adaptador físico (NIC), pero basado en software (fiel al concepto de virtualización mencionado previamente), capaz de trabajar de manera transparente con el sistema operativo en el equipo virtual y con los demás dispositivos físicos o virtuales en la red, manteniendo la compatibilidad en la configuración de red conocida.

2.1.6 Lógica de intercambio, aplicaciones y servicios asociados

Teniendo en combinación el hardware adecuado, compatible con características de virtualización de la red, el almacenamiento y sistemas operativos, se obtiene una base sólida para crear una infraestructura virtual, pero esto cobra relevancia solo cuando se implementé una solución que incluya un hipervisor adecuado, que le ofrezca robustez y eficiencia, convirtiéndose en el software orquestador de la plataforma virtual.

La importancia del hipervisor radica en que debe detectar “las aplicaciones de manera inherente. Tiene una línea de visión directa a cada aplicación que se ejecuta en las VM que están conectadas al servidor del host.

Comprende los requisitos de almacenamiento de la aplicación [9]”de manera que trabaja entre las necesidades de las aplicaciones y el hardware o recurso físico disponible, posicionándose en medio del entorno físico y el virtual, creando el flujo o lógica de intercambio entre ambos, “coordinado los datos de E/S entre el servidor del host y las VM albergadas, y administra la infraestructura de almacenamiento subyacente. Esta posición cubierta permite al hipervisor convertir recursos físicos sólidos como la piedra en grupos fluidos de capacidad de almacenamiento y capacidades que pueden fluir a las aplicaciones según sea necesario [9].”

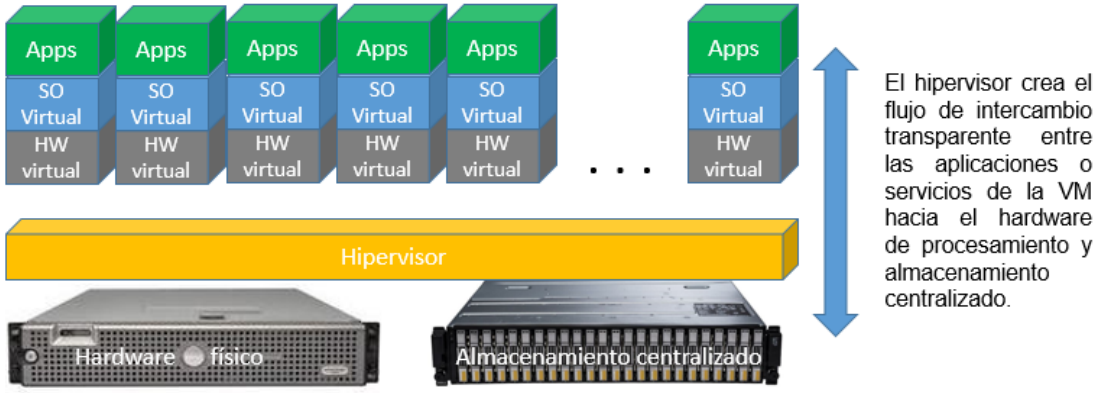

Ilustración 6: El hipervisor permite el intercambio entre aplicaciones y hardware, produciendo infraestructura virtual.

Fuente: Elaboración propia

Mediante la lógica de intercambio descrito, se logra el proceso fundamental de amalgamar los componentes necesarios para concebir infraestructura virtual, al punto que las propias aplicaciones virtuales que brindan servicios de usuario final, son capaces de solicitar o recurrir a los recursos de hardware de manera transparente en su funcionamiento.

Es destacable mencionar que el hipervisor funciona nativamente como sistema operativo sobre el hardware (intercambio directo con el equipo físico), aunque existen versiones desarrolladas para trabajar indirectamente como un servicio instalado en un sistema operativo más tradicional (intercambio de hipervisor con el sistema operativo anfitrión y este último interactúa con el hardware), lo cual puede generar diferencias considerables de administración y rendimiento.

2.1.7 Virtualización del escritorio

Si representamos la infraestructura virtual como una estructura de capas superiores e inferiores, tendríamos que poner en la base al hardware como la primera capa, y en la cima al equipo o máquina virtual como la capa más alta que contiene a las aplicaciones e interactúa con el usuario o cliente.

Esa necesidad de interacción con el cliente o servicio, ha generado que se utilice ampliamente la virtualización del escritorio, conocida también como virtualización del desktop o VDI por sus siglas en inglés (Virtual Desktop Infraestructure), con la capacidad de proveer sesiones de trabajo virtuales y remotas.

Este tipo de tecnología, normalmente de ámbito empresarial, “permite a cada usuario final tener su propia sesión de trabajo sin la necesidad de un ordenador de sobremesa dedicado para cada usuario, virtualizando la sesión y compartiendo un equipo host. Dependiendo de la configuración, un simple equipo de tipo PC puede servir decenas de usuarios simultáneos y un servidor potente hasta cientos de usuarios [10]”.

Aunque las máquinas virtuales posibilitan que un cliente acceda a sus servicios de manera remota, por ejemplo, por red a través de un protocolo o aplicación para tal fin, la característica principal de VDI radica en ir más allá de esa funcionalidad, de manera que un mismo equipo físico o virtual podrá crear múltiples sesiones de trabajo remotas, ampliando así las capacidades de la infraestructura virtual.

Como es presumible, el uso de este tipo de tecnologías tiene una serie de beneficios para las organizaciones modernas que se exponen muchas veces a un ágil entorno operativo formado por redes privadas y públicas, pero también abre un potencial abanico de obstáculos en seguridad informática, los cuales ineludiblemente se deben asumir y resolver dentro de las compañías.

2.1.8 Entorno operativo y gestión de la infraestructura virtual

Teniendo en consideración los componentes descritos de la infraestructura virtual, lo que procede es establecer las características primordiales del entorno donde se alojará.

Actualmente las tecnologías de información constituyen un departamento clave en la organización, con el recurso humano debidamente

capacitado para su gestión, normalmente conforman el departamento de Tecnología de la Información (TI), y es habitual que la infraestructura física la concentren en uno o varios Centros de Datos propios o contratados a terceros, y ubicados en los propios inmuebles o en una ubicación geográfica remota.

Lo anterior ha generado como consecuencia que las redes jueguen un papel fundamental de interconectar la infraestructura tecnológica de manera transparente para su operación, y aún más importante, el almacenamiento debe ser centralizado, para poder tener la información en tiempo real, confiable, y modificable, lo que representa todo un reto para los fabricantes de equipo de almacenamiento que deben perseguir disponibilidad, pero además integridad y confidencialidad.

Particularmente “Para que la infraestructura virtual sea eficiente, altamente disponible y segura, debe contar con al menos un storage de discos en donde se almacenen y se ejecuten las máquinas virtuales [3]”, lo que hace aún más valioso implementar correctamente el almacenamiento centralizado para las exigencias empresariales actuales. También cabe mencionar que actualmente algunas soluciones admiten la redundancia de datos incluso a nivel geográfico, lo cual en términos generales es tener una infraestructura de almacenamiento alterna sincronizada con la que está en producción, en caso de algún inconveniente o falló de una, entra a trabajar la otra.

El consumo de recursos es un tema que décadas atrás representaba un costo considerable a la organización, además del almacenamiento, era importante ver costos de adquirir unidades físicas de servidores, equipos de red, y todo en conjunto representaba un gasto energético y de espacio inevitablemente. Una práctica común consistía en “utilizar un servidor físico por cada aplicación o servicio [3]”, lo que provocaba un deficiente uso de recursos en procesador, memoria, almacenamiento, energía, por mencionar algunos, ”al punto de no llegar en la mayoría de los casos al 10 por ciento (10%) de uso e incluso menos [3]”, y en la actualidad esto se vino a resolver considerablemente con la virtualización de la infraestructura, pues en un mismo equipo físico se pueden crear múltiples máquinas virtuales o incluso varias sesiones en una misma máquina para el caso de virtualización de escritorios, pudiendo calendarizar y consumir recursos en horas de alta demanda y apagando equipos o deteniendo servicios durante baja demanda.

De la misma forma, con el control de la infraestructura virtual, el mantenimiento de la misma cambió, debido a que se reduce el costo en mantenimiento preventivo y correctivo del hardware, se dan menos puntos físicos de falla, baja la demanda de repuestos, y al haber una virtualización de la red disminuye también la adquisición de los dispositivos físicos de comunicación. El centro de datos de las empresas claramente disminuyó el espacio físico ocupado, concentra sus servicios en equipos virtuales, y genera menos consumo de energía y refrigeración. Pero esto desencadenó un efecto sobre la gestión de la tecnología tradicional, pasando de un paradigma donde forzosamente el hardware solo se implementaba en espacio físico dentro de la empresa y en su red privada, a un modelo donde se puede migrar la infraestructura a un entorno virtual, incluso llevándolo a terceros por conveniencia del negocio. Esta implementación virtual además de dar ventajas sobre el hardware físico como las descritas, tiene la particularidad de cambiar la forma en que se adquiere el licenciamiento de equipos y software, brindando versatilidad al instalar, actualizar o dar de baja equipos y servicios.

Otra característica relevante que surge en un entorno virtual es la capacidad de implementar infraestructura y servicios, eliminando tiempos de requerimiento y adquisición de hardware (semanas o meses), al punto que en menos de una hora se puede crear y colocar en funcionamiento pleno una máquina virtual como servidor, por dar un ejemplo usual.

En cuanto a las bondades de poder centralizar el almacenamiento y crear infraestructura de contingencia, está la facilidad de hacer respaldos y recuperación de los mismos, pudiéndose respaldar cada equipo virtual y recuperarlo completamente ante alguna falla o desastre, o también obtener algún dato especifico respaldado en un medio centralizado. Pero con la posibilidad de que uno o varios servidores físicos puedan trabajar en arreglo o *cluster*[4], también se minimiza el impacto ante inconvenientes, de manera que un equipo puede tomar la carga operativa ante la imposibilidad de algún otro miembro del arreglo, y así no alterar la operación, la cual incluso puede migrarse en tiempo real a otro entorno virtual en un punto geográfico diferente.

[4] Cluster, traducido al castellano como agrupar, es un término usado para describir la agrupación de componentes con similares características que funcionan como uno solo, por ejemplo, un arreglo de discos duros, o un arreglo de servidores.

La característica de poder crear arreglos de equipos físicos también nos traslada al surgimiento de otra funcionalidad de la infraestructura virtual, y consiste en la capacidad de escalar, esto en tiempo real, permitiendo que se pueda agregar más poder de hardware físico a la infraestructura, sumándole o ampliándole los recursos, y además permite agregar de igual forma hardware virtual a las maquinas o servidores que componen el entorno virtual. Como es previsible, este esquema de infraestructura virtual respecto a la tradicional conlleva cambios, ”la administración de las aplicaciones es común a ambas infraestructuras [3]”, manteniendo la gestión habitual de las aplicaciones o servicios, pero en el caso de la virtualización, se avoca a administrar y monitorear principalmente al hardware virtual, su comportamiento, consumo de recursos, y en cierta medida la importancia radica en gestionar correctamente la plataforma de virtualización y su hipervisor, incluyendo sus aspectos de seguridad o vulnerabilidad.

Si bien el entorno operativo de una infraestructura virtual es soportado por equipos físicos, estos son adaptados para ser unidades al servicio de la solución virtual y su hipervisor, pudiendo ser reemplazados o escalables en cualquier momento, mientras que la infraestructura virtual se comporta de manera independiente en términos de la operación, logrando mínimos tiempos de parada del servicio por cambios en hardware físico o virtual, sin afectar la producción de la empresa, esto en el escenario ideal de una correcta implementación con los recursos adecuados.

2.2 Infraestructura tradicional, convergente e hiperconvergente

Hasta este punto, se han descrito diferentes conceptos y características de infraestructura tradicional y su variante virtual, sin embargo, recientemente se ha posicionado fuertemente el concepto de convergencia y su versión evolutiva de hiperconvergencia. Para comprender esta confluencia de conceptos o variantes, podemos definir lo siguiente:

Infraestructura tecnológica tradicional: en términos informáticos es “el hardware de propiedad exclusiva diseñado para un fin específico para el almacenamiento y las redes. Estos componentes forman silos separados con su propio software de administración adquirido de varios proveedores. Funcionan mejor cuando especialistas dedicados los optimizan y administran

[9]", por lo que una desventaja usual es que se incurra en una excesiva adquisición de componentes difíciles de optimizar.

Infraestructura tecnológica convergente: por su parte "Una infraestructura convergente mejora el modelo tradicional mediante la incorporación del procesamiento, el almacenamiento, la administración y las redes en un solo rack [9]" o gabinete dentro del centro de datos, brindando mejoras de administración general, principalmente a nivel de hardware, todo esto en el ámbito de componentes físicos y el software primordial de administración en ellos. El defecto en este modelo es que "los paquetes de hardware se preconfiguran para ejecutar cargas de trabajo específicas y estos no pueden alterarse fácilmente, lo que genera una pérdida de flexibilidad. Los límites físicos podrán haberse eliminado, pero los obstáculos operativos y de aprovisionamiento permanecen [9]".

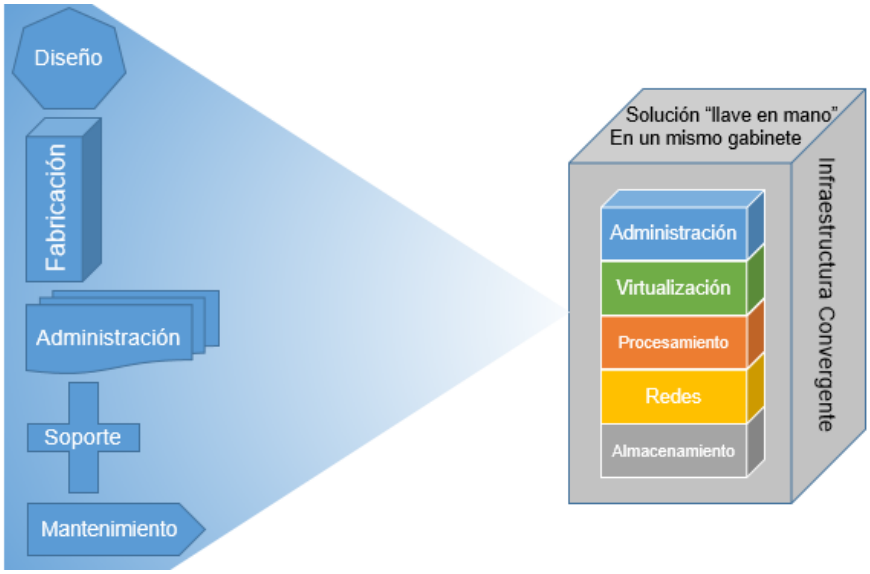

Ilustración 7: Infraestructura convergente, facilita la adquisición de la plataforma como si fuese un solo equipo, se trabaja más fácil con el proveedor del mismo, pero mantiene el formato operativo tradicional

Infraestructura tecnológica hiperconvergente: ante la necesidad de una mejor gestión en la convergencia de equipos, "La infraestructura hiperconvergente (HCI) converge los silos de infraestructura de TI tradicional en servidores estándar de la industria y virtualiza la infraestructura física. Originalmente, la HCI incluía solo el procesamiento y el almacenamiento virtuales, pero ahora puede extenderse con soluciones de red totalmente virtualizadas obteniendo un centro de datos definido por software [9]".

El concepto de la infraestructura hiperconvergente se cimienta en el hipervisor, (incluso de ahí se acuña la raíz “hiper” en el deslumbrante término hiperconvergencia), el cual ejecuta como software las distintas rutinas de administración del procesamiento, almacenamiento y red, de manera que se vuelve más eficiente la operación y administración del espacio físico y tiempos de respuesta en el departamento de tecnología y para el negocio en general.

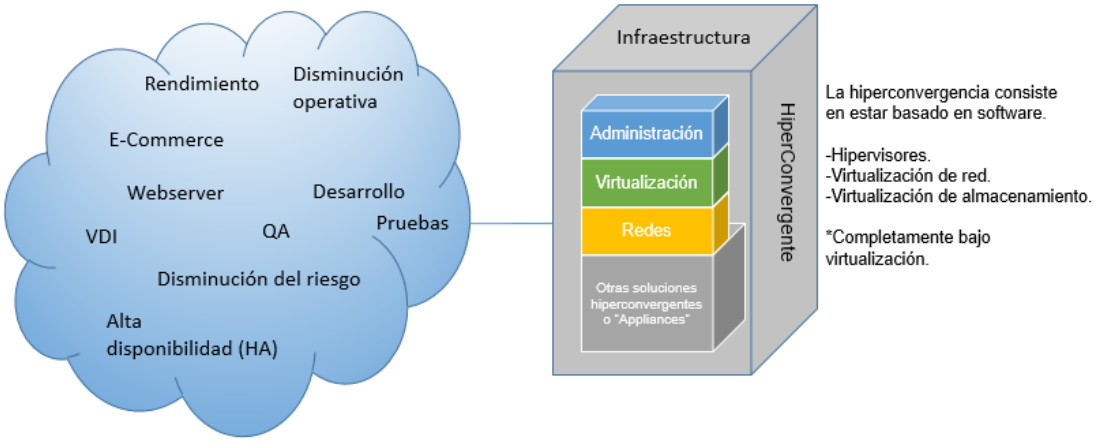

Ilustración 8: La infraestructura hiperconvergente, utiliza la virtualización para crear un centro de datos basado en software, generando las ventajas operativas y de negocio antes descritas.

Fuente: Elaboración propia.

La transición empresarial de pasar por la infraestructura tradicional hasta llegar a su versión hiperconvergente puede variar en cada organización, sin embargo, es claro que esta última representa la base para que una empresa comprometida con su éxito tecnológico pueda establecer un centro de datos definido por software (SDDC por sus siglas en inglés), moderno y completo, y esto la sitúe a las puertas de emplear los servicios en la nube adecuadamente.

A efectos de cuantificar la importancia de la infraestructura hiperconvergente en la actualidad, “el mercado global le da una valorización económica de USD 1459.56 millones en el año 2016 y se espera que alcance USD 17026.74 millones para el año 2023, estimando un crecimiento del mercado de esta tecnología a una tasa anual compuesta del 42 por ciento para el periodo del 2016 al 2023 [11]”. Lo cual nos permite vislumbrar la consolidación y el futuro en este tipo de tecnología para los próximos años.

2.3 La nube tecnológica, clasificación y servicios

Si bien, para las organizaciones modernas, adquirir infraestructura tradicional o convergente está dentro de lo esperado para su funcionamiento, lo que se ha convertido en un avance fundamental es utilizarla o consumir sus recursos a través de una red y comúnmente a través de Internet. Esta tendencia a utilizar servicios en la red local de la organización o a través de Internet, y situarla a disposición de usuarios específicos o al público en general, se le conoce con el término de nube, nube informática, o nube tecnológica, donde el término nube es una forma metafórica de describir a la red conectando a los usuarios, independientemente de su ubicación geográfica y dispositivo de acceso a la misma, estos se conectan y acceden a los servicios que esta nube (red) les brinda. La nube entonces es un modelo de consumo de la infraestructura, y no es la infraestructura como tal.

En general podemos distinguir o clasificar en cuatro formas de implementación la nube tecnológica o informática, a continuación, el detalle:

2.3.1 Nube pública:

Para el caso en que la infraestructura es administrada por un proveedor externo que brinda servicios informáticos a través de la Internet en forma pública, gratuita o con costo, y accesible para todo el que desee utilizarla, se le conoce como nube pública, Dentro de sus características que la hacen atractiva al mercado, está la eliminación del proceso de adquirir infraestructura (el proveedor se encarga de la disponibilidad, mantenimiento, y administración del servicio), además de facilitar y generar con mayor rapidez la puesta en marcha, y permite escalabilidad fácil y transparente al usuario. El debate actual de este tipo de infraestructura es si realmente es conveniente y seguro colocar la información en un entorno de red desconocido físicamente para el usuario, dependiendo de la disponibilidad de acceso a la red y expuesto a potenciales riesgos de seguridad informática.

2.3.2 Nube privada:

En cuanto al caso donde la infraestructura es administrada por la propia organización y brinda servicios propios a grupos definidos de usuarios, se le conoce como nube privada, interna, o corporativa. De igual forma puede utilizarse la Internet como la red de comunicación, pero los servicios y su

acceso son dominio completo de la empresa, lo cual brinda algunas ventajas de escalabilidad, personalización y control del servicio, en forma local. Se le suele atribuir una mejor seguridad informática a la nube privada, principalmente por su seguridad perimetral controlada de manera local o interna, y un acceso confidencial de la información restringido a un grupo específico de usuarios en la organización sin intervención o manipulación de proveedores externos. En consecuencia, lo anterior exige recurso humano profesional a cargo de la infraestructura que soporta la nube privada y sus servicios, bastante similar a la administración de infraestructura tradicional.

2.3.3 Nube hibrida:

Un tercer concepto nace de la utilización de la nube pública y privada, se le conoce como nube híbrida, y corresponde a la configuración de una nube privada con la capacidad de escalar hacia una nube pública en situaciones específicas y controladas, delegando intencionalmente servicios a esta última, pero con la particularidad de permitir un acceso restringido de los datos en la nube privada, resguardando bajo seguridad perimetral el centro de datos local, mientras que se escalan solo ciertos servicio o aplicaciones a la nube pública.

2.3.4 Nube comunitaria:

Existe una cuarta alternativa de nube informática denominada comunitaria, suele ser poco común, consiste en compartir recursos en una red donde solo se comunican organizaciones específicas, principalmente es utilizada para cooperación entre instituciones gubernamentales, o académicas.

En cuanto a los servicios que se brindan en una nube tecnológica, actualmente se distinguen cuatro clasificaciones, tres de ellas ampliamente posicionadas en el mercado actual, y una cuarta alternativa emergente, en ese orden:

2.3.5 Infraestructura como un servicio (IaaS):

La infraestructura como un servicio, abreviado IaaS por sus siglas en inglés, corresponde al primer y más básico servicio que se brinda en la nube, el cual es aprovisionado y administrado a través de la red, comúnmente a través de la Internet, pensado para ser escalable ante la demanda del recurso. En los casos del servicio de pago, el proveedor externo solo factura el recurso

utilizado durante el periodo contratado, mientras que la organización que lo adquiere no invierte en equipos físicos ni costos en centro de datos. La característica principal que lo diferencia de otros tipos de servicios es que sus recursos se contratan como componentes individuales, como el caso del almacenamiento, procesamiento, memoria, red, son ejemplos de recursos que se contratan en cantidad y periodos en que se necesiten, así el proveedor soporta la infraestructura en la nube, mientras la organización que compra el servicio dedica su tiempo a implementar su propio sistema operativo, software, y aplicaciones. En este tipo de implementación el proveedor no debe tener acceso a los datos e información de la organización, esto debido a que las claves de acceso y la seguridad informática del contenido, corresponden solamente a la organización, lo que hace que esta modalidad se utilice ampliamente en ambientes de desarrollo, pruebas, respaldos y sitios web personalizados.

2.3.6 Plataforma como un servicio (PaaS):

La plataforma como un servicio, abreviado PaaS por sus siglas en inglés, es el segundo tipo de servicio en la nube, el cual incluye los mismos componentes de infraestructura como servicio (IaaS), pero además provee entornos completos para desarrollar e implementar aplicaciones o servicios completos, permitiendo que las organizaciones paguen solamente por el uso de estos, principalmente software de integración, desarrollo, inteligencia empresarial (BI), bases de datos, u otros pre configurados por el proveedor y listos para utilizar en ambientes productivos.

2.3.7 Software como un servicio (SaaS):

El tercer servicio en nube se denomina software como servicio, abreviado SaaS por sus siglas en inglés, y corresponde a servicios completamente implementados y funcionales en Internet, disponibles para que los usuarios se conecten a usarlos en cualquier momento, como el caso de los correos electrónicos, ofimática en línea, u otras herramientas ampliamente utilizadas en la actualidad. Estos servicios a nivel empresarial suelen ser contratados por sus características, cantidad de usuarios, y tiempo de uso. En cuanto a la administración de la infraestructura, es completamente

gestionada por el proveedor, incluyendo el software, hardware, disponibilidad, e inclusive la seguridad de la información en muchos casos.

Tabla 3: Responsabilidades del cliente según los Modelos de Servicios en la nube contratados.

Servicio tradicional (En sitio/local)	**IaaS Infraestructura como Servicio**	**PaaS Plataforma como servicio**	**SaaS Software como servicio**
Aplicaciones	Aplicaciones	Aplicaciones	-
Datos	Datos	Datos	-
Procesamiento	Procesamiento	Procesamiento	-
Lógica de intercambio	Lógica de intercambio	-	-
Sistema Operativo	Sistema Operativo	-	-
Virtualización	-	-	-
Servidores	-	-	-
Almacenamiento	-	-	-
Red	-	-	-

Fuente: Elaboración propia

2.3.8 Informática sin servidores:

Una tendencia más reciente en servicios en la nube, es la informática sin servidores, o algunas veces nombrada por su término en inglés como *serverless*[5]. La compañía tecnológica multinacional Microsoft en su portal web propone el concepto de informática sin servidores, definiéndola como "la abstracción de los servidores, la infraestructura y los sistemas operativos [12]" y continúa caracterizándola por su "reacción a eventos y desencadenadores que tienen lugar casi en tiempo real, en la nube [12]", lo cual desliga totalmente la necesidad de gestionar servidores por parte del desarrollador o el administrador. Por lo anterior, el trabajo se centra en ejecutar el código, y la escalabilidad es inmediata, invisible, y es desencadenada por demanda en tiempo real.

[5] Serverless, se puede traducir al castellano como la frase "sin servidores", es usada para indicar la ausencia de estos componentes.

Capítulo 3: La seguridad informática de la infraestructura convergente, hiperconvergente y servicios en la nube.

Como se valoró en los capítulos anteriores, la virtualización es un mundo tecnológico muy amplio en todos sus aspectos, con grandes e innovadores saltos ocasionados por la demanda de las organizaciones modernas, lo cual confluye en la necesidad de gestionar su seguridad informática de manera constante.

El presente capítulo está dedicado a revisar particularmente la seguridad informática relacionada a la infraestructura virtual, revisar los aspectos técnicos involucrados en función de lo descrito en los capítulos anteriores y brindar teoría útil para este tipo de entornos empresariales.

3.1 Seguridad Informática

Como un primer concepto la seguridad de la información consiste en "asegurar la identificación, valoración y gestión de los activos de información y sus riesgos, en función del impacto que representan para una organización [13]", por lo que es muy importante recalcar que "no se centra en la protección de las TIC sino de todos los activos de información que son de un alto valor para la institución [13]". Después de todo cierta información aún está contenida en medios físicos ajenos a la tecnología.

Por su parte la seguridad informática es "la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable [14]", aunque podemos reforzar esta definición "como el conjunto de procesos destinados a proteger la disponibilidad, la privacidad y la integridad de los datos, sea de personas o instituciones [15]", aunque como nota aclaratoria, la seguridad total no se puede garantizar en nuestros días.

De lo anterior se tiene que en general las empresas acostumbran atender normalmente a la disponibilidad de la información, pero son pocas las que realmente prestan una correcta atención a la integridad y confidencialidad de la misma y en algunos casos esto es un error muy costoso.

La importancia de la seguridad de la información radica en que las personas están exponiendo su privacidad, volcando datos públicos y privados en entornos tecnológicos, en muchas ocasiones por desconocimiento o por la necesidad de utilizar un servicio bajo ciertas condiciones del proveedor.

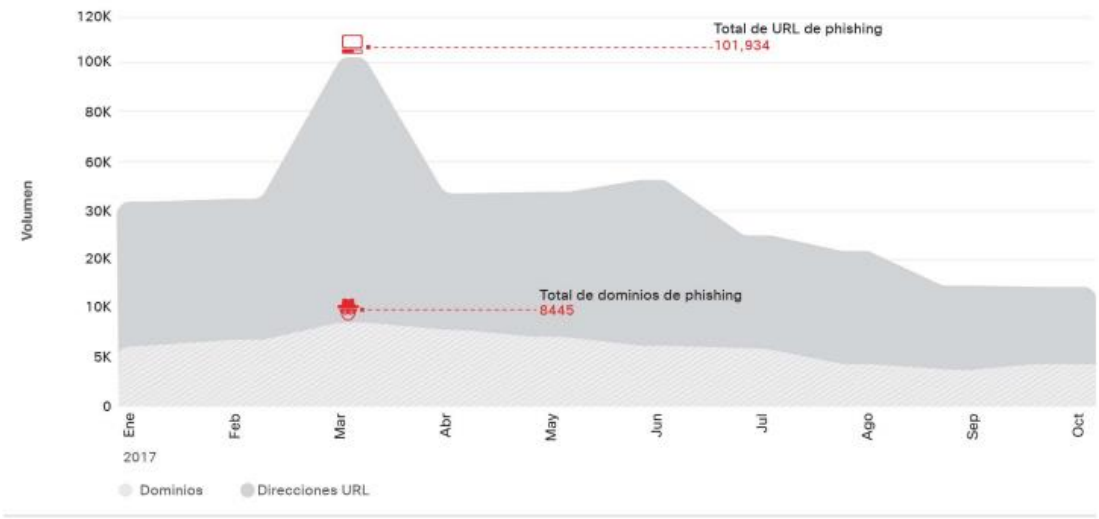

Ilustración 9: Número de URL y dominios phishing observados por investigadores de CISCO en un año.

Fuente: Cisco Security Research [16]

La figura anterior es solamente un ejemplo concreto de como los usuarios se exponen a miles de amenazas en un año, incluso desapercibidos aun cuando todo esto pasa dentro de la infraestructura tecnológica que soporta servicios y a otros usuarios.

3.2 La seguridad de la infraestructura física

El panorama de la infraestructura que soporta a los equipos virtuales y sistemas convergentes, es que definitivamente dependen de una seguridad física, la cual se debe revisar en orden de criticidad, pues si bien una ventaja conocida de la virtualización es poder concentrar en poco espacio muchos equipos y servicios virtuales, esto también los vuelve más cruciales, debido a que si bien es complejo tener acceso o sustraer servidores tradicionales físicos o pesados, lo contrario es la facilidad con la que en un pendrive en nuestros bolsillo podemos transportar uno o varios servidores virtuales y toda su información.

Para cubrir esta amenaza física de seguridad, actualmente se cuentan con soluciones, desde las más convencionales como acceso con cerraduras

físicas estándar, hasta algo más especializado como la biometría. Esta última es la que mayormente se está utilizando, consiste en “identificar y verificar de forma automatizada la identidad de las personas, animales y objetos mediante características físicas y pautas de comportamiento de estos [17]”. Entre las formas de biometría utilizadas actualmente, encontramos la lectura de huellas dactilares, reconocimiento de voz, ojos, facial, la secuencia o velocidad de tecleo, firma, termografía de rostro y geometría de manos.

También existen alternativas adicionales a estos sistemas biométricos, como los tradicionales accesos con usuario y contraseña a digitar en la puerta del centro de datos, o validar identidad utilizando la posición geográfica de las personas.

Lo anterior es un panorama de control físico y lógico para acceder a la infraestructura que soporta los equipos virtuales y la combinación de algunos de estos métodos origina el doble, triple, o múltiple factor de autenticación como la opción deseada para resguardar equipos físicos importantes.

Al contemplar que la infraestructura virtual conlleva adquirir costosos equipos empresariales para gestionar información y servicios, es entonces que se debe tomar especial cuidado de las amenazas tanto naturales como humanas, no solo considerando las formas de acceso descritas, sino también en aspectos de ubicación interna de los equipos convergentes, ubicación geográfica, alimentación eléctrica, refrigeración, material de pisos y paredes, detección de incendios, perímetro, cerrojos electrónicos, ventanas, alarmas, cámaras, monitoreo, vigilancia profesional y personal a cargo del sitio.

En cuanto a normativas, existe documentación como el estándar TIA-942, elaborado por la Asociación de la Industria de Telecomunicaciones (TIA) norteamericana, la cual entre otras recomendaciones y directrices, incluye aspectos de diseño e implementación de Centros de Datos, sus gabinetes, equipos físicos como servidores o unidades convergentes, dispositivos de comunicaciones, cableado de la red, además de categorizar la disponibilidad y seguridad del centro en cuatro niveles o [6] “*tiers”*.

[6] Categorías Tier (nivel), usado para categorizar la disponibilidad en Centros de Datos.

Tabla 4: Resumen de Niveles o Tier de disponibilidad y seguridad según el Estándar de infraestructura de telecomunicaciones para centros de datos TIA-942

Niveles	Disponibilidad	Descripción general
Tier 1: Centro de Datos Básico	99,671%	-Susceptible a interrupciones tanto de actividades planificadas como no planificadas. -Requiere detener operación para mantenimiento.
Tier 2: Centro de Datos con componentes redundantes	99,741%	-Menos susceptibles a las interrupciones de actividades planificadas y no planificadas. -Requiere detener operación para mantenimiento.
Tier 3: Mantenimiento en caliente	99,982%	-Permite actividades planificadas de infraestructura sin interrumpir la operación. Mantenimiento programado, reparación y reemplazo de componentes. -Actividades no planificadas o fallas pueden causar interrupción de operación.
Tier 4: Tolerancia a fallas	99,995%	-Soporta interrupciones de actividades planificadas y al menos un evento no planificado crítico, sin detener operación. -Requiere sistema completo redundante.

Fuente: Elaboración propia con información obtenida del documento TIA-942-A. [18]

3.3 La seguridad de los equipos convergentes y virtualización

En el diseño y la implementación de un Centro de Datos seguro es donde se fortalece la seguridad informática de la organización, pero otro punto focal son los equipos de cómputo que se utilizan y nuestra actualidad incluye combinación de infraestructura tradicional, convergente, hiperconvergente, e incluso servicios de nube informática y ambientes virtuales.

La convergencia de equipos ofrece ciertas mejorías en seguridad informática física y lógica, como la simplicidad de apilar en poco hardware la operación, su implementación, costos, administración, escalamiento, entre

otros, pero además brinda ventajas de seguridad por software, mediante cifrado nativo de datos, eliminación lógica de la información, disponibilidad, rendimiento y gestión nativa de normativas o regulaciones.

En principio para la seguridad física de este tipo de tecnología, se aplican las mismas prácticas tradicionales de resguardo, pero adicionalmente los fabricantes proveen herramientas propias para monitorear la infraestructura convergente, con alarmas y monitoreo de los gabinetes, apertura irregular de los mismos, detección de desastres como indicios de incendio, inundación, u otros factores a los que se le puedan aplicar controles mediante sensores y software. Los fabricantes siempre entregarán recomendaciones para los equipos, incluso servicios conexos para dar soporte externo en algunos casos.

La inversión a realizar en la infraestructura y su seguridad, depende en gran medida a una correcta identificación de los puntos o equipos críticos de la misma. Por eso resulta relevante que exista documentación que de visibilidad de los equipos que se contienen en los gabinetes, tanto en sus características físicas como lógicas, su configuración y exposición a la red.

Ilustración 10: La seguridad de la Infraestructura convergente inicia en la correcta implementación y se continua en la administración de todos sus componentes físicos y virtuales.

Fuente: Implementación de unidad convergente, Universidad Estatal a Distancia, Costa Rica, 2017.

3.3.1 Vulnerabilidades

En cuanto a vulnerabilidades conocidas que puedan amenazar infraestructuras modernas, es necesario comprender que existen, por lo que se debe tener visibilidad de las mismas. Las ventajas de la infraestructura convergente, hiperconvergente y servicios en la nube son grandiosas en términos técnicos y de negocio, pero también son susceptibles a numerosas vulnerabilidades, algunas en implementación física, pero principalmente el foco de amenazas se concentra en su software y en el hipervisor cuando es tecnología virtual.

Un primer ejemplo de vulnerabilidad documentada es VENOM, identificada en el año 2015, está documentada en la lista CVE[7] con el id CVE-2015-3456, consiste en usar el controlador de disquete (FDC) en el entorno virtual QEMU, Xen 4.5.x, o KVM, y mediante usuarios del host invitado puede provocar una denegación de servicio por desbordamiento haciendo fallar el equipo, o ejecutar código a través de ciertos comandos del dispositivo. Ver Anexo #1: Detalle de CVE para la vulnerabilidad conocida VENOM para mayor detalle.

Otras vulnerabilidades conocidas y documentadas son Spectre y Meltdown, también identificadas en la lista CVE con los identificadores CVE-2018-7112, CVE-2018-19965, y CVE-2017-5754. Meltdown se aprovecha de los microprocesadores Intel fabricados desde el año 1995, leyendo zonas de memoria reservadas con datos sensibles, incluyendo contraseñas, y por su parte Spectre utiliza microprocesadores Intel, ARM, y algunos AMD, abusando de la función de ejecución especulativa con que se fabrican, accede a procesos a través de la memoria virtual usada por los mismos. El problema de estas vulnerabilidades actualmente reside en que se documentaron a inicios del 2018, su detección temprana es muy difícil, y afecta a la gran mayoría de microprocesadores, incluyendo a los que soportan la mayoría de servicios en la nube. La reacción de los grandes fabricantes como Intel, o proveedores como Google y Amazon, ha sido realizar cambios en el acceso de la memoria, aislando la tabla de páginas del Kernel y aplicar actualizaciones para

[7] La lista CVE consiste en registros de vulnerabilidades de seguridad con número de identificación único, y acceso público. Es gestionada sin fines de lucro por MITRE Corporation.

contrarrestar la amenaza, lo cual teóricamente puede disminuir en cierta forma el rendimiento de los equipos.

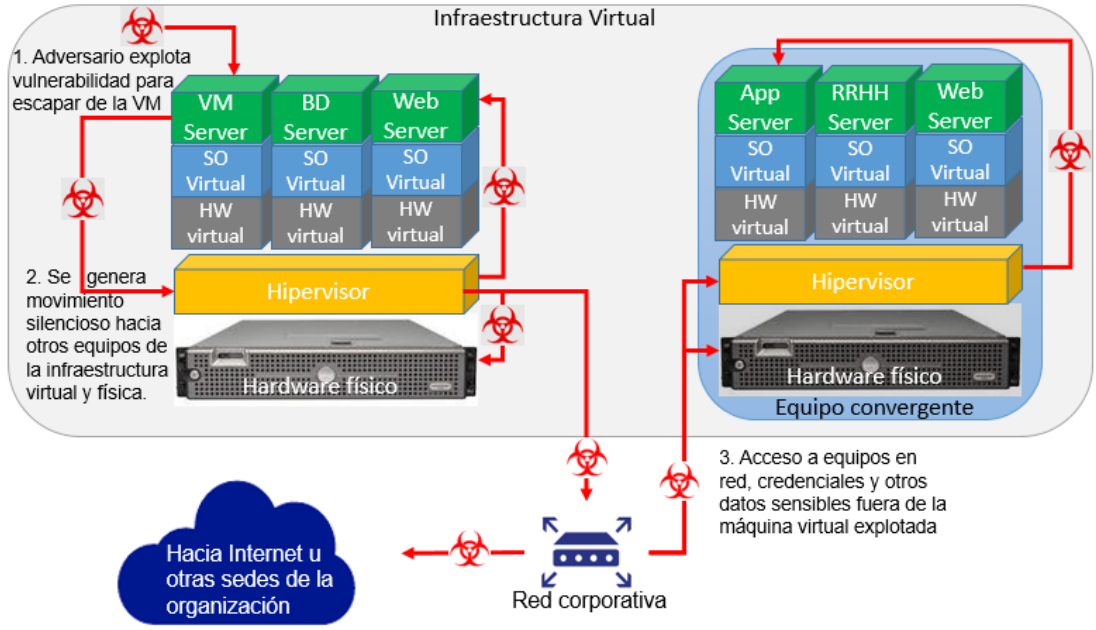

Ilustración 11: Proceso de explotación de vulnerabilidad VENOM en la infraestructura tecnológica.

Fuente: Elaboración propia

Como se puede apreciar en la figura anterior, la infraestructura tecnológica de la organización está expuesta constantemente a vulnerabilidades conocidas y a las que puedan surgir en el futuro cercano, las cuales en gran medida logran acceso a través de los equipos virtuales que brindan servicio y la red en la que conviven. Por lo anterior resulta crucial el aseguramiento informático de las máquinas virtuales, sus sistemas operativos, y los equipos físicos que soportan la operación.

Dentro de las principales prácticas que se deben adoptar, está en concebir la seguridad de las máquinas virtuales en función de archivos almacenados en el host, creados mediante plantillas, y almacenados de una manera lógica, por lo que todo el proceso de diseño, creación, almacenamiento, respaldo, redundancia, acceso, y gestión, merece especial atención en su seguridad.

3.4 Seguridad de la red física y virtual

Como se mencionó previamente, una de las formas comunes para que un atacante tenga acceso a la infraestructura, es a través de la red informática, y al factor humano que la utiliza o gestiona.

La realidad tecnológica hace que cada vez más usuarios consuman servicios en la red, accedan a servidores, utilicen escritorios virtuales, consulten información en red, entre otras acciones, pero todo eso se logra a través de dispositivos de comunicación como enrutadores y conmutadores cada vez más inteligentes o sofisticados, y dependientes del software. Todos los fabricantes de estos equipos de comunicación están innovando constantemente en seguridad informática por las continuas amenazas cibernéticas a las que están expuestos los dispositivos, por lo que no basta su implementación segura, y según el negocio o las dimensiones de cada organización, se debe recurrir a otra serie de mecanismos para brindar un mayor aseguramiento, como el caso de sistemas de monitoreo, corta fuegos, sistemas de prevención y detección de intrusos, entre otros.

Otro factor creciente en el uso de redes es su modalidad inalámbrica, que si bien es una apertura funcional importante y necesaria para todo negocio, también representa un punto de amenaza para la seguridad informática, con técnicas conocidas para vulnerar este tipo de red, engañar a usuarios de la misma, y esto hace que también se deba recurrir a técnicas de aseguramiento, tanto en la configuración de los dispositivos que emiten la señal, así como en métodos más robustos de autenticación y autorización.

Dentro de las particularidades de la seguridad de la red en una infraestructura virtual, está la amenaza tradicional en que un atacante pueda lograr una conexión no autorizada, pero adicionalmente entra el juego del software que origina tarjetas de red virtuales, la forma en que se crean estas tarjetas, y la gestión que un hipervisor brinda sobre estas. Si bien las tarjetas de red físicas y el cableado estructurado conectado a ellas les brinda características propias de su naturaleza que le impiden variar parte de su configuración, en el caso de los dispositivos virtuales, en esencia son archivos lógicos, los cuales requieren cuidado y atención justamente por esa característica.

Si bien en los aspectos estructurales mencionados existe un riesgo de seguridad en la red, es necesario tener visión y control de lo que sucede a través esta, pues es común que las organizaciones estén utilizando cada vez más herramientas en línea, colaborativas, y con diversas funcionalidades, generando apertura de puertos y uso de protocolos que pueden dejar en riesgo la malla corporativa, por ejemplo en el uso indiscriminado de acceso a servicios web internos o externos, administración remota de dispositivos, herramientas para ingresar al escritorio remoto, entre otros.

3.4.1 Diseño de redes seguras

Entonces resulta necesario un adecuado diseño de la red física y virtual en la organización, que contemple todos los aspectos de infraestructura, telecomunicación, y configuración lógica de la misma.

El modelo OSI es el referente utilizado para abstraer la red, básicamente define siete capas por las que se transfieren los datos de un dispositivo a otro en la red, se aplica indiferentemente de si esta red es física o virtual, por lo que es susceptible a técnicas de ataque pasivo o activo, donde el primero intercepta y analiza el tráfico de los datos, mientras el segundo intercepta y modifica los datos para un fin particular.

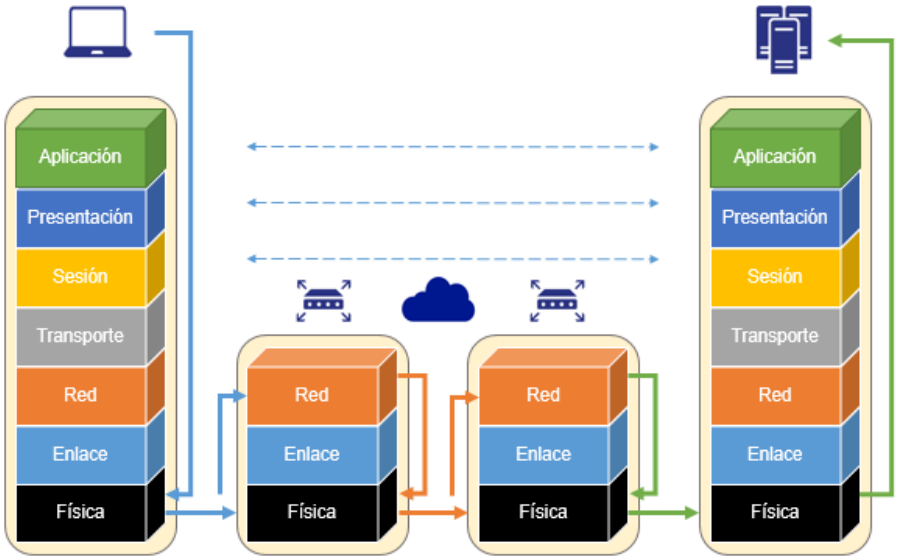

Ilustración 12: Flujo de datos de un dispositivo en red, hacia otro, según modelo OSI.

Fuente: Elaboración propia

Una antigua estrategia militar conocida como defensa en profundidad, suele ser aplicada a los sistemas informáticos para manejar estas situaciones de seguridad, la cual en esencia es desconfiar y entender que todo componente de un sistema puede ser vulnerado, y por lo tanto se debe trabajar en cada uno de ellos hasta donde sea posible asegurarlos como si fuesen líneas de defensa o capas, desde las más expuestas hasta la más interna.

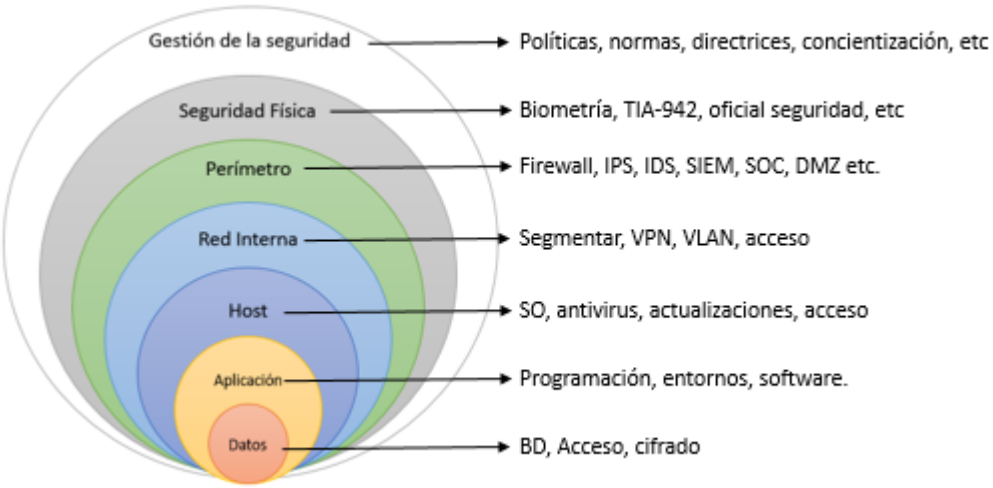

Ilustración 13: Propuesta general de modelo de defensa en profundidad, en un entorno informático.

Fuente: elaboración propia

Como se aprecia en la figura anterior, dividir y trabajar en segmentos la infraestructura tecnológica es una práctica recurrente para abordar la seguridad en la red informática. La "red más insegura es aquella que se denomina plana, en la cual todos los equipos tienen conectividad abierta entre unos y otros, sin ningún tipo de filtrado [19]", esto desemboca en la necesidad de conocer los entornos, y poder separarlos para fines productivos, desarrollo, pruebas, administrativos, o categorizarlos según lo requiera la organización. Dentro de las alternativas principales es necesario contemplar una zona desmilitarizada (DMZ[8]) para los servicios expuestos, utilizar cortafuegos para filtrar conexiones, utilizar capacidades de lista de control de acceso en enrutadores, configurar en los conmutadores distintas VLANs para aislar

[8] DMZ, siglas en inglés de Zona Desmilitarizada, consiste en un segmento de red donde se alojan servicios expuestos a Internet, con el fin de contener potenciales ataques, sin afectar servicios internos.

segmentos de red lógicos que se comporten independientes e identificados por etiquetas, y adicionalmente se debe recurrir a redes privadas virtuales (VPN) para asegurar la comunicación cuando se utilicen medios inseguros como el Internet al extender la red corporativa. También, las capacidades de la infraestructura pueden extenderse a nodos inalámbricos que pueden requerir herramientas de autenticación, autorización, prevención y detección, como Radius, IDS, IPS, SIEM, honeypots[9], u otros.

Contemplando que todos los dispositivos de red involucrados pueden ser completamente virtuales o definidos por software, es necesario prestar atención a su configuración, actualización, y control de quien los accede, máxime por su capacidad de ser administrados remotamente y estar expuestos sin acceso físico, ante la situación, es buena práctica implementar algún software administrador de contraseñas alineado a la gestión de seguridad de la información.

3.5 Seguridad de los servicios, programación segura y separación de entornos

Sobre la infraestructura virtual claramente se ofrecen servicios consumidos por los usuarios, estos colocan su información, y los datos son manipulados, almacenados, o reutilizados, a través de la red asegurada. Sin embargo, la implementación y mantenimiento de estos servicios en virtualización, requieren sus propios mecanismos de seguridad informática.

Cuando la organización desea brindar un servicio, realiza diversos análisis, como identificar activos de información, definir los que desea proteger, establecer control de acceso, recuperación, entre otros, y cuando se habla de activos lógicos o de información digital, entra en juego la seguridad informática en función de ese valor identificado, se debe abordar el desarrollo, pruebas, y la producción del servicio. Lo anterior nos lleva a la primera situación de seguridad informática en este tipo de servicios virtuales y es establecer entornos de forma adecuada.

La infraestructura tecnológica virtual como se ha mencionado tiene características propias, y existe tendencia a concentrarse en cuatro

[9] Honeypot: es una herramienta de seguridad informática colocada en algún punto de la red o en algún software, con el fin de detectar, capturar, y analizar un probable ataque informático.

categorías: virtualización del escritorio, la red, aplicaciones, y almacenamiento [20]. En consecuencia, se debe contemplar al menos esas cuatro categorías para separar recursos y adicionalmente en cada uno de ellos es importante establecer ambientes.

Ahora bien, en cuanto al servicio o aplicación, como mínimo su desarrollo se debe realizar en un ambiente para ese fin, posteriormente se traslada a un ambiente de producción, y es recomendable contemplar ambientes de pruebas o los que requiera la organización para no exponer la seguridad informática de los equipos y servicios durante el ciclo de vida del software. Todo lo anterior debe contemplar aspectos como definir responsables y roles, hacer una separación lógica y física del procesamiento, entre otros.

En cuanto al servicio, este normalmente corresponde a software para un fin específico, es ubicado en un equipo que le provee los recursos de procesamiento, puede ser una aplicación web y esta puede requerir revisión adicional de seguridad informática en su código de programación, en primera instancia se deben desarrollar sobre tecnologías robustas, actualizadas, y con soporte, pero además se debe tener claro conocimiento de las vulnerabilidades conocidas y aplicar estándares de programación segura y buenas prácticas.

Otro factor a contemplar desde el desarrollo, es la arquitectura de la base de datos, la cual se define en un motor de base de datos y se utilizan modelos para establecerla, sin embargo, la utilización de características seguras en la administración de la base de datos es fundamental para evitar problemas conocidos y vulnerabilidades.

Por lo anterior, se pueden considerar algunas pautas generales para la protección de servicios virtuales, como mantener aplicaciones y bases de datos en contenedores seguros, programar bajo estándares y conocimiento en seguridad, revisar constantemente las vulnerabilidades que afecten la aplicación, actualización de los estándares utilizados o los que puedan surgir, y valerse de distintas capas de seguridad o características de protección.

3.6 Seguridad de los servicios en la nube

Para señalar aspectos de seguridad informática de los servicios en la nube, es necesario reconocer que "independientemente de que la virtualización es la tecnología fundamental gracias a la cual existe la computación en la Nube, son conceptos diferentes y sus aplicaciones también varían [21]", tanto así que la seguridad informática debe readecuarse a características nuevas que aparecieron con la nube.

Como asentamos de previo, la virtualización respondió a una mejor capacidad de procesamiento, almacenamiento y conectividad, bajó costos de hardware, e incluyó tecnológicamente a la mediana y pequeña empresa, pero la nube ofreció mejoras basadas en diseño de servicios flexibles, acondicionados al cliente, cobrando solo por los recursos consumidos, y ofreciendo opción de nube pública, privada, comunitaria e híbrida. Lo anterior ha gustado y continúa desarrollándose, ofreciendo los diferentes modelos de servicio. Entonces la seguridad informática se trasladó a la nube también, y en primer lugar afecta a los modelos de servicio descritos como IaaS, PaaS, SaaS, por lo que "en la nube se usan herramientas de seguridad basadas en software para monitorizar y proteger el flujo de información que entra y sale de los recursos en la nube [22]", donde la gestión y seguridad de estos recae en diferentes actores.

El proveedor de la nube, puede ser la propia organización, algún tercero que cuenta con la infraestructura virtual adecuada, o combinación de ambos, por lo que, según el caso, la seguridad está estrechamente relacionada a quien provee la nube. Al considerar que la información y los datos residen en un entorno virtual, es necesario aplicar ciertas prácticas de seguridad como encriptación de discos duros, gestionar las copias de respaldos en sitios alternos, establecer roles de quienes tienen acceso a la configuración de la infraestructura virtual, contemplar el riesgo proveniente de los usuarios finales y el uso que estos le dan a sus dispositivos móviles, portátiles, computadores, u otros medios de consumo del servicio, y estar en constante alerta ante la exposición de ataques dirigidos al proveedor, organización, o al usuario final, principalmente en tipos de ataques que

pretenden vulnerar o interrumpir el servicio, por ejemplo DDoS[10], análisis de paquetes en red, suplantación de identidad, u otra serie de mecanismos activos y pasivos utilizados para infringir la seguridad de la información de los usuarios finales.

Por lo anterior, se deben contemplar todas las medidas de seguridad conocidas para asegurar el canal de transmisión de la información, pero además es necesario revisar el contrato del servicio, adquirir estos de un proveedor con trayectoria comprobada en el área, establecer un acuerdo de nivel de servicio (SLA por sus siglas en inglés) adecuado a la necesidad, incluir aspectos de privacidad de la información, identificar ubicaciones geográficas donde se almacenará la información, y validar aspectos de legislación nacional e internacional que no pongan en riesgo el servicio y a los usuarios (algunos países exigen que los datos no salgan de sus fronteras). No está de más hacer el ejercicio de validar si el servicio contratado realmente cumple con pilares de la seguridad de la información como confidencialidad, autenticación, integridad y no repudio.

Entonces, la nube informática nos ha proveído diversos servicios desde la aparición de Internet, pero la adopción natural de servicios flexibilizados hacia nuestras necesidades cada vez es más recurrente, con grandes beneficios y nuevos riesgos de seguridad informática, principalmente apuntados a la virtualización de tecnología sobre la que se asienta la nube.

Actualmente diversos países, incluyendo Estados Unidos, España, entre otros, han definido a través de sus organismos o agencias a cargo de la seguridad (NIST en Estados Unidos), ciertas pautas sobre seguridad y privacidad en la computación en nube pública, lo cual refleja una clara preocupación por establecer aspectos claves de la nube, entre ellos la seguridad informática.

3.7 El negocio y la gestión de la seguridad informática en infraestructura virtual.

En términos generales, una organización debe establecer un sistema de gestión de la seguridad de la información (SGSI), además sigue etapas

[10] Es un ataque informático que busca dejar inaccesible un recurso o servicio para los usuarios, normalmente provocado por utilizar todo el ancho de red disponible o por consumir todo el recurso de procesamiento.

para diseñarlo, implementarlo, y mantenerlo a largo plazo, de manera que puede gestionar los activos de información, trabaja su confidencialidad, integridad, disponibilidad, y se constituye en función de los riesgos de estos activos. El SGSI recurre a la norma ISO/IEC 27001 (SGSI) e ISO/IEC 27002 (controles dentro del proceso para la implementación del SGSI) como estándares para la seguridad de la información, y a su vez utiliza el círculo de Deming (PDCA), que significa “Planificar-Hacer-Controlar-Actuar” en busca de la mejora continua de la seguridad informática. Sin embargo, ante diferentes necesidades, surge la posibilidad de trabajar con diversas metodologías, o marcos de trabajo, que permitan tener el panorama de la seguridad informática, inclusive en infraestructura virtual y servicios en la nube. Ver Anexo #2: Modelos utilizados para la gestión de la seguridad de la información, para mayor detalle.

Si bien existen distintos modelos para la gestión de la seguridad, la selección de cual conviene implementar en una infraestructura virtual y servicios en la nube requiere que se preste atención a sus componentes y actores como se ha señalado antes, pues algunos marcos de trabajo o guías de mejores prácticas como por ejemplo SAFE de CISCO ofrecen particular atención a la seguridad de la red, ISO/IEC 27001 contempla aspectos operativos de comunicación interna y externa, o el modelo SOGP del Foro de Seguridad de la Información (ISF) que señala gobierno, requisitos, control, seguimiento y mejora de la seguridad. Todo lo anterior nos muestra que existen alternativas para que se pueda abordar responsablemente la seguridad de las nuevas tecnologías virtuales.

A lo anterior se le debe sumar la importancia de que los diferentes actores estén comprometidos con el tema de seguridad informática, pues primeramente desde las autoridades debe venir un apoyo alineado a objetivos y políticas institucionales, mientras que por su parte los colaboradores del área de seguridad de la información deben ser facilitadores antes que auditores, proponiendo soluciones al negocio, comunicando eficientemente, utilizando lenguaje entendible, y brindando estatus real o transparente a las autoridades, y si existiese intervención de proveedores o terceros, estos también deben estar envueltos con el fin de la organización y su seguridad informática.

La gestión de la seguridad debe mirar considerablemente hacia la continuidad del negocio (CN), de manera que incluya a la infraestructura virtual en aspectos de respaldos, pérdida o robo de información, monitoreo, control cambios, incidentes, contar con análisis de impacto al negocio (BIA), plan de continuidad del negocio (BCP), plan para la recuperación de desastres (DRP), normas, controles, procedimientos, estándares, certificaciones en seguridad, roles, responsables de la información, concientización en la organización, entre otros. También se debe avistar factores externos, como la comunicación y protocolo con el CERT o CSIRT[11], por ejemplo.

Siempre está latente la aparición de algún evento que ponga a prueba la capacidad de la organización, y cuando este tipo de incidentes aparecen, además de lo mencionado, se debe divisar la respuesta adecuada, recabar evidencia, valorar los procesos o activos de información afectados, y no menos importante ver los aspectos legales que puedan emerger como consecuencia. Ante esto, una adecuada gestión de la seguridad informática incluye localizar rastros en ambientes virtuales, mantener contacto e informes con el CSIRT respectivo, establecer y cuidar una posible cadena de custodia de todo el ambiente virtual o servicio en la nube afectado, valora posibles delitos informáticos, y acatar cualquier otra acción técnica, administrativa, o legal. En definitiva, la infraestructura de virtualización, y los servicios en la nube informática, abren un abanico de potenciales incidentes que exigen una respuesta profesional, máxime que cada día las personas invierten más información en este tipo de sistemas digitales.

3.8 Consideraciones generales de la seguridad informática en tecnologías emergentes

La infraestructura de virtualización y los servicios de cómputo en la nube llegaron para quedarse, pues en la sociedad moderna las personas se vuelven cada vez más dependientes de estos, su información se traslada al mundo digital, incluso a diferencia de las personas de mayor edad las nuevas generaciones nacen y se les empieza a colocar toda su información en datos

[11] El CERT (Equipo de Respuesta ante Emergencias Informáticas) o CSIRT (Equipo de Respuesta ante Incidencias de Seguridad Informática) recibe, analiza, coordina, y genera informes de incidentes locales/globales desde y hacia su comunidad, otros CSIRT, o terceros.

digitales, lo cual parece desembocar en tecnologías emergentes dependientes de la red global, Internet, o similar.

Dentro de este tipo de tecnologías innovadoras, son ampliamente conocidas las redes sociales, el Internet de las cosas (IoT), la inteligencia artificial (IA), minería de datos, big data, realidad aumentada, las versiones de la web 1.0 (páginas web), 2.0 (web social), 3.0 (webs semánticas), 4.0 (web inteligente), solo por mencionar algunos. Pero de todos estos ejemplos, nacen aspectos de seguridad informática ligados a características digitales o virtuales, ya no se habla solamente del acceso físico o de un ataque a un dispositivo informático, sino de técnicas sociales que aprovechan la dinámica del mundo virtual. Ejemplo de ello es la exposición diaria en servicios de mensajería, WhatsApp, iMessage, Skype, transferencia de archivos, la fuga de información, el SPAM en correo electrónico, la suplantación de identidad, telefonía IP (VoIP), espionaje en telecomunicaciones (3G, 4G, red informática), videoconferencias, u otros.

Un paso más adelante a los ejemplos descritos, se vislumbran tecnologías enfocadas a interactuar en procesos de medicina y salud humana, procesos automatizados y controlados por inteligencia artificial, asistentes digitales, criptomonedas, y ordenadores cuánticos, por mencionar casos donde no solo consumimos servicios virtuales como los vistos, sino que les delegamos acciones y decisiones que finalmente serán ejecutadas por un software con acceso a recursos descomunales.

Las tecnologías emergentes representan una inquietud relacionada al tema de infraestructura virtual que, si bien escapa del alcance planteado en este documento, deja claro que se soportan sobre infraestructuras virtuales como las estudiadas, requieren inclusión en la gestión de la seguridad informática de las mismas, y nos invita a estar atentos a recurrir a las nuevas herramientas y normativas de seguridad que teóricamente entrarán a solventar situaciones en un futuro próximo.

Conclusiones

En la presente investigación se realizó el análisis de los hitos históricos de la virtualización así como su rápido auge hacia los servicios tecnológicos virtuales, y como primer hallazgo relevante anoto como las tecnologías virtuales se fueron moldeando por las distintas necesidades de las organizaciones, entrelazándose cada vez más con los procesos del negocio, y en consecuencia la seguridad informática tomó relevancia al punto tal que hoy día deben contemplarse forzosamente en conjunto con las actividades del negocio, esto al tiempo que las nuevas tecnologías van innovándose.

El presente texto también evidencia la composición de la infraestructura tecnológica virtual convergente y los servicios en la nube, de manera que, al comprender sus componentes, se demostró una gran y acelerada exigencia de seguridad informática en un breve período de tiempo, esto fue potenciado por las redes informáticas que facilitaron las conexiones de manera global, originando necesidades específicas en la sociedad moderna, se volvieron indispensables para las organizaciones, lo que abrió brechas de seguridad informática de las que no se tenía conocimiento.

Es entonces mi opinión profesional en el campo, y a la luz de la investigación plasmada en este texto, que debo subrayar la importancia de tener una mirada atenta y crítica hacia el diseño (de infraestructura virtual) y la normativa vigente, así como apoyarse en las metodologías de seguridad de la información existentes, lo anterior para atender el tema de la seguridad informática alrededor del creciente uso de infraestructuras tecnológicas virtuales.

Finalmente, por los hallazgos descritos, debo señalar que es claro como la seguridad informática converge con las infraestructuras tecnológicas virtuales, entrelazándose con los diversos procesos de las organizaciones, en consecuencia, se invita a los diferentes profesionales o involucrados del área de la seguridad informática y del ámbito académico a profundizar mediante nuevas investigaciones, y explícitamente recalco dos áreas de interés a saber:

Primeramente, se requiere prestar atención y abordar los fenómenos de ciberseguridad que se puedan presentar en tecnologías virtuales emergentes.

En un segundo foco, se vislumbra necesario indagar las diferentes metodologías de seguridad de la información que puedan ser aplicadas a estas particulares plataformas tecnológicas virtuales.

Anexos

Anexo #1: Detalle de CVE para la vulnerabilidad conocida VENOM

(Volver al texto)

CVE-ID	
CVE-2015-3456	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

The Floppy Disk Controller (FDC) in QEMU, as used in Xen 4.5.x and earlier and KVM, allows local guest users to cause a denial of service (out-of-bounds write and guest crash) or possibly execute arbitrary code via the (1) FD_CMD_READ_ID, (2) FD_CMD_DRIVE_SPECIFICATION_COMMAND, or other unspecified commands, aka VENOM.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:74640
- URL:http://www.securityfocus.com/bid/74640
- CONFIRM:http://git.qemu.org/?p=qemu.git;a=commitdiff;h=e907746266721f305d67bc0718795fedee2e824c
- CONFIRM:http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10693
- CONFIRM:http://support.citrix.com/article/CTX201078
- CONFIRM:http://www.fortiguard.com/advisory/2015-05-19-cve-2015-3456-venom-vulnerability
- CONFIRM:http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
- CONFIRM:http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-438937.htm
- CONFIRM:http://xenbits.xen.org/xsa/advisory-133.html
- CONFIRM:https://access.redhat.com/articles/1444903
- CONFIRM:https://bto.bluecoat.com/security-advisory/sa95
- CONFIRM:https://kb.juniper.net/JSA10783
- CONFIRM:https://kc.mcafee.com/corporate/index?page=content&id=SB10118
- CONFIRM:https://securityblog.redhat.com/2015/05/13/venom-dont-get-bitten/
- CONFIRM:https://support.lenovo.com/us/en/product_security/venom
- CONFIRM:https://www.suse.com/security/cve/CVE-2015-3456.html
- DEBIAN:DSA-3259
- URL:http://www.debian.org/security/2015/dsa-3259
- DEBIAN:DSA-3262
- URL:http://www.debian.org/security/2015/dsa-3262
- DEBIAN:DSA-3274
- URL:http://www.debian.org/security/2015/dsa-3274
- EXPLOIT-DB:37053
- URL:https://www.exploit-db.com/exploits/37053/
- FEDORA:FEDORA-2015-8249
- URL:http://lists.fedoraproject.org/pipermail/package-announce/2015-May/158072.html
- GENTOO:GLSA-201602-01
- URL:https://security.gentoo.org/glsa/201602-01
- GENTOO:GLSA-201604-03
- URL:https://security.gentoo.org/glsa/201604-03
- GENTOO:GLSA-201612-27
- URL:https://security.gentoo.org/glsa/201612-27
- HP:HPSBMU03336
- URL:http://marc.info/?l=bugtraq&m=143229451215900&w=2
- HP:HPSBMU03349
- URL:http://marc.info/?l=bugtraq&m=143387998230996&w=2
- HP:SSRT102076
- URL:http://marc.info/?l=bugtraq&m=143229451215900&w=2
- MISC:http://venom.crowdstrike.com/
- REDHAT:RHSA-2015:0998

- URL:http://rhn.redhat.com/errata/RHSA-2015-0998.html
- REDHAT:RHSA-2015:0999
- URL:http://rhn.redhat.com/errata/RHSA-2015-0999.html
- REDHAT:RHSA-2015:1000
- URL:http://rhn.redhat.com/errata/RHSA-2015-1000.html
- REDHAT:RHSA-2015:1001
- URL:http://rhn.redhat.com/errata/RHSA-2015-1001.html
- REDHAT:RHSA-2015:1002
- URL:http://rhn.redhat.com/errata/RHSA-2015-1002.html
- REDHAT:RHSA-2015:1003
- URL:http://rhn.redhat.com/errata/RHSA-2015-1003.html
- REDHAT:RHSA-2015:1004
- URL:http://rhn.redhat.com/errata/RHSA-2015-1004.html
- REDHAT:RHSA-2015:1011
- URL:http://rhn.redhat.com/errata/RHSA-2015-1011.html
- SECTRACK:1032306
- URL:http://www.securitytracker.com/id/1032306
- SECTRACK:1032311
- URL:http://www.securitytracker.com/id/1032311
- SECTRACK:1032917
- URL:http://www.securitytracker.com/id/1032917
- SUSE:SUSE-SU-2015:0889
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-05/msg00009.html
- SUSE:SUSE-SU-2015:0896
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-05/msg00042.html
- SUSE:SUSE-SU-2015:0923
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-05/msg00018.html
- SUSE:SUSE-SU-2015:0927
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-05/msg00019.html
- SUSE:SUSE-SU-2015:0929
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-05/msg00021.html
- SUSE:openSUSE-SU-2015:0893
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-05/msg00013.html
- SUSE:openSUSE-SU-2015:0894
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-05/msg00014.html
- SUSE:openSUSE-SU-2015:0983
- URL:http://lists.opensuse.org/opensuse-security-announce/2015-06/msg00001.html
- SUSE:openSUSE-SU-2015:1400
- URL:http://lists.opensuse.org/opensuse-updates/2015-08/msg00021.html
- UBUNTU:USN-2608-1
- URL:http://www.ubuntu.com/usn/USN-2608-1

Assigning CNA	
MITRE Corporation	
Date Entry Created	
20150429	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20150429)	
Votes (Legacy)	
Comments (Legacy)	
Proposed (Legacy)	
N/A	

Fuente: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3456

(Volver al texto)

Anexo #2: Modelos utilizados para la gestión de la seguridad de la información:

(Volver al texto)

Modelo, marco normativo, estándar, o buenas prácticas	**Descripción general**
Modelo de Negocio de Seguridad Informática (BMIS)	-Creado por la asociación ISACA. -Establece personas, procesos, tecnologías y organización como ejes fundamentales para la seguridad
Modelo ISO/IEC 27001	-Define lineamientos para implementar un SGSI, dominios y roles en la organización. -Incluye aspectos capacitación y concientización. -Incluye aspectos operativos de comunicación interna y externa.
COBIT	-Es una guía de mejores prácticas para la gestión de tecnología de la información (TI), sus principios, dominios, procesos y actividades. -Aunque no es orientada a gestión de seguridad, incluye aspectos de confidencialidad, integridad, disponibilidad, entre otros.
Modelo de Madurez de Gestión de Seguridad de la Información (ISM3)	-Provee un enfoque moderno de gestión de seguridad de la información para los sistemas de gestión de calidad, ISO 9001. -Puede resultar útil para apoyar la procesos de seguridad de información.
Modelo SOGP Estándar de Buenas Prácticas del Foro de Seguridad de la Información	-Elaborado por el Foro de Seguridad de la Información (ISF) en 2010, es una guía para la seguridad de la información del negocio. -Se divide en 4 categorías: gobierno de la seguridad, requisitos de seguridad, marco de control, seguimiento y mejora de la seguridad. -Pretende cubrir generalidades de estrategia de seguridad, gestión de incidentes, continuidad del negocio, recuperación y gestión de crisis.
Modelo de seguridad para redes de empresas (SAFE)	-Desarrollado por CISCO, enfocado a seguridad de redes informáticas. -Brinda mejores prácticas para el diseño e implementación de redes seguras y sus requisitos de seguridad. -Adopta un enfoque de defensa en profundidad para el diseño de la seguridad de las redes informáticas.
Otros: ITIL, PRINCE2, y TLLJO	-Incluyen aspectos de seguridad, gestión de proyectos, implementación de un SGSI, otros.

(Volver al texto)

Bibliografía

[1] K. Shirriff, «Iconic consoles of the IBM System/360 mainframes, 55 years old,» [En línea]. Available: http://www.righto.com/2019/04/iconic-consoles-of-ibm-system360.html. [Último acceso: 08 02 2019].

[2] GRABii, «GRABii,» [En línea]. Available: http://grabii.blogspot.com/2010/02/vmware-workstation-7-virtual-machine.html. [Último acceso: 08 02 2019].

[3] E. A. Marchionni y O. M. Formoso, «Virtualización con VMware, Lo mejor de la computación en la nube,» 1 ed., Buenos Aires, Fox Andina Dalaga, 2012, pp. 18,21,22,24,35,314.

[4] A. Tecnologia, «https://www.areatecnologia.com,» [En línea]. Available: https://www.areatecnologia.com/informatica/cloud-computing.html. [Último acceso: 15 01 2019].

[5] V. Inc, «¿Qué son la tecnología de virtualización y la máquina virtual? VMware AR,» VMware Inc, 2019. [En línea]. Available: https://www.vmware.com/ar/solutions/virtualization.html. [Último acceso: 15 01 2019].

[6] M. Corporation, «¿Qué es virtualización?,» Microsoft Corp, 2019. [En línea]. Available: https://azure.microsoft.com/es-es/overview/what-is-virtualization/. [Último acceso: 15 01 2019].

[7] R. H. Inc., «Understanding virtualization,» 2019. [En línea]. Available: https://www.redhat.com/es/topics/virtualization. [Último acceso: 15 01 2019].

[8] F. G. Pacheco y H. Jara, «Hackers al descubierto,» Banfield-Lomas de Zamora, Gradi, 2009, p. 178.

[9] M. Haag, «Infraestructura hiperconvergente para Dummies,» Hoboken-New Jersey, John Wiley & Sons Inc, 2018, pp. 7,8,29,30.

[10] Bios-ts, «¿Qué es VDI?,» Bios-ts, 2018. [En línea]. Available: http://www.bios-ts.es/wpcontent/uploads/2016/04/VDI.pdf. [Último acceso: 15 01 2018].

[11] R. a. markets, «Hyper-Converged Infrastructure (HCI) - Global Market Outlook (2017-2023),» 2019. [En línea]. Available: https://www.researchandmarkets.com/reports/4480633/hyper-converged-infrastructure-hci-global. [Último acceso: 18 01 2019].

[12] M. Inc., «Informática sin servidores,» 2019. [En línea]. Available: https://azure.microsoft.com/es-es/overview/serverless-computing. [Último acceso: 18 01 2019].

[13] Uv.mx, «Seguridad de la información,» 2019. [En línea]. Available: https://www.uv.mx/celulaode/seguridad-info/tema1.html. [Último acceso: 18 01 2019].

[14] P. A. López, «Seguridad informática,» de *Seguridad informática*, Madrid, Editex, 2010, p. 9.

[15] H. D. Scolnik, «Qué es la Seguridad Informática,» de *Qué es la Seguridad Informática*, Ciudad Autónoma de Buenos Aires, Paidós, 2014, p. 19.

[16] CiscoSecurityResearch, «Reporte Anual de Ciberseguridad 2018,» 2019. [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf. [Último acceso: 20 02 2019].

[17] E. Villanueva y V. Díaz, Derecho de las nuevas tecnologías (en el siglo XX derecho informático), Oxford UK: Oxford University Press, 2015.

[18] A. d. l. I. d. l. T. (TIA), Estándar de infraestructura de telecomunicaciones para centros de datos TIA-942, Arlington, VA 22201 U.S.A.: TIA STANDARDS AND ENGINEERING PUBLICATIONS, 2012.

[19] F. Portantier, «Gestión de la Seguridad Informática,» de *Gestión de la Seguridad Informática*, Ciudad Autónoma de Buenos Aires, Fox Andina,Dalaga, 2013, p. 130.

[20] M. Corporation, «Microsoft Azure,» Microsoft, 2019. [En línea]. Available: https://azure.microsoft.com/es-es/overview/what-is-virtualization/?cdn=disable. [Último acceso: 10 03 2019].

[21] GlobalLogic, «VIRTUALIZACIÓN != CLOUD COMPUTING,» GlobalLogic, 2019. [En línea]. Available: https://www.globallogic.com/latam/gl_news/virtualizacion-cloud-computing/. [Último acceso: 10 03 2019].

[22] AmazonWebServicesInc, «¿Qué es la seguridad en la nube?,» AmazonWebServicesInc, 2019. [En línea]. Available: https://aws.amazon.com/es/security/introduction-to-cloud-security/. [Último acceso: 15 03 2019].