Universitat Oberta de Catalunya

uoc.edu

La transformación del centro de datos. Seguridad en entornos virtualizados.

Alumno: Leopoldo Álvarez Huerta

TFM: Máster Universitario de Seguridad en las Tecnologías la Información y de las Comunicaciones (MISTIC)

Área: Hacking

Director: Pau del Canto Rodrigo

Fecha: Enero de 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*La transformación del centro de datos. Seguridad en entornos virtualizados.*
Nombre del autor:	*Leopoldo Álvarez Huerta*
Nombre del consultor/a:	*Pau del Canto Rodrigo*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	01/2021
Titulación:	*Máster Universitario en Seguridad de la Información y las Telecomunicaciones*
Área del Trabajo Final:	*Hacking*
Idioma del trabajo:	*Español*
Palabras clave	*Seguridad, cloud, malware*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados y conclusiones del trabajo.*

En esta última década, el número de dispositivos conectados a la red ha crecido exponencialmente, lo que ha obligado a evolucionar las infraestructuras que los soportan y proporcionan los servicios demandados. Los requisitos de accesibilidad, disponibilidad, seguridad y, en definitiva, la manera continua, y de forma remota, de explotar los servicios, han impactado directamente sobre los centros de datos.

Tecnologías ya consolidadas como la virtualización, sumada a otras tendencias tecnológicas como Cloud o Edge Computing, han generado una descentralización de los centros de datos, propiciando la creación de nuevos entornos, más cercanos a la información que se demanda, y más accesibles. Este modelo favorece el envío de la información a un único punto virtual, distribuyendo, en realidad, los datos en varios centros y consiguiendo una infraestructura distribuida, escalable, y flexible.

Esta transformación de los centros de datos, donde se aplican nuevas técnicas de virtualización, plantea la duda de si los actuales sistemas de seguridad son capaces de mitigar las amenazas y, por consiguiente, eliminar posibles brechas de seguridad.

En el aspecto teórico, este trabajo intenta demostrar que, aunque la seguridad sea un pilar en el diseño de cualquier tecnología, los sistemas de gestión de seguridad tradicionales no son suficientes para cubrir el paradigma de los nuevos centros de datos. Además, se analizan las nuevas soluciones integrales de seguridad que hay en el mercado. Por otro lado, se realiza un acercamiento práctico desarrollando y aplicando una guía de seguridad a un componente esencial de la virtualización como es el hipervisor.

Abstract (in English, 250 words or less):

Over the last decade, the number of devices connected to the network has grown exponentially, which has forced the infrastructures that support them and provide the services demanded to evolve. The accessibility, availability, security requirements and, ultimately, the continuous and remote way of exploiting the services, have had a direct impact on data centers.

Nowadays, consolidated technologies such as virtualization, added to other technological trends such as Cloud or Edge Computing, have generated a decentralization of data centers, pushing the creation of new environments, closer to the information that is demanded, and more accessible. This model favors the sending of information to a single virtual point but distributing the data in several centers and achieving a distributed, scalable, and flexible infrastructure.

This transformation of data centers, where the new virtualization techniques such network virtualization are applied, raises the question of whether current security systems are capable of mitigating threats and, consequently, eliminating possible security gaps.

In the theoretical aspect, this work tries to demonstrate that if although security is a pillar in the design of any technology, traditional security management systems are not enough to cover the paradigm of new data centers. In addition, the new comprehensive security solutions on the market are analyzed. On the other hand, a practical approach is done by developing and applying security measures to an essential component such as the hypervisor.

Índice

Lista de figuras

1. Introducción

En estos últimos años, al igual que en otras revoluciones tecnológicas o industriales, la sociedad está experimentando cambios significativos. El crecimiento exponencial de *gadgets* y *smartphones*; conectados continuamente a las diversas redes, fomentan la expansión del IoT y, en definitiva, IoE. Se suma, además, la llegada del 5G, las *smart cities* y *smart homes*, realizando una serie de cambios significativos, no solo a nivel personal del individuo sino también a nivel profesional y empresarial.

En el marco de esta nueva actualidad, las empresas intentan adaptarse de la mejor manera posible, optimizando las soluciones tecnológicas para ser lo más eficientes posibles a la hora de entregar servicios. Esta optimización, sobre todo en grandes empresas, pasa por llevar a cabo una transformación de los centros de datos, exprimiendo las posibilidades que ofrece Internet hoy en día. Actualmente, nuevas tecnologías como IoT, IoE, Cloud, Edge o Fog Computing, además del problema de consumo de energía y refrigeración, han propiciado dicha transformación.

Por lo tanto, el modelo que se conoce como tradicional va dejando sitio a otro tipo de entornos. Las empresas han ido migrando sus CPDs; basados en silos, con sobrecostes operativos, escalabilidad limitada, y con unos consumos de electricidad en contraposición con la tendencia de eficiencia energética, a la Cloud.

Este trabajo, denominado “Transformación del centro de datos: seguridad en entornos virtualizados”, pretende describir el recorrido de dicha transformación de los CPDs, y estudiar, del mismo modo que los entornos han ido transformándose, los ataques o amenazas de seguridad que también han evolucionado. Además, se hace hincapié en los productos y medidas de seguridad para este tipo de entornos virtuales, manteniendo los pilares de la seguridad de la información: autenticidad, confidencialidad, disponibilidad e integridad.

1.1 Contexto y justificación del Trabajo

En la última década, tal y como se ha indicado en la introducción del trabajo, se ha podido observar un cambio en los centros de datos. Los sistemas de información han evolucionado desde la virtualización clásica a la nube, gestionando grandes volúmenes de información. Este cambio se ha acelerado recientemente, recayendo parte de responsabilidad en empresas de gran envergadura y, aún más importante, con una contrastada madurez como

proveedores de Cloud Computing, por ejemplo; Amazon, Google o Microsoft. No obstante, muchas empresas siguen considerando que la estrategia de una Cloud privada o híbrida es necesaria, siendo esencial la persistencia de un centro de datos propio y con un entorno que cumpla los estándares actuales de eficiencia energética y seguridad; uno de los aspectos clave de este trabajo.

La seguridad en los centros de datos actuales, tal y como se puede ver en alguno de los informes de la consultora Gartner [1] , ha cobrado una mayor relevancia. Aspectos como el tratamiento de grandes volúmenes de datos y garantizar la privacidad de estos, sumado, a que existen ataques más específicos y sofisticados hace que sea un aspecto relevante para cualquier empresa u organización, por lo que las medidas de protección y herramientas necesarias de seguridad son básicas.

En la investigación previa al trabajo se ha identificado la necesidad de realizar un estudio de este tipo de medidas, es decir, las medidas de seguridad tanto en los entornos virtuales clásicos como en los nuevos entornos híbridos de *cloud* local y pública, así como el análisis de las soluciones comerciales de proveedores de seguridad, haciendo foco en el *malware* y *antimalware* en este tipo de entornos.

Actualmente, tal y como se puede ver en la Figura 1, la mayoría de las empresas emplean la virtualización, sin embargo, las medidas de seguridad se han ido heredando de soluciones tradicionales como antivirus e IPSs o *firewalls* físicos.

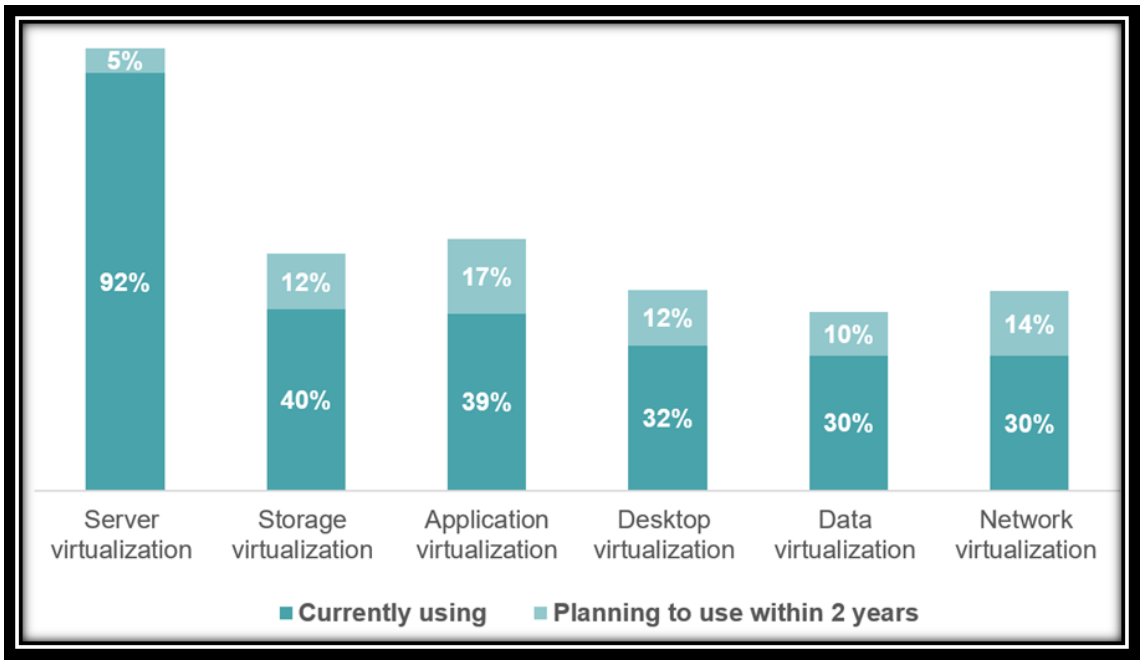


Figura 1: The 2020 State of Virtualization Technology [2]

Existen en el mercado soluciones de seguridad para entornos virtuales, así como medidas específicas para prevenir ataques o acotar su impacto, por ejemplo, con microsegmentación de los *switches* virtuales, analizadores de tráfico, securización del hipervisor o configuración de una *sandbox.*

En este marco se desarrolla este trabajo; aportando y analizando las diferentes soluciones actuales y detallando medidas específicas de securización de entornos virtuales, con el propósito de marcar unas pautas o guía para securizar este tipo de entonos desde el hipervisor hasta un entorno completo de nube privada o híbrida.

1.2 Objetivos del Trabajo

Los objetivos de este proyecto son:

I. Establecer un contexto o marco histórico de la evolución de los sistemas de información y los centros de datos
II. Definir y detallar la arquitectura de un entorno de virtualización. La transformación del CPD
III. Realizar un análisis de nuevas amenazas en entornos virtualizados y *cloud*
IV. Elaborar un estudio de las ventajas y desventajas, haciendo foco en la seguridad, de la transición de los entornos convencionales a entornos virtualizados.
V. Realizar un estudio de mercado de soluciones de seguridad en entornos virtualizados. Comparar dichas soluciones con las tradicionales.
VI. Implementar y desarrollar una prueba de concepto. Securización del hipervisor

1.3 Enfoque y método seguido

El objetivo principal de este trabajo es realizar un estudio de mercado de las soluciones de seguridad disponibles en los entornos virtuales actuales, haciendo foco en el antimalware, además de analizar las amenazas inherentes en este tipo de entornos virtualizados.

En primer lugar, se realiza una introducción a los entornos virtualizados clásicos, entornos Cloud, y NFV/SDN; de cara a introducir conceptos actuales donde la securización de los entornos es aún más necesaria.

En segundo lugar, dentro de la pila de un entorno virtual, se describe como *hardenizar* un hipervisor, es decir, la securización de uno de los pilares del entorno virtualizado.

Por último, al hilo del objetivo principal del proyecto, se realiza un estudio de las ventajas y desventajas de los entornos virtuales, así como las amenazas genéricas y específicas que surgen con estos entornos, realizando un estudio de mercado de las soluciones de seguridad específicas en entornos virtuales, comparando estas con las tradicionales y analizando conceptos como EPP, EDR, etc. Es decir, además del acercamiento teórico se realiza una aproximación práctica que consiste en realizar el despliegue y una guía para la securización de un hipervisor como es el ESXi de VMware, así como detalle y referencias para el despliegue de una *sandbox*.

Por lo tanto, la propuesta de trabajo se desarrolla dentro del marco de un proyecto de investigación y análisis cuya finalidad es profundizar en la seguridad de los entornos virtualizados, es decir, realizar un estudio de los cambios que han sufrido los sistemas de información con la llegada de nuevas tecnologías de virtualización y, con ello, nuevas amenazas en forma de *malware*. Esta última premisa, aunque previa al estudio del TFM, se basa en la experiencia y el conocimiento; los entornos virtualizados, sólo por el hecho de ser virtuales, no son inmunes a los ataques de software malicioso.

De cara a cumplir los objetivos del proyecto planteados en el punto anterior, y realizar una correcta planificación, se diferencian varias fases que incluyen, entre otros, los siguientes puntos:

- Fase de estudio e investigación
    - Evolución de la virtualización; virtualización clásica, Cloud y virtualización de red.
    - Ventajas y desventajas referentes a la seguridad
    - Nuevas amenazas ligadas a las nuevas tecnologías y entornos
    - Tecnologías de virtualización de red NFV/SDN; transformación del CPD
    - Evolución de las soluciones de seguridad entornos tradicionales y entornos virtualizados.
    - Análisis de mercado soluciones de seguridad en entornos virtuales
    - El hipervisor; tipos y prácticas de securización
- Fase de implantación o caso práctico
    - Instalación, configuración y despliegue de un nodo basado en un *hypervisor*.
    - Securización del *hypervisor*.
    - PoC solución seguridad en entornos virtuales
- Fase de documentación
    - Elaboración de documentación; PECs, memoria, presentación
    - Guía de *hardening* de un hipervisor ESXi.

- Fase de control y seguimiento
    - Evaluación PECs
    - Interlocución con el tutor del TFM

1.4 Planificación del Trabajo

La distribución de las tareas globales del proyecto consistirá en los apartados que se detallaran a continuación, cuyo desglose en la estructura de descomposición del trabajo (EDT) se estima en 225 horas equivalentes a un TFM de 9 créditos.
El proyecto está marcado principalmente por cuatro hitos o entregas:

I. **Primer hito o PEC1:**
    a) Propuesta, descripción, objetivos y planificación del proyecto
    b) Estudio y bases para el Estado del Arte
    c) Entregable PEC1 29/09/2020

II. **Segundo hito o PEC2:**
    a) Estado del arte
    b) Ventajas y desventajas relativas a la seguridad en entornos clásicos vs virtualizados vs virtualizados nueva generación
    c) Posibles problemas y soluciones
    d) Análisis de soluciones de seguridad integrales en entornos virtuales
    e) Entregable PEC2 27/10/2020

III. **Tercer hito o PEC3:**
    a) Detalle arquitectura de un entorno virtual de nueva generación
    b) Estudio detallado del hipervisor
    c) Acercamiento práctico:
        a. Seguridad en entornos virtuales; concepto *sandbox*
        b. Securización de un hipervisor
    d) Entregable PEC3 24/11/2020

IV. **Cuarto hito o PEC4:**
    a) Finalización y revisión del acercamiento práctico: securización hipervisor y configuración *sandbox*
    b) Cierre de la memoria técnica
    c) Elaboración de contenido multimedia y presentaciones
    d) Entregable PEC4 29/12/2020
    e) Entregable TFM 05/01

Este apartado se ha elaborado a través de la aplicación MS Project Professional 2016, de la que se adjuntan dos figuras; una del EDT y otra del diagrama de

Gantt, a alto nivel por cuestiones de visibilidad. El resto del detalle de la planificación se encuentra en el Anexo I de esta memoria.

El TFM se ha planificado teniendo en cuenta el inicio en septiembre de 2020, concretamente el 22 de septiembre, y concluyendo el 15 de enero de 2021 tras la defensa de este.

Se estima una duración temporal de 84 días, incluyendo el tiempo disponible entre entrega final y defensa, lo que da un resultado de 81 días útiles con una dedicación parcial de 2,7 horas, lo que da un resultado de las 225 horas indicadas anteriormente. Se distribuye de esta forma utilizando un calendario estándar.

TFM - Transformación del DC. Soluciones de seguridad en entornos virtualizados	**84 días**	**mar 22/09/20**	**vie 15/01/21**		**Leopoldo Álvarez**
Planificación del proyecto	**5,5 días**	**mar 22/09/2**	**mar 29/09/20**		
Propuesta de proyecto	2 días	mar 22/09/2	mié 23/09/20		Leopoldo Álvarez
Descripción del proyecto	1 día	jue 24/09/20	jue 24/09/20	3	Leopoldo Álvarez
Objetivos del proyecto	1 día	vie 25/09/20	vie 25/09/20	4	Leopoldo Álvarez
Contexto y base para estado del arte	1 día	lun 28/09/20	lun 28/09/20	5	Leopoldo Álvarez
EDT y diagrama de GANT	0,5 días	mar 29/09/2	mar 29/09/20	6	Leopoldo Álvarez
Entregable PEC1	0 días	mar 29/09/2	mar 29/09/20	7	Leopoldo Álvarez
Investigación	**20 días**	**mar 29/09/2**	**mar 27/10/20**		
Estado del arte	5 días	mar 29/09/2	mar 06/10/20	2	Leopoldo Álvarez
Ventajas y desventajas entornos clásicos vs virtualizados	5 días	mar 06/10/20	mar 13/10/20	10	Leopoldo Álvarez
Posibles problemas y soluciones: nuevas amenazas	3 días	mar 13/10/20	vie 16/10/20	11	Leopoldo Álvarez
Seguridad en entornos virtuales; concepto sandbox	2 días	vie 16/10/20	mar 20/10/20	12	Leopoldo Álvarez
Análisis de soluciones de seguridad en entornos virtuales	3 días	mar 20/10/20	vie 23/10/20	13	Leopoldo Álvarez
Securización de un hypervisor	2 días	vie 23/10/20	mar 27/10/20	14	Leopoldo Álvarez
Entregable PEC2	0 días	mar 27/10/2	mar 27/10/20	15	Leopoldo Álvarez
Arquitectura de un entorno virtual	**8 días**	**mar 27/10/2**	**vie 06/11/20**		
Diseño físico	3 días	mar 27/10/2	vie 30/10/20	9	Leopoldo Álvarez
Diseño lógico	3 días	vie 30/10/20	mié 04/11/20	18	Leopoldo Álvarez
Stack virtual: El hypervisor	2 días	mié 04/11/2	vie 06/11/20	19	
Implantación y despliegue: Caso práctico	**12 días**	**vie 06/11/20**	**mar 24/11/20**	17	
Soporte digital	**30 días**	**mar 24/11/2**	**mar 05/01/21**	**21**	
Memoria TFM (entrega PEC4)	25 días	mar 24/11/2	mar 29/12/20		Leopoldo Álvarez
Contenido multimedia: Video y presentació	5 días	mar 29/12/2	mar 05/01/21	33	Leopoldo Álvarez
Análisis licencias / subscripciones / prespuesto	1 día	vie 23/10/20	lun 26/10/20	14	Leopoldo Álvarez
Entrega TFM	0 días	mar 05/01/2	mar 05/01/21	34	Leopoldo Álvarez

Figura 2: Estructura desglose de tareas EDT

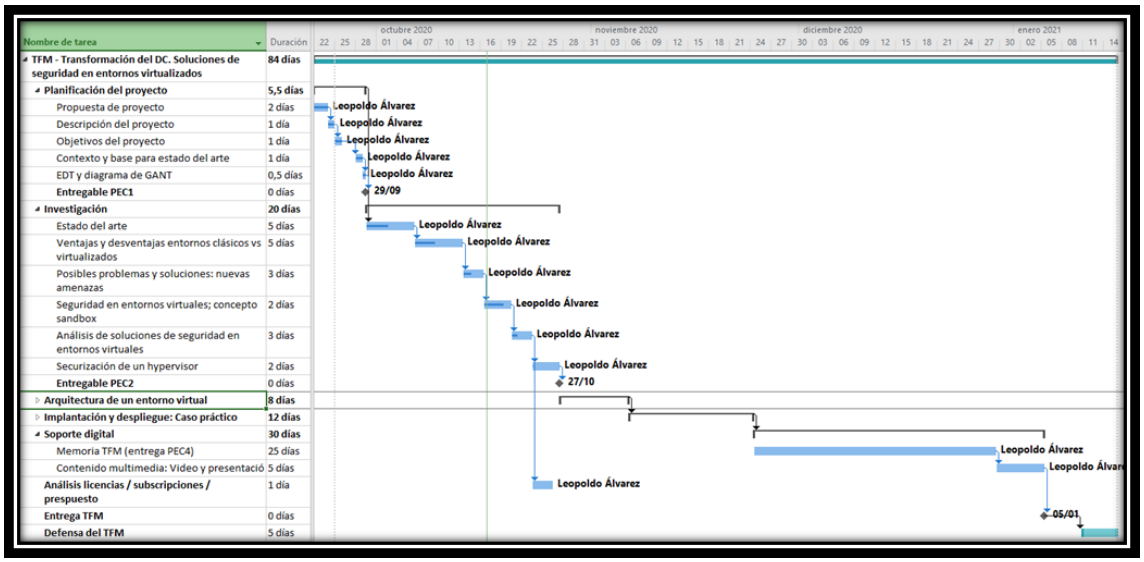


Figura 3: Planificación alto nivel

1.5 Breve sumario de productos obtenidos

Los productos obtenidos, los cuales se detallan en apartados posteriores, se basan en el análisis de la evolución de los entornos virtuales y la seguridad en los mismos. Se ha identificado una carencia en el aspecto de la seguridad, ya que se detecta que el crecimiento de la virtualización en las empresas no ha ido de la mano de la securización de este tipo de entornos.

Algunos de los productos resultado de este trabajo son:

- Diseño físico y lógico de un sistema de virtualización. Detalle de una arquitectura virtual de referencia.
- Análisis de la transformación de los centros de datos. Acercamiento teórico a tecnologías como Cloud computing, NFV, y SDN.
- Diseño funcional de una solución antimalware en entornos virtualizados. Tipos de protección, EDRs y EPPs.
- Presentación de soluciones de seguridad en entornos virtuales. Despliegue de un hipervisor ESXi de VMware.
- Guía de securización de un hipervisor. Aplicación caso práctico.
- Recomendaciones de despliegue y configuración de una *sandbox*.

1.6 Breve descripción de otros capítulos de la memoria

En los siguientes capítulos se desarrollan las diferentes fases por las que transcurre el trabajo, que finaliza, con las conclusiones obtenidas durante la ejecución de este.

- **Capítulo dos.** Estado del arte. Se detalla la evolución en los sistemas de información. Desde la virtualización clásica hasta la foto actual del modelo de servicios basados en la nube o Cloud Computing y los cambios relacionados con las medidas de seguridad.

- **Capítulo tres.** La transformación del centro de datos: Virtualización y seguridad. En este capítulo se detalla la información que, en parte, da nombre al título del trabajo. Detalle técnico de cómo ha ido evolucionando la virtualización, con nuevas tecnologías como la virtualización de red; SDN, NFV, definiendo la arquitectura de un entorno virtual de nueva generación. Se describen otras tendencias tecnológicas, y como se han ido adaptando los sistemas de seguridad.
- **Capítulo cuatro.** Sistemas de gestión seguridad. Se realiza un estudio de mercado de soluciones de seguridad en entornos virtuales. Describiendo amenazas que han surgido en este tipo de entornos y medidas para evitar o minimizar.
- **Capítulo cinco.** Caso práctico. Implantación, despliegue y securización. En este capítulo se detalla la instalación de un hipervisor como es ESXi, así como su configuración y *hardening.* Además, se incluyen referencias para desplegar una *sandbox* en otro tipo de hipervisor; Virtual Box.
- **Capítulo seis.** Conclusiones y trabajo futuro. Se exponen las conclusiones obtenidas durante la ejecución del trabajo, los hitos conseguidos, y un posible enfoque sobre las opciones de siguientes trabajos en el área.

2. Estado del Arte

En la sociedad de la información se experimenta tanto el auge de nuevas tecnologías emergentes como la desaparición de otras consolidadas. Aunque la tecnología de virtualización lleva varias décadas entre nosotros, ha sido en esta última década cuando se ha experimentado un nuevo ciclo de vida o regeneración, evolucionando y extendiéndose la virtualización de los sistemas hacia la virtualización de los puestos de trabajo o de los centros de datos, entrelazando o fusionándose con tecnologías conocidas como Cloud, Edge o Fog Computing [3] [4], [5].

Desde el inicio en 1960 de las computadoras mainframe, también conocidas como "Big Iron"[6] ; computadoras utilizadas principalmente por grandes organizaciones para aplicaciones críticas: procesamiento de datos masivos, como censos o estadísticas industriales, la tecnología de virtualización ha ido evolucionando hasta nuestros días. Dicha tecnología es definida por VMware [7], uno de los proveedores principales de virtualización, de la siguiente manera: “La virtualización consiste en crear una representación basada en software, o virtual, de una entidad física como, por ejemplo, aplicaciones, servidores, redes y almacenamiento virtuales. Es la forma más eficaz de reducir los gastos de TI y, a la vez, aumentar la eficiencia y la agilidad para empresas de cualquier tamaño.”

La virtualización, buscando una definición más técnica, consiste en abstraer el componente físico o hardware, del aplicativo o software instalando sistemas operativos de forma virtual (VMs o Guest OS) sobre otro sistema denominado anfitrión o hipervisor, instalado a su vez sobre un servidor físico o *host*. Esta tecnología proporciona una mayor flexibilidad a la hora de desplegar diferentes sistemas, de forma aislada, aprovechando el hardware virtual parametrizable, como del host físico; CPU, memoria, red, discos, etc. Sin olvidar otras ventajas como escalabilidad, rendimiento y disponibilidad de recursos. Estas ventajas han dado como resultado la amplia adopción de las tecnologías de virtualización en las infraestructuras de computación en la nube, constituyendo un bloque fundamental en la misma.

Los hipervisores, que son los principales responsables de presentar esta capa virtualizada del *hardware* a las máquinas virtuales o contenedores, son uno de los componentes de *software* cruciales para el funcionamiento exitoso de la infraestructura en la nube. A pesar del falso mito o creencia de que un entorno virtual aislaba los componentes del exterior, los últimos informes de investigación han indicado que las capas de virtualización, entre ellas el hipervisor, pueden ser fácilmente identificadas para explotar las vulnerabilidades y comprometer la infraestructura informática de manera parcial o completa. Se han demostrado

muchos ataques no intrusivos y sigilosos dirigidos a estas capas, que tienen el potencial de causar daños importantes a la infraestructura o derivar en una fuga masiva de información [8].

Este estudio intenta destacar los problemas, vulnerabilidades y posibles ataques focalizados en la pila virtual. El siguiente apartado 3. La evolución del centro de datos: Virtualización y seguridad realiza un recorrido por la transformación del centro de datos; desde los tipos de virtualización clásica a los centros de datos definidos por *software,* adaptados para la utilización de tecnologías de nueva generación como NFV y SDN. Además, se presentan al lector conceptos, técnicas y una descripción general de las tecnologías de virtualización de VMware, *hardware* soportado, haciendo foco en componentes esenciales para este trabajo como su hipervisor; el ESXi, y NSX. Dicho apartado también proporciona una introducción a la seguridad en entornos virtuales, así como las amenazas inherentes en este tipo de entornos, ya que se ha introducido un nuevo conjunto de amenazas a la seguridad de cierta relevancia. Muchas de estas amenazas son únicas en entornos virtualizados y no son pertinentes en los escenarios informáticos tradicionales. Por lo tanto, estas amenazas han sido menos estudiadas y, en consecuencia, no se han abordado de la misma manera por la mayoría de los proveedores de aplicaciones de seguridad. Por esta razón, es importante analizar cuidadosamente las diversas amenazas que surgen en los diferentes componentes de la virtualización y así crear soluciones de manera efectiva para defender los sistemas contra ellas.

Estas amenazas a la seguridad podrían surgir como resultado del uso de arquitecturas no certificadas por fabricante, tecnologías relativamente más novedosas, bajo el paraguas de XaaS (Everything as a Service), que facilitan el aislamiento y los modelos informáticos impulsados por servicios en la nube, y mala praxis en la configuración del hipervisor o VMM. No obstante, este último, es un componente que necesario para coordinar el ciclo de vida de la VM, que puede ser, también, propensa a errores de *software*.

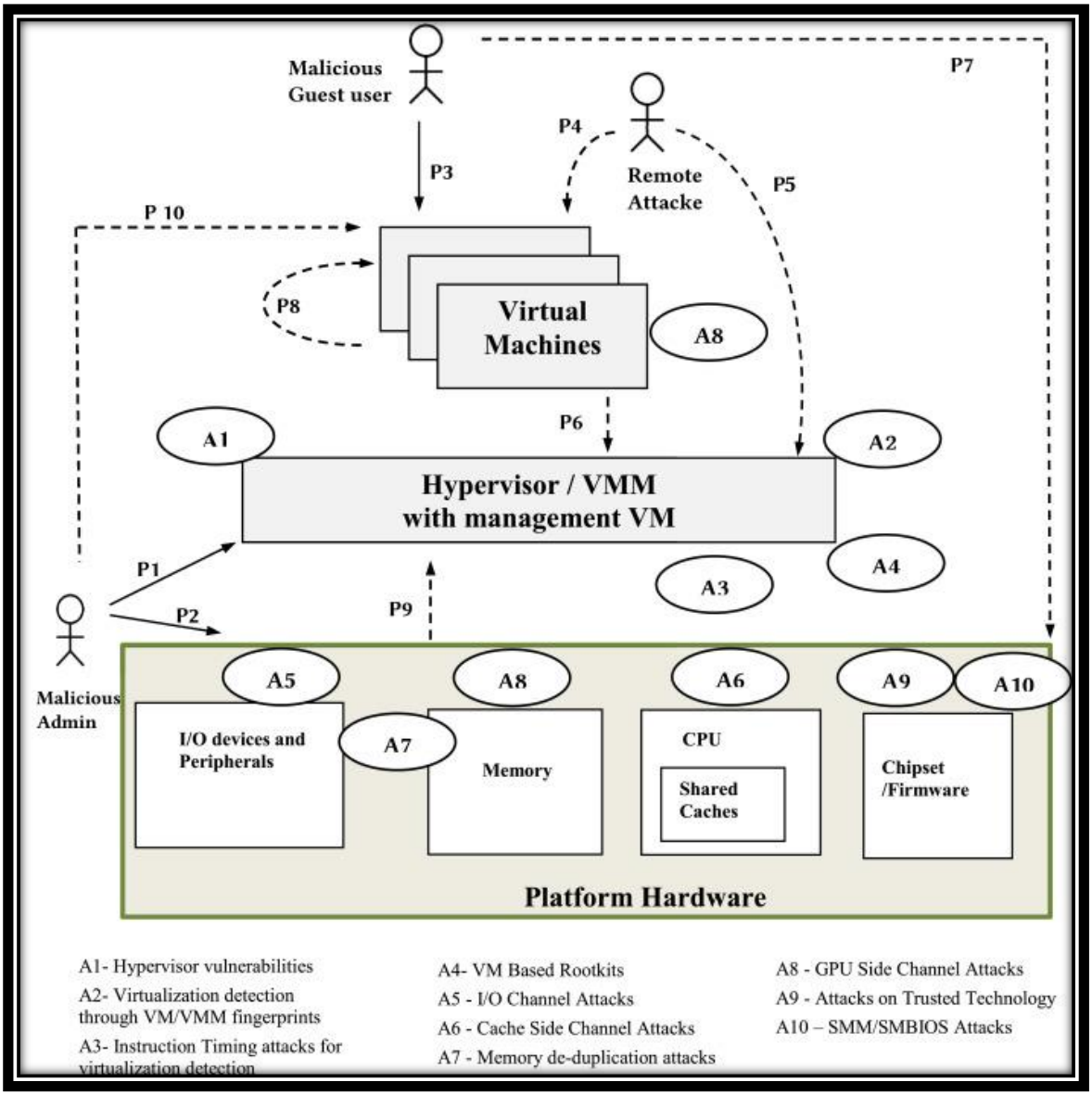


Figura 4: Rutas y grupos de ataque (Ax). [1]

Tal y como se puede ver en diferentes trabajos de investigación; “Security in hardware assisted virtualization for cloud computing [9]”, “Security Threats and Deployment Models [10]”, existen un gran número de vulnerabilidades reportadas y se hace necesario agrupar las mismas en múltiples familias. Por ejemplo, según la semántica del ataque y los componentes tecnológicos involucrados, como se puede ver en la Figura 4 extraída del primer artículo de investigación reseñado. Las flechas de puntos, numeradas de P4 a P10, representan las posibles rutas de ataque en el entorno. Un atacante remoto puede acceder directamente al hipervisor o a una máquina virtual; rutas P5 y P4. Por otro lado, un usuario invitado malintencionado que haya accedido a una VM podría abstraerse de la misma y acceder al hipervisor, representado por P6. Otras rutas,

[1] Security in hardware assisted virtualization for cloud computing
https://ars.els-cdn.com/content/image/1-s2.0-S1389128618302998-gr3.jpg

como la P8 representa el escenario de ataques cross VM o movimientos laterales, muy presentes en los *ransomware* actuales como Ryuk o Emotet. La ruta P9 representa el caso de *rootkits* y ataques de f*irmware* en *hardware* a través de los cuales, nuevamente, el hipervisor puede verse comprometido y ser manipulado con fines maliciosos. P3 y P10 representan accesos de usuarios con diferentes roles, bien por robo de credenciales u otro ataque conocido, de ahí la importancia de implementar un modelo de acceso Zero-trust, otro eslabón débil en la cadena de muchas organizaciones actualmente.

Volviendo al A1 de la Figura 4, el acceso al hipervisor es un objetivo perseguido en la mayoría de los ataques actuales, debido a que este se ejecuta en modo privilegiado en los *hosts.* Al ser un componente de *software*, accesible por diferentes protocolos IP, el hipervisor es un objetivo constante para explotar errores y vulnerabilidades existentes en el código de implementación. Una brecha de seguridad en el hipervisor puede tener serias implicaciones. Las vulnerabilidades en esta capa pueden hacer que un atacante acceda como un usuario invitado, pero escale privilegios o pueda realizar ejecución de código arbitrario provocando una denegación de servicio, afectando a todas las máquinas virtuales que corriesen sobre el mismo. Cabe indicar que estas máquinas virtuales, que pueden ser multitud según el servicio y los recursos del *host,* pueden ser propiedad de diferentes usuarios, compañías, departamentos, etc. Actualmente, aunque existen este tipo de ataques, se conoce que el fin económico del atacante es primordial, lo que puede llevar a este a obtener privilegios en la máquina *host* para provocar robo de datos o ejecutar un cifrado de los sistemas con el objetivo de la recompensa económica.

La certificación y verificación del código de los hipervisores se convierte en un reto para los fabricantes, debido a que el código base tiene un tamaño considerable y constantemente creciente debido a las nuevas funcionalidades requeridas. Por poner un ejemplo, el hipervisor Xen[2] actual tiene más de 400.00 líneas de código, similar el ESXi de VMware o KVM de RedHat. Este volumen de líneas de código es un problema a la hora de realizar las pruebas pertinentes de verificación, además, los drivers que integran según el *hardware* complican aún más el proceso. Por lo tanto, parece imposible actualmente disponer de un hipervisor sin vulnerabilidades.

Cada fabricante de virtualización dispone de su hipervisor, como se detalla en el apartado “3.3.6 Capa de virtualización: El hipervisor”, y aunque sea haya seleccionado el ESXi de VMware para el estudio de este trabajo, se ha analizado, como se puede observar en la Figura 5, que todos los hipervisores del mercado

[2] https://www.openhub.net/p/xenproject-hypervisor/analyses/latest/languages_summary

presentan vulnerabilidades conocidas. Se ha realizado una pequeña muestra representativa de varias vulnerabilidades altas y críticas en ESXi, XEN y KVM.

CVE ID	Score	VVM Type	Vulnerability Type(s)	CWE ID	Complex.
CVE-2013-1405	10	ESXi	DoS Exec Code Mem. Corr.	287	L
CVE-2013-3658	9.4	ESXi	Dir. Trav.	22	L
CVE-2013-3658	9.3	ESXi	DoS Exec Code Mem. Corr.	22	M
CVE-2012-1517	9.0	ESXi	DoS Exec Code Mem. Corr.	119	L
CVE-2012-1517	9.0	ESXi	DoS Exec Code Mem. Corr.	119	L
CVE-2017-10912	10	XEN	NA		L
CVE-2017-10918	10	XEN	NA	119	L
CVE-2017-10920	10	XEN	DoS Overflow	119	L
CVE-2017-10921	10	XEN	DoS Overflow	476	L
CVE-2017-10917	9.4	XEN	DoS +Info	125	L
CVE-2010-2784	6.6	KVM	DoS +Priv	20	M
CVE-2013-3658	6.6	KVM	DoS +Priv	264	M

Figura 5: Extracto parcial vulnerabilidades conocidas ESXi, XEN y KVM

El CWE ID es el grupo de debilidades de seguridad al que pertenecen, donde se encuentran comúnmente otros componentes, mientras que el “VVM typpe” es el modelo de hipervisor y “Complex.” la complejidad: L– baja y M – Media. El hecho de que muchas de las vulnerabilidades reportadas tengan una complejidad de ataque marcada como baja, indica que los hipervisores pueden convertirse en objetivos fáciles para el atacante, además de lo comentado anteriormente. Por otro lado, un número bajo o alto de vulnerabilidades no implica únicamente la ausencia o presencia de errores, se debe cruzar esta información con el tipo de producto, si es de código abierto o cerrado, por experiencia, existe la posibilidad de que el proveedor, en soluciones de código cerrado, solvente los errores sin que se informe.

Attack family	Suggested countermeasures	Remarks / challenges
Virtualization detection (A2, A3)	Hardening and patching of the hypervisor	Can prevent VM detection through fingerprints
	Time cheating [27]	Can prevent VM detection through timing analysis
Virtual machine based rootkits (A4)	Signature analysis of malware [118], [119]	Can work only with known signatures. Intelligent malware can escape
	VM detection [13], [120]	Can help only in detecting VMBR presence
	Use of trusted execution technologies	Can prevent VMBRs. Known breaches exist
	Firmware protection [29]	Can prevent VMBRs. Known breaches exist
Hypervisor vulnerabilities (A1), I/O channel attacks (A5)	Hardening and regular patching of the hypervisor	Regular exercise to be carried out by cloud admin
	Avoiding hypervisor itself [113]	Only a research solution. Commercially no implementation available

Figura 6: Resumen de contramedidas sugeridas. [3]

Tras este estudio se proponen varios enfoques para fortalecer la capa de virtualización, debido a la cantidad de vulnerabilidades que se identifican. Sin embargo, al igual que cualquier otro componente de *software* crítico en una infraestructura tradicional, el hipervisor o cualquier otro componente de esta capa deberá actualizarse y ser parcheado constantemente, algo que el día a día y las necesidades del servicio demuestran que no se realiza al ritmo que se requiere. Algunas de las investigaciones analizadas, por ejemplo: "Securing Cloud Hypervisors: A Survey of the Threats, Vulnerabilities, and Countermeasures" [11], también ha estudiado la importancia del hipervisor y sus vulnerabilidades, haciendo foco en la fuga de datos y la debilidad en el canal de autenticación.

En resumen, la virtualización es fundamental en el Cloud Computing, ya que reduce la utilización de *hardware*, ahorra energía y costes, y hace posible la

[3] Table 6. Summary of suggested countermeasures and their issues. https://doi.org/10.1016/j.comnet.2019.01.013

ejecución de múltiples aplicaciones, facilitando además la descentralización y el acceso remoto y, de manera continua, a la información. Son tecnologías complementarias y no son intercambiables. Algunas organizaciones han comenzado virtualizando sus servidores y luego adoptando el *cloud* para lograr una mayor agilidad y capacidad de gestión o autoservicio. De ahí que las empresas que ya tenían su parque de sistemas virtualizado, de forma completa o parcial, han sabido entender y aprovechar esta tecnología de una manera muy diferente, en lo que a impacto y eficiencia se refiere.

Además, el nacimiento de otras tendencias como NFV y SDN han acelerado la transformación del centro de datos, tal y como se conocía hasta ahora. Al igual que pasó hace unos años con el Cloud Computing, términos como Network Virtualization (NV), Software Defined Networks (SDN) y Network Function Virtualization (NFV) copan diversos congresos, webinars, y porfolios de proveedores de servicios Cloud o de Internet. Empresas de redes, virtualización, y hardware, se han volcado en estas tecnologías ofreciendo soluciones en uno o varios de estos campos. La aplicación de estas tecnologías emergentes, y complementarias, cambia completamente el escenario de las administraciones públicas, de las grandes y medianas empresas, en especial, de los proveedores de servicios digitales y Internet.

La heterogeneidad y complejidad de este escenario hace que la inteligencia artificial (IA) y el *machine learning* sean necesarios en el campo transversal de la seguridad. Tal y como se puede ver alguno de los últimos informes CCN-CERT [12] sobre tendencias, los ataques son cada vez más organizados, siendo algunos de los grupos más activos: Snake, APT27, Sofacy, etc., y el *ransomware,* como se ha indicado anteriormente, el tipo de código o *malware* más dañino en la última década.

En los últimos años, las acciones de este tipo de *malware* han pasado de ser una amenaza en equipos personales a ser un quebradero de cabeza para cualquier empresa, evolucionando el código con el objetivo de cifrar el mayor volumen de equipos posible. El crecimiento de este *software* malicioso y sus variantes ha derivado a lo que se conoce como RaaS o Ransomware as a Service, servicio por el cual los atacantes facilitan el despliegue a cambio de un porcentaje en la retribución económica que se consiga.

Según el objetivo del ataque, este puede ser masivo o dirigido, teniendo como objetivo comprometer un único equipo final, por ejemplo, una MV sobre un hipervisor afectado por alguna vulnerabilidad referenciada anteriormente. Este aspecto, sumado al desarrollo de código dañino avanzado, ha forzado a que los fabricantes de soluciones de seguridad hayan evolucionado sus productos,

acuñando términos como NGFW o NGAV; *firewall* de nueva generación y antivirus de nueva generación, respectivamente. No obstante, insuficiente para proteger ciertos tipos de entornos, de ahí la revisión en el trabajo de las últimas soluciones de EPP, EDR y XDR, las cuales utilizan *machine learning* para estudiar comportamientos normales y anómalos dentro de la red de cada organización, con capacidad de respuesta, de evolución y, por consiguiente, de mejora.

Por lo tanto, este estudio se puede utilizar para comprender las posibles rutas de ataque y, además, intentar mitigarlas mediante la aplicación de las medidas de seguridad que se analizan; tanto de un hipervisor, como de soluciones específicas de seguridad en entornos virtuales.

3. La evolución del centro de datos: Virtualización y seguridad

3.1 Tipos de virtualización

Una vez se conoce el concepto de virtualización, para entender la evolución de dicha tecnología, se deben explicar los tipos de virtualización, y como se ha evolucionado desde una virtualización clásica representada en la Figura 7, a una extensión de la virtualización en el mundo empresarial, fundamental para la consolidación del Cloud Computing.

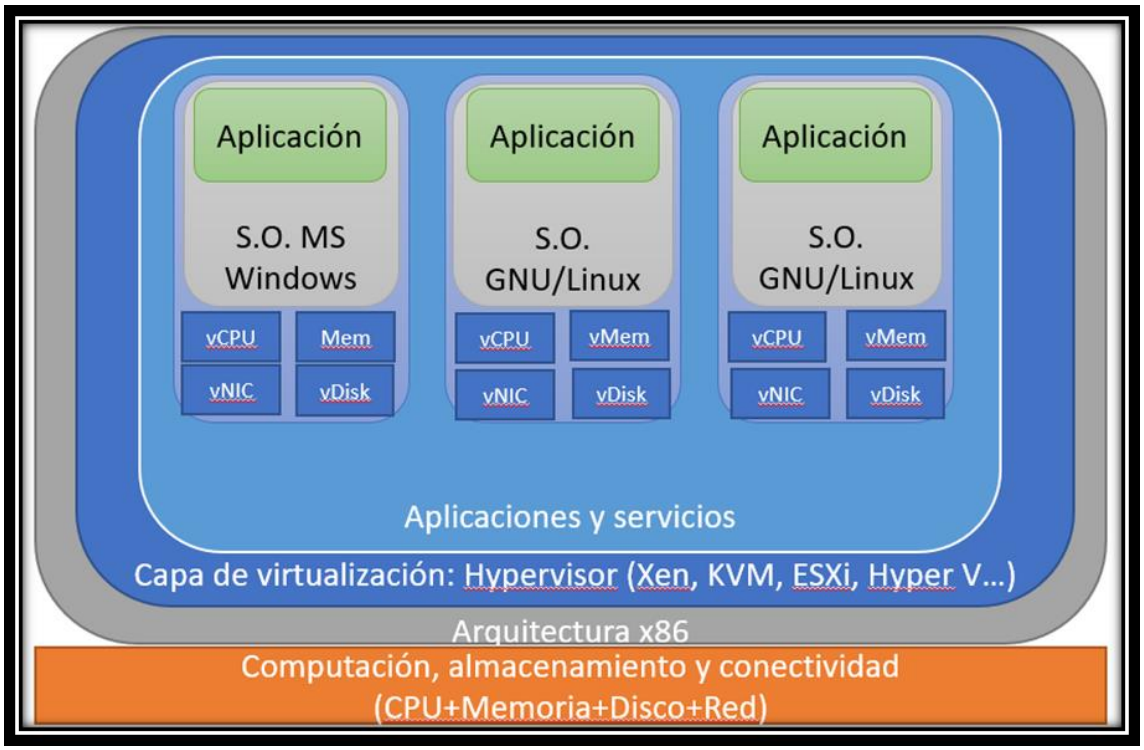


Figura 7: Arquitectura virtual clásica

Los tipos de virtualización componen una tecnología que continúa transformando el mapa de TI cambiando la forma en que las empresas gestionan y utilizan sus recursos tecnológicos. Entre otros, se pueden indicar los siguientes tipos de virtualización:

- **Virtualización de servidores.** La virtualización de servidor es la técnica más extendida o de mayor difusión. El objetivo principal es el de combinar muchos servidores en un servidor físico para que el procesador u otros recursos, como la memoria, puedan ser utilizados de una manera más eficiente. El sistema operativo que se ejecuta en un servidor físico se convierte en un sistema anfitrión, denominado hipervisor, donde se ejecutan otros sistemas operativos. Este hipervisor controla el procesador, la memoria y otros

componentes permitiendo que diferentes sistemas operativos se ejecuten en la misma máquina sin necesidad de un código fuente específico.

- **Virtualización de escritorios.** Mediante esta técnica se permite acceder de forma remota para poder trabajar desde cualquier lugar con acceso securizado y/o en cualquier PC. Dicha técnica proporciona una gran flexibilidad para que los empleados trabajen desde cualquier dispositivo que pueda acceder al escritorio virtual, protegiendo los datos confidenciales contra pérdidas o robos al encontrarse en servidores centrales, por normal general, con más medidas de protección o seguridad.
- **Virtualización de almacenamiento.** Mediante esta técnica diversos recursos de almacenamiento de red se utilizan como si fueran un único dispositivo de almacenamiento tipo vSAN, permitiendo una gestión más fácil y eficiente de estos recursos. Este tipo de virtualización mejora de la gestión del almacenamiento en un entorno de TI heterogéneo e intenta reducir el tiempo de inactividad.
- **Virtualización de red.** La virtualización de red es la técnica que más evolución ha tenido en los últimos años. Consiste en gestionar la administración y monitorización de una red desde un punto único de control, es decir, como sí la red se administrase desde una sola consola de administración, basada en software y no en un equipo tradicional de red. El objetivo principal es el de optimizar la red; reduciendo la tasa de transferencia de datos innecesarios, mejorando la escalabilidad, fiabilidad, flexibilidad y, además, seguridad.

3.2 Principio del cambio: Virtualización de la red

Las empresas y organismos que llevan varios años utilizando tecnologías de virtualización son conscientes de lo que es una red virtual, ya que independientemente de la tecnología de virtualización que utilicen, deberán haber gestionado la creación de pequeñas y sencillas redes virtuales. Básicamente, dentro del equipo que soporta las máquinas virtuales para que estas puedan estar conectadas entre ellas, aisladas entre sí o para que tengan conexión con el exterior. Estas redes virtuales son definidas dentro del hipervisor, y se comunican con el exterior a través de las interfaces virtuales de red mapeadas con las interfaces de red físicas de este equipo, utilizando el resto de los elementos físicos de la red donde se ubique el hipervisor: *switches, routers*, *firewalls*, cableado, etc.

La virtualización de redes permite dar respuesta a esta situación, bien virtualizando funciones de red o centralizando mediante *software* todos los servicios que se ejecutaban tradicionalmente en el *hardware* de un centro de datos, provocando una transformación de este.

Según VMware [13], “La virtualización de red (NV) hace referencia a la desvinculación de los recursos de red que tradicionalmente se proporcionaban en forma de hardware. La virtualización de red puede combinar varias redes físicas en una red virtual, mediante software o dividir una red física en redes virtuales independientes y separadas. Los recursos de la red física, tales como conmutadores y enrutadores, se agrupan y están accesibles para cualquier usuario a través de un sistema de gestión centralizado. La virtualización de red también hace posible la automatización de muchas tareas administrativas, lo que reduce los errores manuales y el tiempo de aprovisionamiento. Puede aumentar la productividad y la eficiencia de la red”.

El éxito de la virtualización de servidor o de escritorio hace que los fabricantes se planteen la virtualización de red, que entra en contraposición con los intereses de las empresas que han dominado determinados sectores, por ejemplo, el caso de VMware; especializada en *software* de virtualización adquiere la empresa Nicira[4] (agosto 2012), especializada en SDN, pasando a competir en un nuevo sector, dominado por empresas como Cisco o Juniper. Sin entrar en detalle, hay que indicar que en el caso de OpenStack este dispone de un componente denominado Neutron, el cual incorpora diversas características de red y SDN.

Este tipo de virtualización es especialmente útil para las empresas cuyas redes experimentan un aumento de utilización notable, rápido e impredecible, como puede ser la virtualización de nodos de voz o del *core* de datos de una operadora, por ejemplo, servicios como VoLTE o vEPC. No obstante, cualquier centro de datos con dispositivos físicos de red puede verse beneficiado virtualizando y centralizando servicios de optimización WAN, cortafuegos, enrutamiento, etc. Esto es posible debido a dos tecnologías como NFV y SDN. En lugar de asignar a cada equipo físico una funcionalidad específica, se le asocia un *software* virtual parametrizable, aportando la posibilidad a futuro de intercambiarlo con otros equipos de la red.

Más relevante que definir cada una de estas tecnologías, que no se considera objetivo del proyecto, es identificar las diferencias que ofrecen respecto a las redes clásicas o redes virtuales definidas como hasta ahora. A continuación, se indican algunas de estas diferencias:

- Todos los elementos de la red pasan a gestionarse de forma centralizada.
- Los elementos de la red pueden interactuar entre ellos independientemente del fabricante. Las redes dejan de estar ligadas a fabricante y protocolo específico.

[4] https://www.vmware.com/company/acquisitions/nicira.html

- Se facilita la creación de una única red de gestión y control a nivel lógico, que se puede dividir en las subredes necesarias. La misma red virtual puede definirse en varios hipervisores, gestionarse de forma centralizada, y automatizar la asignación del *pool* de IPs.
- Funciones de red como cortafuegos, balanceadores, DNS, DHCP, *proxies*, IDSs, QoS, etc. se pueden definir por *software*, ubicar en cualquier punto de la red y controlar centralizadamente.
- Utilización de VXLAN[5]. Aumento de escalabilidad. VXLAN 24 bits frente a VLAN 12bits., 16 millones de redes aisladas frente a 4094. Aumento de funcionalidad, mayor abstracción de dispositivos y capa de red física subyacente.

En la siguiente figura se puede observar una representación de la evolución de la red en los centros de datos. Se refleja el desacoplamiento entre la topología física y la lógica, a nivel de toda la red de una organización:

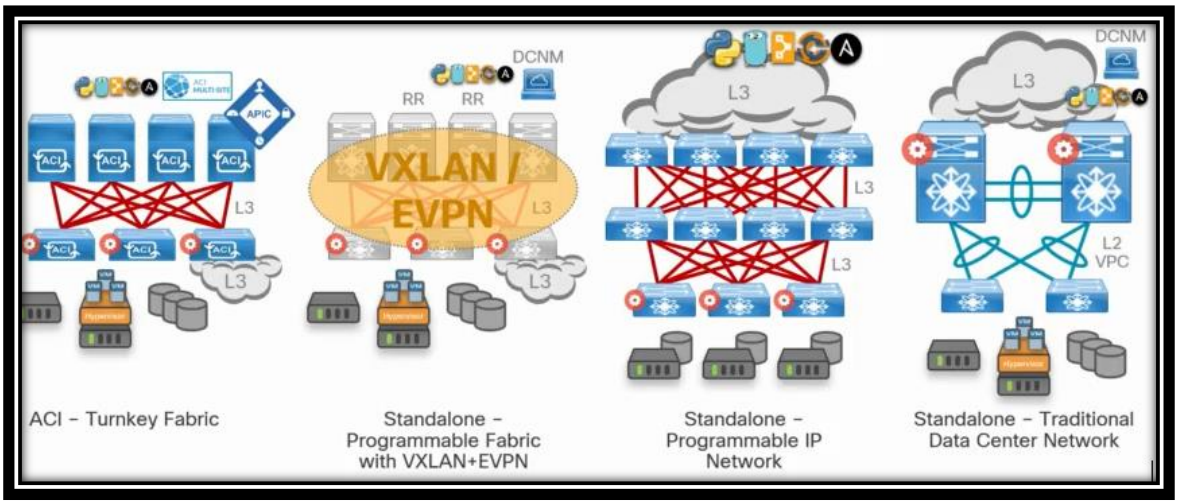


Figura 8: Diseñando nuevos datacenters. Cisco Live! Barcelona Jan 2020, Cisco Inc..

Uno de los resultados que se espera de la virtualización de redes es una mayor productividad y eficiencia de la red, bases necesarias para afianzar la llegada de tecnologías como IoT o 5G, y posteriormente, continuar con su desarrollo y evolución. Clave para esta evolución es la seguridad, surgiendo en este tipo de entornos nuevas posibilidades de gestión de esta, de manera centralizada y con mayor transparencia. Es importante indicar que las redes SDN diferencian claramente el tráfico a nivel de aplicación, por lo que evitan que soluciones de tipo cortafuegos o detectores de intrusión tengan impacto negativo en el rendimiento. Además, hay determinados tipos de *software* SDN/NFV que son capaces de enviar los flujos de tráfico a los sistemas de protección para su análisis. Previamente, se definen reglas y, en el momento que se detecta tráfico

[5] https://tools.ietf.org/html/rfc7348

diferente de los patrones establecidos, se redirecciona para su supervisión y control [14], [15] [16] .

Algunas de estas nuevas posibilidades, y como las implementan los sistemas de virtualización o de terceros, se detallan en los siguientes apartados, empezando por la arquitectura de un centro de datos basado en redes definidas por *software*.

3.3 Arquitectura de un entorno virtual de nueva generación.

La arquitectura de un entorno virtual se detalla, a continuación, haciendo referencia al diseño físico y lógico por capas, a alto nivel, de VMware [17] . Mientras que en el diseño físico entran en juego el *hardware* y el tipo de *software de virtualización,* en el diseño lógico, según la elección del proveedor de HW y de SW de virtualización, se podrían detallar diferentes diseños lógicos con sus respectivos componentes. Por lo tanto, aunque se intenta realizar una aportación lo más estandarizada y general posible, pueden existir otros diseños lógicos diferentes, por ejemplo, basados en OpenStack o Citrix.

A continuación, se puede observar la arquitectura de referencia actual SDDC[6] para este tipo de centros de datos definidos por *software*, ilustrada por VMware.

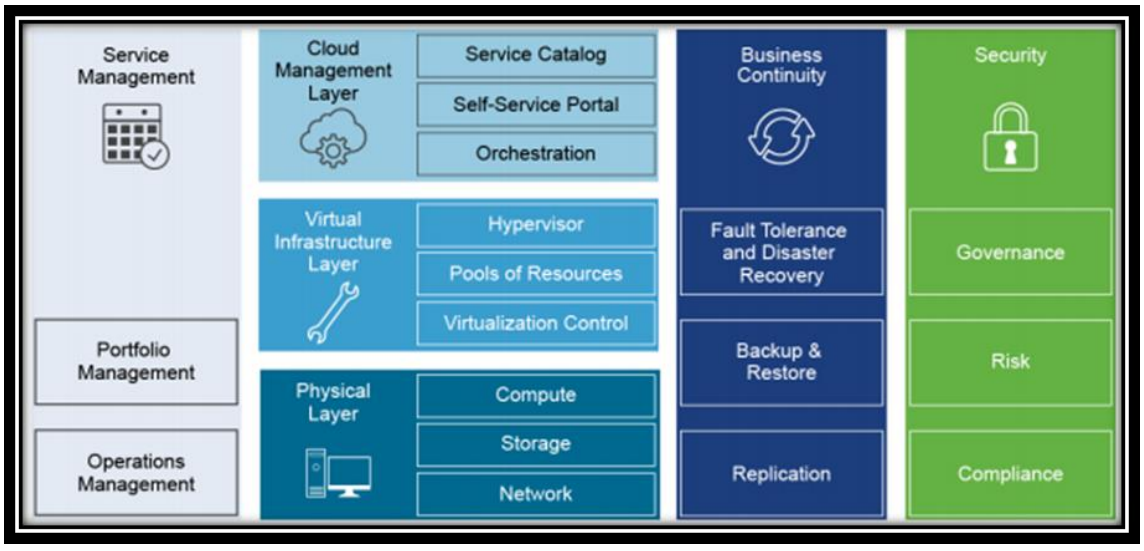


Figura 9: Arquitectura de referencia SDDC. VMware Inc.

En esta Figura 9, se pueden diferenciar claramente las capas que forman la arquitectura; secuenciales o superpuestas, y transversales. A continuación, se describen dichas capas.

[6] VMware reference architecture 2020 https://www.vmware.com/pdf/vmware-validated-design-20-reference-architecture-guide.pdf

3.3.1 Capa física. Infraestructura

La capa más baja de arquitectura es la capa física, que consta de tres componentes principales; CPU y memoria, que se engloban en el componente denominado *computing,* almacenamiento*,* y red. Dentro del *compute* se sitúan los servidores basados en x86, como es el caso de VMware, que proporciona alguna orientación sobre las capacidades necesarias para ejecutar esta arquitectura, sin embargo, no da recomendaciones sobre el tipo o proveedor de *hardware*, como es lógico. No obstante, existen otras arquitecturas físicas como pueden ser las de servidores basados en RISC y en ARM, esta última adoptada por el fabricante Huawei, con procesador propio; Kunpeng 920, el cual aparece por encima de Intel i9 en diferentes medios[7] y *benchmarks.*

Sin entrar en detalle, cabe destacar tres tipos de servidores para la virtualización; servidor de tipo rack o clásico, servidor tipo *blade,* y servidor hiperconvergente. Fabricantes como Cisco, HP, Dell o Huawei proporcionan cualquiera de estos tipos de servidores específicos para virtualización, con diferentes combinaciones de memoria; tipo de RAM, slots, etc., y CPU; familia, número de *cores*, velocidad de reloj, etc. según los requerimientos del cliente.

Figura 10: Tipo de hardware y proveedores: Cisco Inc. Huawei, HPE.

En el caso de VMware, todos los componentes físicos deben ser compatibles con su guía de compatibilidad de *hardware.*

Una vez descrito el componente de computación quedarían el componente de almacenamiento y el de red. En la arquitectura física validada por VMware, se utiliza un pequeño conjunto de bloques denominados *pods*. Un *pod* es una agrupación lógica de hardware que admite una determinada función y es fácil de

[7] https://www.extremetech.com/computing/313641-huaweis-upcoming-24-core-kunpeng-cpu-faster-than-intel-core-i9-9900k

replicar, además, diferentes *pods* pueden en paralelo proporcionar diferentes características, por ejemplo, un módulo de procesamiento podría usar redundancia de *hardware* completa para cada componente para una mayor disponibilidad mientras que otro módulo podría usar *hardware* sin ninguna redundancia física.

Uno de los principios de este tipo de implementaciones es que la capa de virtualización de red no abarca las VLAN más allá de un solo *pod*. Aunque esta restricción de VLAN parece ser un requisito simple, tiene un impacto generalizado en cómo se puede construir una infraestructura de conmutación física y en cómo se escala.

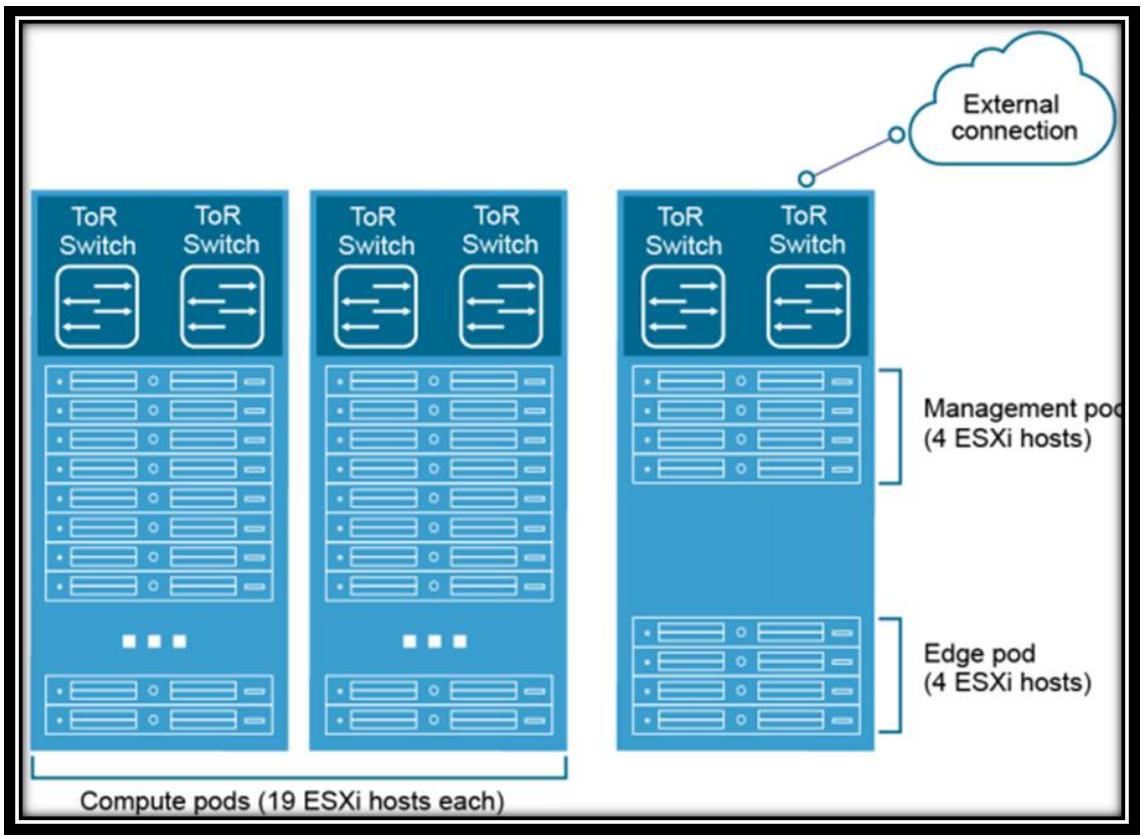


Figura 11: Pods en el diseño de datacenter. VMware Inc.

El SDDC de VMware diferencia entre los siguientes tipos de pods:

- Computing
- Management
- Edge
- Storage

Otro de los aspectos clave y novedosos en esta arquitectura respecto a la arquitectura clásica, tal y como se ha visto en el punto 3.2 Principio del cambio: Virtualización de la red, es la incorporación de la infraestructura de equipos de

red al entorno virtualizado. Esta arquitectura está estrechamente ligada al uso de *pods*, utilizando una arquitectura basada en *leafs* y *spine switches*, en lugar del diseño más tradicional del centro de datos en tres niveles. Se puede implementar una estructura de capa dos, equivalente a los *switches* físicos y ofreciendo servicios de transporte de capa dos o servicios de transporte de capa tres a todos los componentes, si se precisa una red escalable e independiente del proveedor.

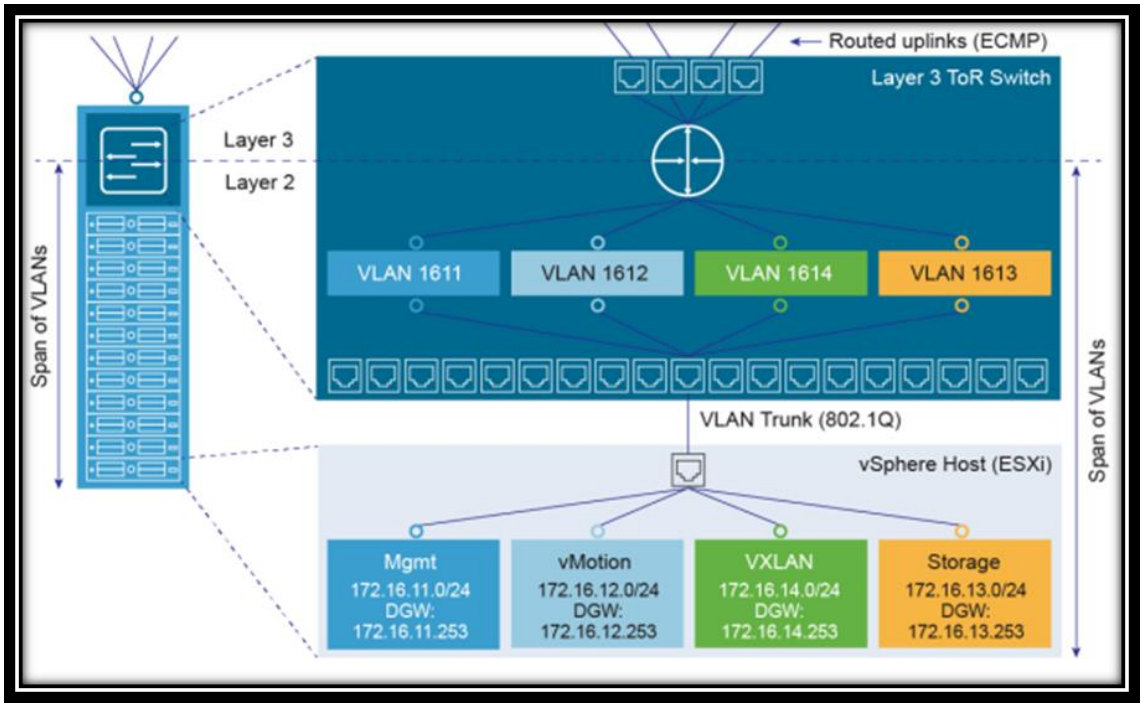


Figura 12: Representación a alto nivel de un nodo Leaf. VMware Inc.

3.3.2 Capa de virtualización o infraestructura virtual

La capa de virtualización es la capa de *software* que, en su definición clásica, permite virtualizar los servidores. No obstante, como se ha ido viendo durante el desarrollo de este trabajo, la evolución en el área de la virtualización ha posibilitado la virtualización de otros componentes *hardware* como dispositivos de almacenamiento o de red.

Por norma general esta capa se sitúa sobre la de infraestructura, es decir, se posiciona directamente sobre la capa descrita en el apartado anterior. Dentro esta capa se encuentra la gestión de la infraestructura física subyacente donde se realizan, entre otras tareas, la asignación de recursos, cargas de trabajo, y administración de los *hosts* y *GuestOS* (VMs).

A nivel de componentes la capa de infraestructura virtual consta principalmente del hipervisor, que se detalla en el apartado 3.3.6 Capa de virtualización: El

hipervisor el *software* de gestión de estos hipervisores, y los flujos de interactuación con capas superiores y transversales; capa de gestión de la nube, gestión de servicios, seguridad, etc.

En VMware, aunque existen diferentes paquetes que engloban esta capa y la de *cloud,* el producto destinado para entornos corporativos se denomina VMware vSphere. Este producto incluye, entre otros, el hipervisor ESXi, el gestor conocido como vCenter, el cliente ligero vSphere Client, etc.

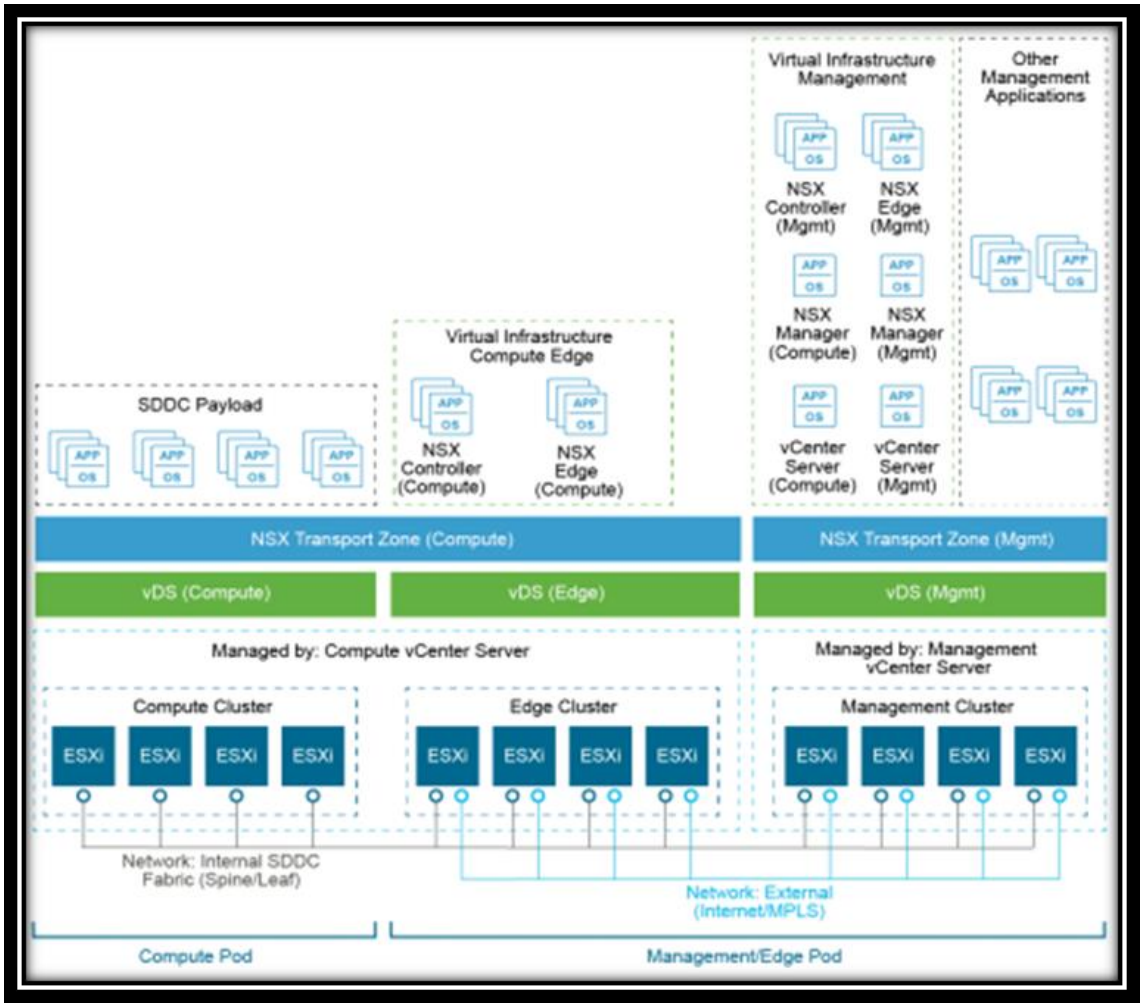


Figura 13: Diseño lógico de referencia capa de virtualización. VMware Inc.

Tal y como se puede ver en la Figura 13, la infraestructura lógica de un centro de datos definido por *software* difiere de otro convencional, a alto nivel, en los componentes de virtualización de red, por ejemplo:

- NSX Controller
- NSX Edge
- NSX Manager

3.3.3 Capa de gestión Cloud

La capa de la nube o gestión del Cloud es la capa superior de la pila, y es en esta capa donde se gestionan los servicios y su utilización. Por lo general, a través de una interfaz de usuario o API, esta capa solicita o reserva recursos y luego administra las acciones de las capas inferiores. Se debe tener en cuenta, a nivel de seguridad, que acciones típicas del vCenter como arrancar, parar o reiniciar servidores pueden hacerse también desde vCloud, además de automatizar todo tipo de tareas de administración, modificar políticas de FW, routing, VXLANs, etc. De cara a un posible acceso indebido o una escalada de privilegios, la posibilidad de una capa superior que permita automatizar todo tipo de tareas, y tener control absoluto del entorno, implica la necesidad de securizar la autenticación y autorización al mismo.

Por lo tanto, aunque la arquitectura de referencia del SDDC se sostiene sin ningún otro componente adicional, para una operativa optima, se recomiendan otros componentes de apoyo como las capas de seguridad, continuidad de negocio o de gestión de servicios.

3.3.4 Capa de gestión y continuidad de negocio

Al construir cualquier tipo de infraestructura de TI, la operación juega un papel importante en la prestación de servicio, especialmente en infraestructuras críticas de alta disponibilidad. El área de gestión de servicios de esta arquitectura se centra en la gestión de operaciones, en particular, en la integración con sistemas de gestión de aseguramiento tipo Netcool, TeMIP, etc. y de respaldo ante situaciones tipo *disaster recovery* como pueden ser Networker o Avamar. Es decir, para garantizar la eficiencia de un sistema corporativo este debe contener elementos para respaldar la continuidad del negocio en el área de copias de seguridad, restauración y recuperación ante desastres.

3.3.5 Capa de seguridad

Se parte de la base de que todos los sistemas deben ser diseñados inherentemente seguros, con el objetivo de reducir los riesgos y cumplir con la normativa requerida. Esta capa de seguridad, y sus componentes, es necesaria para garantizar que el centro de datos sea resistente tanto a amenazas internas como externas, y se analiza en más detalle durante el desarrollo de este trabajo. No obstante, NSX proporciona en la capa de virtualización una serie de mecanismos de seguridad para este tipo de entornos virtuales:

- Distributed firewall
- Edge firewall

- Logical VPNs
- Service Composer
- Microsegmentación

3.3.6 Capa de virtualización: El hipervisor

En este apartado se describe uno de los componentes clave de la capa virtual como es el hipervisor. Dicho componente se considera uno de los pilares del *stack* virtual y se describe a bajo nivel con el fin de cubrir, posteriormente, uno de los objetivos de este proyecto; la securización de un hipervisor.

El hipervisor, también conocido como VMM o monitor de máquina virtual, es definido por Red Hat como:" un *software* que crea y ejecuta máquinas virtuales (VM) y que, además, aísla el sistema operativo y los recursos del hipervisor de las máquinas virtuales, y permite crearlas y gestionarlas." [18]. La definición de VMware [19], por su lado, no es muy diferente: "… *software* que crea y ejecuta máquinas virtuales (VM). Un hipervisor permite que una computadora *host* admita múltiples VM invitadas al compartir virtualmente sus recursos, como la memoria y el procesamiento." En definitiva, el hipervisor es un sistema que permite la multiplexación de otros sistemas sobre unos recursos físicos, permitiendo la optimización del uso de estos. Además, al abstraer los recursos físicos de la primera capa virtual se proporciona una agilidad y movilidad para entornos de TI, ya que las VM o *guests* son independientes del *hardware* del host, donde se encuentra el hipervisor. Esto se traduce en la posibilidad de mover las VM entre diferentes servidores.

Como se ha ido mencionando durante el trabajo, el *hardware* físico donde se instala el sistema que se usa como hipervisor se denomina host, y las múltiples máquinas virtuales que utilizan sus recursos se denominan VM, *guests* o *guestOS*. El hipervisor utiliza y gestiona recursos, como la CPU, la memoria, el almacenamiento, puertos serie, interfaces de red, etc., como un conjunto de medios que pueden redistribuirse fácilmente entre las máquinas virtuales presentes y los nuevos despliegues.

Cualquier hipervisor proporciona a las diferentes máquinas virtuales los recursos previamente asignados, gestionando los mismos en función de los recursos físicos disponibles. De ahí que, independientemente del hipervisor que se utilice, este necesita componentes conocidos de un sistema operativo tradicional como un gestor de procesos, administrador de la pila de memoria, de entrada y salida (E/S), controlador de dispositivos, de la pila TCP/IP, etc. Esto posibilita que muchos sistemas operativos diferentes pueden funcionar en paralelo utilizando recursos físicos compartidos que se traducen en recursos virtuales dedicados.

Debido a que VMware es el fabricante con más peso en el área de la virtualización se hará foco en su hipervisor (ESX/ESXi), no obstante, hay diferentes opciones de hipervisores. Algunos de ellos, se indican a continuación:

Tipo I (*unhosted*):

- **KVM:** Acrónimo de Kernel-based Virtual Machine. Solución de código abierto de Red Hat bajo el proyecto Open Shift.
- **XenServer:** Hipervisor de código abierto desarrollado por la Universidad de Cambridge. Posibilidad de paravirtualiación.
- **Xen Hypervisor**: En 2007 Citrix adquiere XenSource y lanza su nuevo hipervisor. A partir de la versión 8.0 se conoce como Citrix Hypervisor, no obstante, Citrix sigue dando soporte a las versiones anteriores.
- **Hyper-V:** Es el hipervisor de Microsoft. Específico para sistemas de 64 bits y *hardware* basado en procesadores basados en AMD-V o Intel VT (VT-x).

Tipo II (*hosted*):

- **Proxmox VE**: Se incluye en distribuciones GNU/Linux basadas en Debian con una versión modificada del Kernel RHEL, permite el despliegue y la gestión de máquinas virtuales y contenedores. Código abierto, incluye una consola Web, herramientas de línea de comandos, y proporciona una API REST para herramientas de terceros.
- **VirtualBox:** *Software* de virtualización para arquitecturas x86/amd64 de Oracle. Se puede utilizar sobre diferentes sistemas operativos como GNU/Linux, Mac OS X, OS/2 Warp, Genode,1 Windows y OpenSolaris.
- **Workstation:** hipervisor específico de VMware para el sistema operativo Windows.
- **Parallels:** hipervisor destinado a ordenadores Macintosh con procesadores Intel.
- **Virtual PC:** *software* gestor de virtualización desarrollado por Connectix y adquirido por Microsoft para crear equipos virtuales
- **QEMU:** emulador de procesadores basado en la traducción dinámica de binarios con capacidades de virtualización dentro de un sistema operativo. Licenciado en parte con la LGPL y la GPL de GNU.
- **Bhyve:** hipervisor desarrollado para FreeBSD, que ha sido recientemente portado a varias distribuciones basadas en illumOS, como SmartOS.4 y OmniOS5.

Por otro lado, tal y cómo se han distribuido en el listado, estos hipervisores se clasifican en dos tipos:

- **Hipervisor de tipo uno** [20]: Este tipo es denominado también *bare metal, unhosted* o nativo. En este hipervisor el *software* se ejecuta directamente

sobre el *hardware,* es decir, la capa de virtualización se instala directamente sobre el servidor físico y el *hardware* subyacente, sin existir ningún otro *software* entre medias. El rendimiento y estabilidad, demostrado, de este tipo de hipervisores hace que se encuentren, principalmente, en entornos empresariales. El ESX/ESXi de VMware pertenece a este tipo.

- **Hipervisor de tipo dos**: Este tipo es denominado también *hosted*. En este tipo de hipervisor el *software* se ejecuta sobre un sistema operativo, el cual se encuentra instalado en un servidor físico, de ahí que el hipervisor reciba el nombre de *hosted (*alojado). Por lo tanto, la diferencia con el tipo uno es la capa de *software* intermedia entre el servidor físico y el hipervisor. Esta capa intermedia no es más que un sistema operativo tradicional; MS Windows, GNU/Linux o MacOS donde se instala, por ejemplo, alguno de los hipervisores de tipo dos mencionados anteriormente. Los hipervisores de este tipo son adecuados para probar *software* nuevo o potencialmente peligroso, proyectos de investigación, etc., es decir, son una herramienta muy útil a nivel de seguridad para configurar *sandboxes* de manera sencilla y ágil, sin entrar en virtualización con contenedores.

  Tal y como se muestra en Figura 14, de un entorno doméstico, permite la ejecución de varios sistemas operativos diferentes, pudiendo crear configuraciones específicas de red entre el host y las máquinas virtuales; NAT, bridge, LAN, etc.

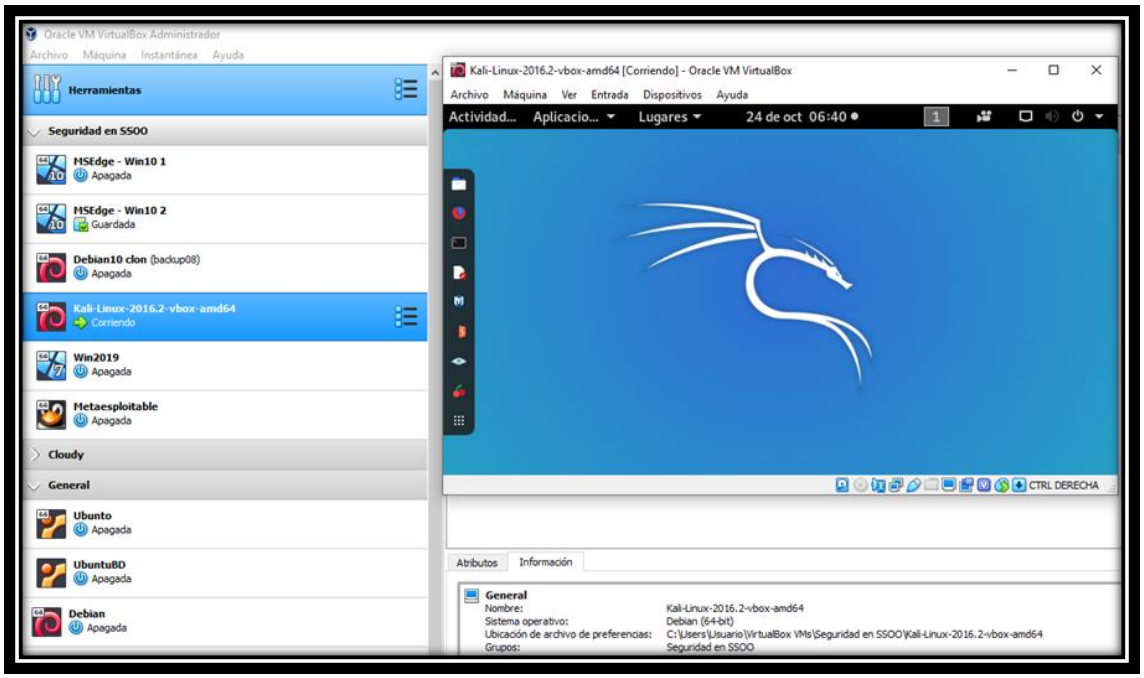


Figura 14: Entorno doméstico hipervisor tipo II basado en Virtual Box.

Seleccionar un tipo u otro de hipervisor depende del uso que se le vaya a dar y en que situaciones o contexto; uso empresarial, académico, individual, por otro

lado, se debe tener en cuenta el tamaño del entorno virtual que se pretende ejecutar.

Para un uso individual, y un despliegue acotado, se puede optar por uno de los hipervisores tipo dos, en el cual hay opciones de pago con diversas funciones, como es el caso de VMware Workstation, no obstante, Oracle VM VirtualBox es un hipervisor gratuito que proporciona la mayoría de las funcionalidades que se puedan necesitar.

En entornos corporativos o empresariales la situación es diferente, la tendencia es el uso de hipervisores de tipo uno bajo algún paquete licenciado, tipo el vSphere de VMware, que incluye más productos y un soporte asociado. El soporte, además del coste de la licencia, suele ser uno de los puntos donde se suele hacer hincapié en este tipo de entornos. Las licencias pueden ser por servidor, por CPU, e incluso, por número de *cores*. Es un detalle importante a tener en cuenta, también, para el despliegue de un *software* de securización de este tipo de entornos.

En la situación actual, el mercado está liderado por VMware, Microsoft y RedHat, con vSphere ESXi, Hyper-V y OpenStack KVM, respectivamente. En este proyecto, académico y de alcance virtual acotado, se utilizan tanto VirtualBox como ESXi de Vmware, el cual se detalla a continuación.

3.3.6.1 Hipervisor ESXi

VMware ESXi [21], anteriormente VMware ESX, es el *software* de virtualización de VMware Inc. específico para un centro de datos empresarial. Como se ha indicado, pertenece al tipo uno de hipervisores, se encuentra en el nivel inferior de la capa de virtualización, directamente instalado sobre el servidor. Es una de las partes fundamentales de la *suite* VMware vSphere, que tiene otros componentes como el vCenter (psc y vcsa), y un cliente para facilitar la administración remota del entorno.

El arranque de la máquina anfitriona se produce a través de la ejecución de unas interfaces propias basadas, en teoría, en un kernel de Linux, denominado VMkernel. Este proporciona servicios de consola y *hardware* a nivel del anillo, como se puede ver en la Figura 15. El ESXi aplica teoremas de la para-virtualización, creando un nivel de anillo menos uno, y pasando a ejecutar el entorno operativo como una máquina virtual. Este sistema de anillos reproduce una protección jerárquica por dominios, donde cada uno de los niveles delimita un sector con determinados privilegios; nivel de hipervisor, nivel de *kernel* de VM, nivel de servicios del sistema, extensiones, y aplicaciones.

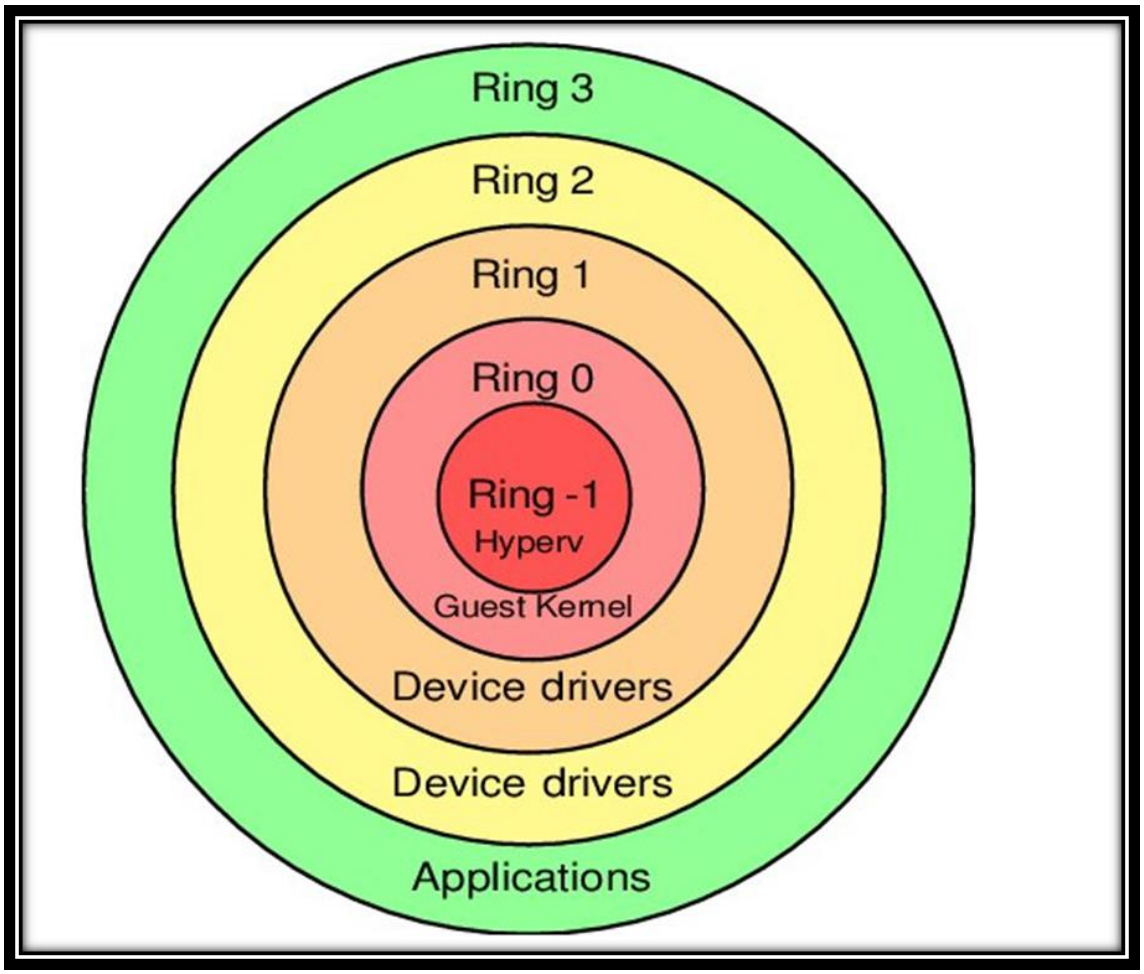


Figura 15: Anillos de ejecución en x86 virtual de HyperV [22].

El vmkernel está programado y configurado siguiendo la arquitectura de microkernel. Tiene varias interfaces con el exterior, con las que administra la mayoría de los recursos físicos del *hardware*; la memoria, los procesadores físicos, el almacenamiento[8], las controladoras de redes[9], y el programador.

El programador se encarga de escalar de manera proporcionada o justa los recursos de CPU, incluso cuando están comprometidos. VMkernel distribuye de manera justa los recursos de la CPU a todas las máquinas virtuales, al menos, hasta 4 veces el sobre compromiso (*oversubscription*), de la CPU. Por supuesto, en un sistema con la CPU sobre comprometida cuatro veces, cada VM solo se ejecutará a un cuarto de velocidad nativa, pero el programador mantiene las VM funcionando con ese rendimiento.

[8] https://docs.vmware.com/es/VMware-vSphere/6.0/com.vmware.vsphere.storage.doc/GUID-E3FAD26A-EF98-4BE0-B5BD-FB4597CED793.html

[9] https://docs.vmware.com/en/VMware-vSphere/6.0/com.vmware.vsphere.networking.doc/GUID-D4191320-209E-4CB5-A709-C8741E713348.html

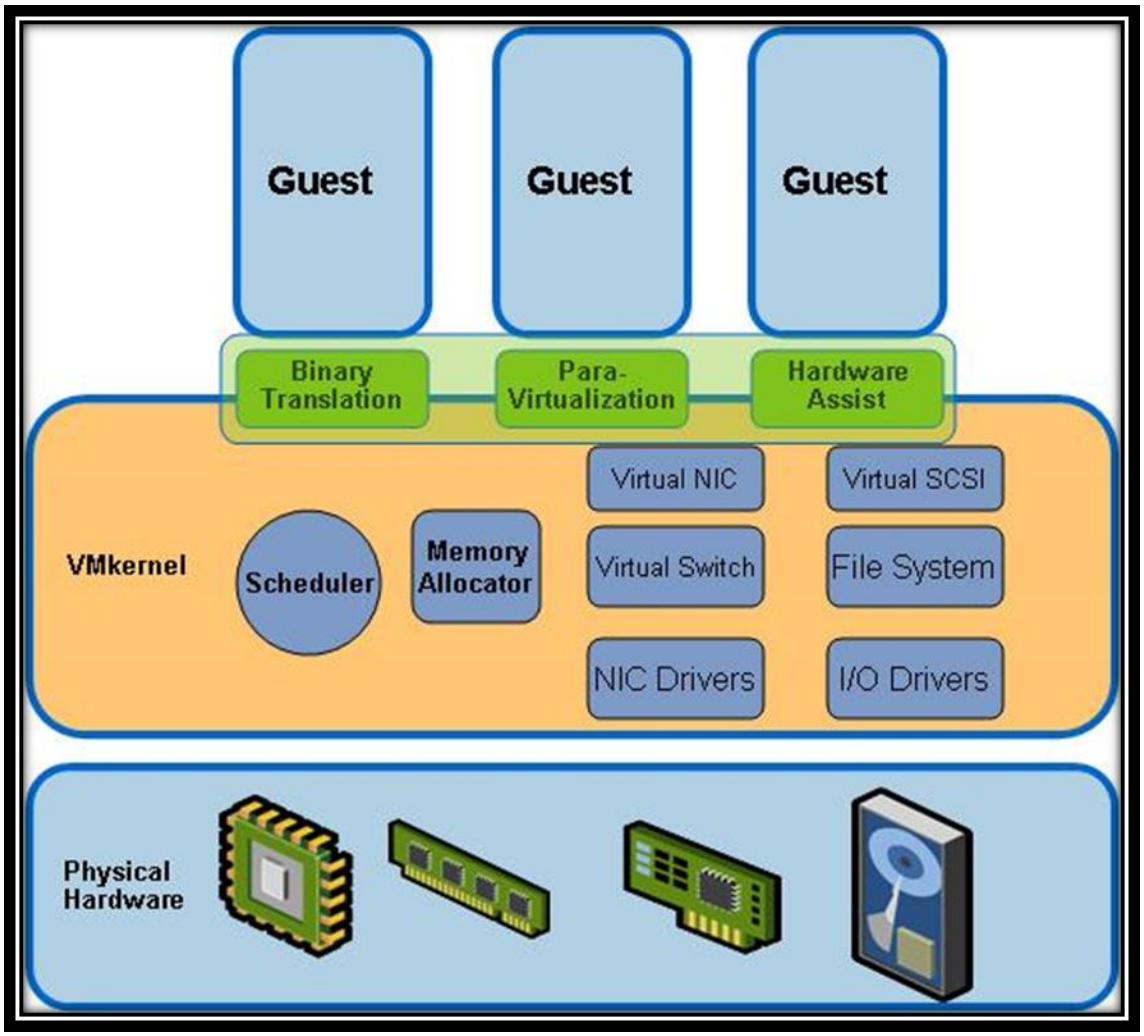


Figura 16: VMkernel: Interfaces virtuales y drivers [23].

3.3.6.2 Principios de seguridad en el hipervisor ESXi

El ESXi proporciona unos mecanismos de seguridad por capas:

- Aislamiento seguro de máquinas virtuales en la capa de virtualización. Esto incluye aislamiento seguro de instrucciones, aislamiento de memoria, aislamiento de dispositivos y uso de recursos administrados y aislamiento de red.
- Gestión segura configurable del entorno virtualizado. Esto incluye comunicación segura entre componentes de virtualización a través de SSL; protección de host a través del modo de bloqueo; y el menor privilegio por un mecanismo de control de acceso detallado y basado en roles.
- Implementación segura del ESXi en servidores mediante el uso de varios mecanismos de integridad de plataforma como paquetes de *software* firmados digitalmente y arranque confiable basado en Intel Trusted Platform Module (TPM).

- Ciclo de vida de desarrollo de *software* seguro y riguroso que permite a los desarrolladores crear software utilizando principios de diseño y codificación, como superficie mínima de ataque, privilegio mínimo y defensa en profundidad.

Estos aspectos de seguridad de un hipervisor se estudian en los siguientes apartados con el fin de comprender el funcionamiento a bajo nivel, tanto de la correcta parametrización de seguridad de este componente, como de la integración con sistemas de terceros, para securización con o sin agente.

3.4 Seguridad en entornos virtualizados

3.4.1 Amenazas de seguridad

La seguridad en los centros de datos se diseña pensando en la seguridad física del edificio desde el primer momento, teniendo en cuenta la ubicación, los sistemas de construcción, y los estándares legales para este tipo de infraestructuras. A la hora de escoger la ubicación para un centro de datos se evalúan factores como la disponibilidad de potencia eléctrica, opciones de conectividad, logística, etc. No obstante, la seguridad física en un entorno virtual de nube pública deja de ser relevante ya que se deriva dicha responsabilidad a un tercero, como es un proveedor de Cloud. Por lo tanto, se analizan únicamente las amenazas de seguridad de un entorno tradicional y virtual, desde el punto de vista lógico, observando sinergias entre ambos, por ejemplo:

- **Perdida e integridad de la información:** Deben existir mecanismos que eviten que los datos sean manipulados o borrados, tanto accidentalmente como de manera intencionada. En los entornos tradicionales existen sistemas de *backup* que deben ejecutar copias de respaldo; totales, parciales, además de aplicar políticas como periodicidad, retención, etc. Existiendo la posibilidad de uso de agentes con comunicación cifrada, y una red dedicada. Del mismo modo, en entornos virtuales se proporciona este tipo de solución, añadiendo las figuras de sistemas *agentless* (funcionamiento sin agente), y de los *snapshots* o clonados, tanto de máquina virtual completa como de memoria del sistema.
- **Control de acceso:** Únicamente los usuarios autorizados deben acceder a los SSII bajo unos parámetros específicos del rol que desempeñen, es decir, se debe garantizar una autenticación lícita y una autorización específica para el desempeño de la función de cada usuario. Una de las amenazas, tanto en un entorno convencional como virtual, es el escalado de privilegios. Ambos entornos pueden ser susceptibles de accesos no autorizados, no obstante, en apartados posteriores se desarrollan las medidas complementarias en entornos virtuales.

- **Código malicioso:** Al igual que un entorno tradicional, el entorno virtual es susceptible de ser infectado con *malware.* Este aspecto es uno de los objetivos de este proyecto, responder al interrogante del nivel de seguridad en los entornos virtuales respecto a una amenaza como es el *malware.*

Aunque se hayan identificado únicamente tres amenazas o aspectos de seguridad que coinciden en ambos entornos, en líneas generales, los entornos virtuales pueden ser víctimas de ataques similares o padecer las mismas amenazas. Estas pueden afectar a los sistemas independientemente de si se encuentran en un entorno físico convencional o en un entorno virtual. No obstante, de cara a aplicar medidas de seguridad se debe conocer la existencia de condiciones propias de cada entorno sobre la forma de implementar las mismas. Especialmente si consideramos que la administración de los sistemas virtualizados se opera a partir de un hipervisor, pilar básico de un entorno virtualizado.

Independientemente del modo en el que se trabaje, los riesgos se encuentran presentes, tal y como sucedió con Venom [24], una vulnerabilidad que permitiría a un atacante o un programa malicioso salir del entorno de una máquina virtual y afectar al equipo anfitrión o *host,* posibilitando la expansión a otras máquinas virtuales que se ejecutasen en el mismo equipo.

Una amenaza de este tipo, en la capa de virtualización, podría afectar a capas superiores y otros procesos o cargas de trabajo dependientes. Por lo tanto, la propia capa de virtualización debe ser considerada como otro componente importante plataforma de TI en la infraestructura de una empresa y, como cualquier otro *software*, puede contener vulnerabilidades que se traducen en amenazas o ataques.

Otro tipo de amenazas específicas de entornos virtuales son:

- **Consumo excesivo de recursos**: Debido a efectos avalancha, de soluciones tradicionales de antivirus, por actualizaciones simultaneas de bases de datos o replicación de bases de datos de firmas, se produce una saturación en los *hosts*, provocando posibles “ventanas de vulnerabilidad”, denegación de servicio, etc.
- **Tráfico interno:** El tráfico que se produce dentro del entorno virtual, en concreto, origen y destino dentro del mismo host, suele ser catalogado como confiable y no es visible, por normal general, desde la red física.
- **Máquinas *zombies* o inactivas:** En este tipo de máquinas, aunque estén registradas en el sistema virtual, no se pueden actualizar las bases de datos de virus o antimalware por lo que, si se inician estas máquinas, desde el

arranque hasta el proceso de actualización dicho sistema será vulnerable a ciertos ataques de código malicioso.

- **Incompatibilidades:** Los sistemas operativos estándar tradicionales no estaban diseñados para gestionar muchas funciones virtuales, la conversión a virtual de este tipo de sistemas obsoletos puede generar bloqueos del sistema virtual, inestabilidades, etc. Además de otras amenazas derivadas.
- **Persistencia de datos**: La descentralización del centro de datos y la utilización de la nube puede hacer que el movimiento o replicación de una VM entre entornos afecte a la privacidad y confidencialidad de la información o incluso, ciertos aspectos legales.

No obstante, tal y como se ha indicado, el hipervisor es uno de los componentes de mayor importancia dentro de la capa de virtualización, siendo el componente que más amenazas representa, por ejemplo:

- **Configuración del servidor:** La incorrecta configuración del *firmware* del servidor, así como una mala configuración del sistema hipervisor, por ejemplo, del nivel -1 del anillo, pueden afectar y comprometer a todas las máquinas virtuales, ya que en ese nivel se configuran instrucciones privilegiadas.
- **Aislamiento de dispositivos tradicionales:** Las comunicaciones entre las VMs se realizan a través del hipervisor, por lo tanto, los IDS/IPS físicos no tienen acceso a este tráfico, al igual que los firewalls. Además, en caso de un escenario mixto; virtual y físico, tampoco se dispondría del detalle extremo a extremo.
- **Escenario heterogéneo de red:** En entornos virtuales pueden convivir diferentes VMs con direccionamiento público o DMZ, corporativo, de gestión, etc. con diferentes políticas de seguridad, tráfico y acceso, que puede dificultar el diagnóstico en caso de un ataque externo o en la identificación de patrones de red.

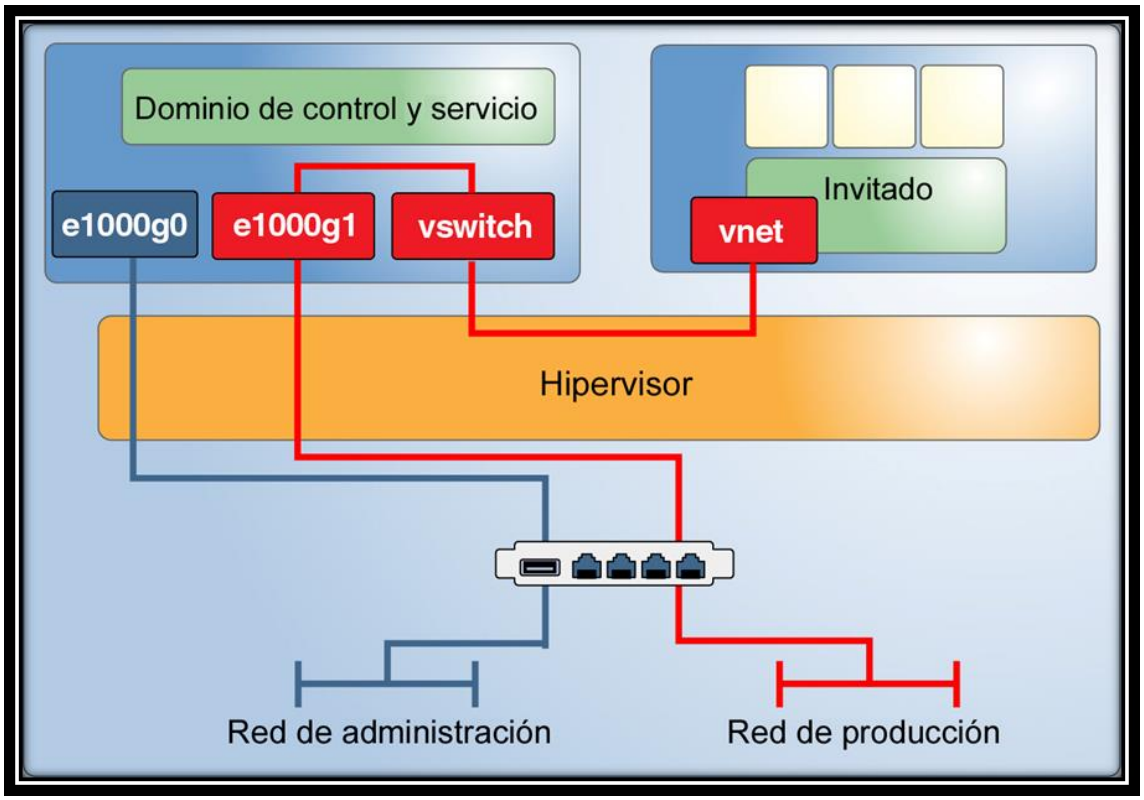


Figura 17: Tráfico de red hipervisor: Red de gestión dedicada. Oracle Inc.

De ahí que, durante todo el desarrollo del trabajo, se hace foco en el hipervisor, y se realiza una prueba de concepto sobre su securización. Por último, para adoptar un enfoque general de protección, hay que destacar que las principales consideraciones a tener en cuenta son el tipo de hipervisor utilizado, los recursos de *hardware* y *software*, además de la tecnología de virtualización seleccionada [25], [26] .

Por otro lado, cabe destacar el desarrollo de aspectos técnicos de manera general y, específicamente, de soluciones de fabricantes líderes en el sector de la virtualización como es VMware, y de la seguridad como ESET, Trendmicro, Kaspersky, SentinelOne, F-Secure, etc.

3.4.2 Protección contra *malware* en entornos virtuales

Tal y como ha ido cambiando el escenario de los centros de datos, y la aplicación de las tecnologías que se han ido viendo, la seguridad y el hacking ético son claves para proteger los entornos ante nuevas amenazas y mantener la integridad y la privacidad de los datos.

En apartado se pretende desarrollar los tipos de protección contra virus y *malware* en un entorno de virtualización, aplicable a un entorno en la nube. El objetivo es sentar las bases para seguir desarrollando los apartados posteriores

de componentes de VMware, su interoperabilidad, y la evolución de las soluciones de seguridad, hasta llegar a las últimas tendencias para centros de datos completamente virtualizados.

Existen varias opciones para proteger equipos virtuales contra virus y *malware*:

- **Protección basada en la premisa de caja de arena o *sandbox.*** La primera opción consiste en no aplicar ninguna medida específica, basándose en la premisa de que un entorno virtual es seguro por el hecho de ser virtual, por ejemplo, considerando que un entorno virtual es una caja de arena, es decir, un entorno aislado que no se ve afectado por *software* potencialmente peligroso, no instalando ningún *software* de protección. Tal y como se describe en este proyecto, un entorno virtual no es una *sandbox* y, por tanto, no está exento de *malware*.

  En alguno de los artículos de Infosecurity-magazine[10], basados en información de Symantec, se puede observar cómo ante el crecimiento del uso de máquinas virtuales, las cuales se estaban volviendo más comunes en los entornos operativos empresariales, hace que los desarrolladores de *malware* modifiquen el código para adaptarse a este tipo de entornos.
- **Protección basada en antivirus.** Esta opción se apoya en la solución de un *software* antivirus instalado en el sistema operativo de la máquina virtual, al igual que se conocía en los entornos físicos convencionales. La solución de seguridad está preinstalada como parte del equipo directamente instalado en la máquina virtual o *Guest OS.*
- **Protección basada en agente.** Esta opción se basa en la solución de un agente instalado en el sistema operativo de la máquina virtual. Estos agentes, por normal general, pueden pertenecer a una plataforma de gestión centralizada de seguridad. Este tipo de plataformas se las conoce como EPP, y aunque se define a continuación, se detalla en el apartado 3.7 La evolución del antivirus convencional, EPP, EDR y XDR ya que son un avance significativo frente a las soluciones tradicionales de antivirus.,

  Un EPP o Endpoint Protection Platform es una plataforma de seguridad de dispositivos o puntos finales (EP). Este tipo de solución se implementa, entre otros aspectos, para prevenir el *malware* basado en archivos, detectar y bloquear la actividad maliciosa de aplicaciones tanto confiables como no confiables, y para proporcionar las capacidades de investigación y corrección.

[10] Malware No Longer Avoids Virtual Machines https://www.infosecurity-magazine.com/news/malware-no-longer-avoids-virtual/

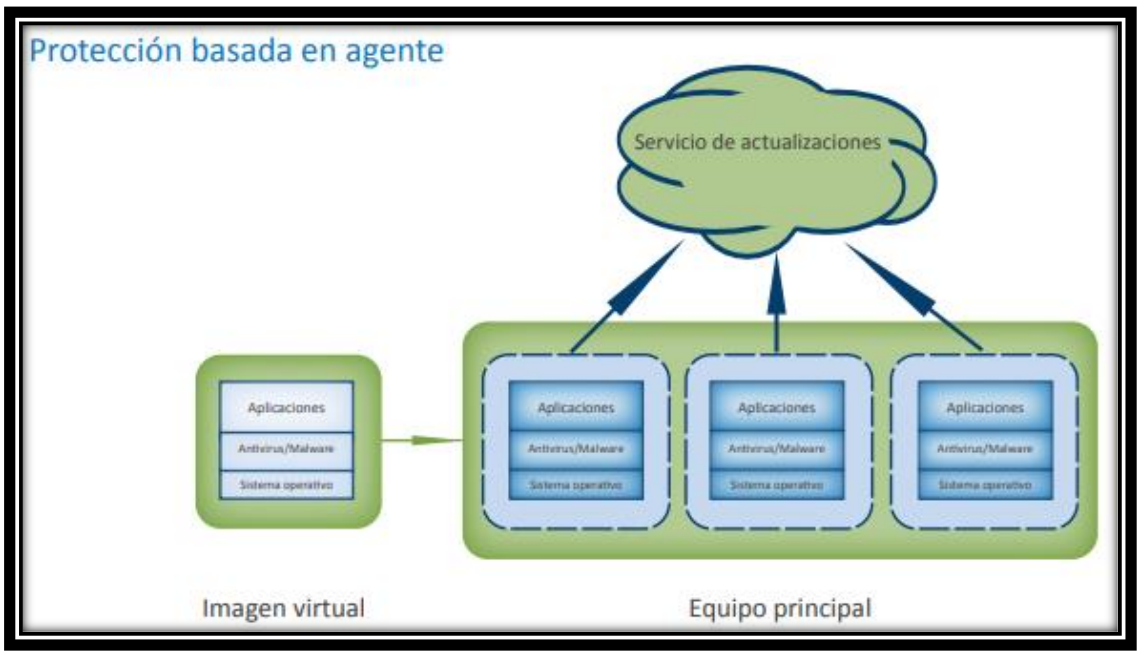


Figura 18: Protección basada en agente. Kaspersky.es

- **Protección basada en solución centralizada sin agente.** Esta opción implica el despliegue de un dispositivo de seguridad centralizada que proporcione protección contra virus y, en definitiva, *malware* o cualquier tipo de ataque. Esta protección se define para un grupo de equipos virtuales, por ejemplo; un clúster de *hosts,* una *cloud* local, etc. La tipología de este grupo, como puede ser un clúster, requiere tener asociado una *virtual appliance* del proveedor de seguridad, en comunicación con el servidor central para aprovechar el potencial de este tipo de solución; DPI, *Virtual patching, Firewall, Antivirus*, etc.

  Esta solución, al no tener como requisito la instalación de un agente por cada VM, requiere menos espacio físico virtual. Por otro lado, reduce de forma significativa la sobrecarga del rendimiento asociada a la ejecución de un conjunto completo de protección en cada cliente o EP [27] .

Una vez descritos los tipos de protección contra *malware*, se considera relevante hacer foco en la protección centralizada sin agente, por lo tanto, se detalla técnicamente en los siguientes apartados la viabilidad de esta técnica mediante diferentes componentes de VMware.

3.5 Concepto *agentless*. Protección sin agentes. vShield y NSX

En este tipo de entornos, muchas organizaciones basan su seguridad desde un punto de vista tradicional, es decir, instalando agentes en cada máquina virtual (VM). La tendencia de replicar la solución completa por agente en cada VM no

es eficiente y degrada el rendimiento o consume los recursos del host. Por poner un ejemplo, se cargan por defecto todas las políticas en un agente indiferentemente de si se trata de un *front-end* web, un servidor de correo o base de datos, es decir, la no especificación de políticas por servicio suele terminar en la generalización y, por tanto, el funcionamiento no eficiente del agente.

Una alternativa, como se ha visto con anterioridad, es integrar la seguridad directamente con la plataforma de virtualización, por norma general, proporcionando un dispositivo virtual de seguridad dedicado en cada host, se pueden usar las API de la plataforma de virtualización y la introspección del hipervisor para comunicarse con cada VM sin requerir agentes internos. El dispositivo virtual garantiza que las VM tengan seguridad actualizada sin el impacto de los recursos de los agentes en cada VM. El dispositivo o *virtual appliance (vAPP)*, también serializa los análisis de seguridad y las actualizaciones para preservar el rendimiento.

La seguridad sin agentes para la virtualización se puso a disposición, por primera vez para antivirus, a través de la integración de VMware vShield Endpoint, con soluciones de *partners* específicos de seguridad como Trendmicro o McAfee. Este enfoque de protección sin agentes se aplica a una seguridad basada en archivos más amplia, donde se incluye la supervisión de la integridad de los archivos y el hipervisor, así como la seguridad basada en la red; prevención de intrusiones, firewall, etc.

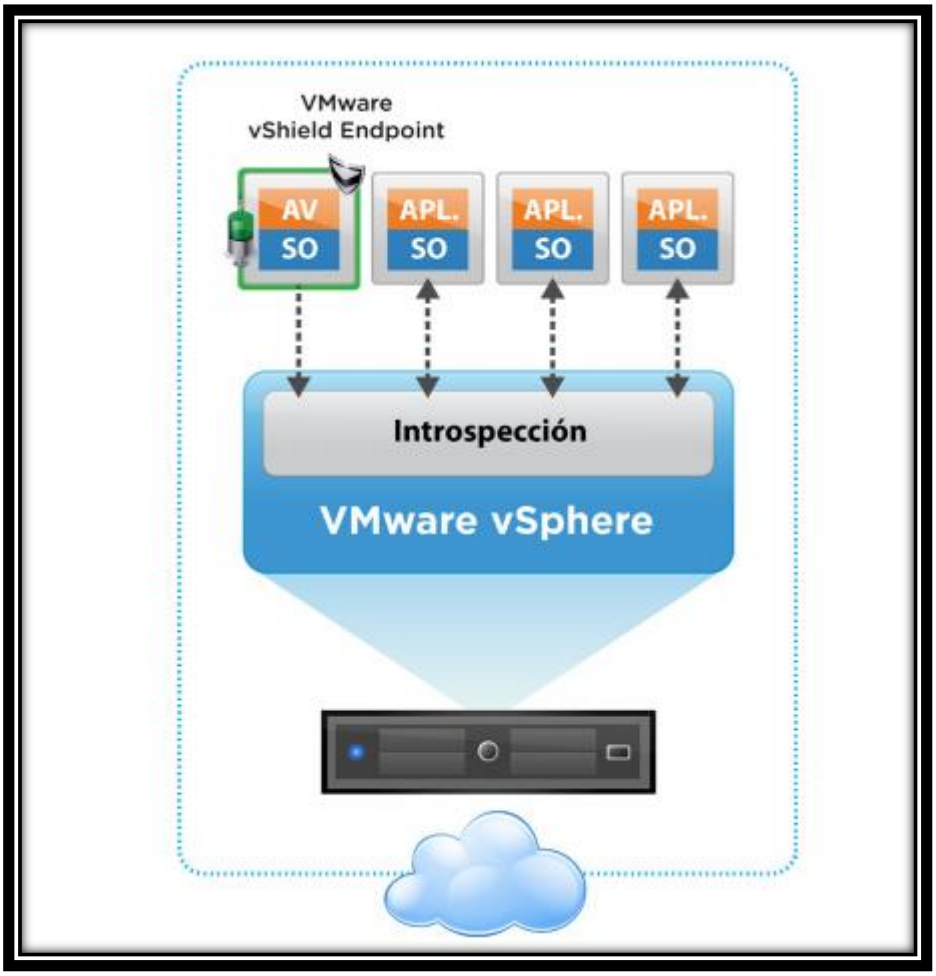


Figura 19: vShield de VMWARE Inc. VMware Inc.

Por lo tanto, se puede confirmar que una de las premisas de la protección sin agentes o *agentless* consiste en liberar la carga de trabajo del *software* de protección, que pasa a uno o varios dispositivos centralizados, además de consolidar otras capas de seguridad de red, anteriormente vinculadas a dispositivos físicos dedicados o que corrían en los propios sistemas con la considerable utilización de recursos. Por ejemplo, *firewalls*, *reverse proxies*, IDSs, IPSs, etc.

No obstante, el modelo sin agentes tiene un inconveniente ya que no cubre todos los servicios de protección proporcionados por algunos de los *partners* de seguridad del mercado, por ejemplo, funciones presentes en la mayor parte de los productos de seguridad como eliminación permanente de documentos y cifrado de los discos.

3.5.1 vShield

El vShield de VMware [28] es un conjunto de dispositivos virtuales de seguridad creados para la integración de VMware vCenter Server y otras plataformas de

gestión de la seguridad. Este producto OpenSource de VMware (vShield[11]), sienta las bases para mejorar la seguridad en este tipo de entornos, siendo un componente de seguridad crítico para proteger los centros de datos virtualizados de ataques y un uso indebido de la información.

vShield incorpora dispositivos y servicios esenciales para proteger las máquinas virtuales, pudiendo ser configurada a través de una interfaz web, como complemento de vSphere Client, vía CLI o API REST.

Cada vCenter incluía un vShield Manager, no obstante, los componentes que gestiona requieren licencia independiente.

- vShield Application
- vShield Data Security
- vShield Edge
- vShield Endpoint[12]

Entre los componentes indicados cabe destacar el servicio vShield Endpoint [29] , ya que, utilizado junto a una solución antimalware compatible, la cual interactúa vía API, proporciona los beneficios siguientes en un entorno VMware:

- **Eliminación de las tormentas de antivirus.** Se concentra la actualización de los archivos de firmas y los análisis antivirus en uno o dos dispositivos virtuales distintos con el fin de que los sistemas finales no tengan que realizar ningún análisis ni aplicar actualizaciones.
- **Optimización y especificación de recursos.** Se trasladan los requisitos de memoria y procesamiento relacionados con la protección de *software* al dispositivo virtual compartido, los recursos reservados a la máquina virtual son únicamente destinados al servicio objeto de esta.
- **Arranque más ágil y eficiente.** La implementación de los archivos de firmas y de base de datos en el dispositivo suprime la necesidad de cargar el archivo de firmas y de buscar actualizaciones durante el arranque.
- **Eliminación del retardo en la propagación de actualizaciones.** Se minimiza el tiempo de espera en la propagación de actualizaciones por todo el entorno virtual, éstas se aplican inmediatamente una vez que el dispositivo de protección las haya descargado.

[11] vShield https://my.vmware.com/web/vmware/downloads/details?productId=183&downloadGroup=VSHIELD10-OS-L

[12] vShield Endpoint https://my.vmware.com/web/vmware/downloads/details?productId=235&downloadGroup=VSHIELD_OSS501

- **Simplificación de la Operativa.** El mantenimiento pasa de realizarse en cada en equipo a realizarse únicamente en el *software* AV del dispositivo virtual.
- **Auditoría central.** El dispositivo virtual almacena registros y códigos de seguimiento, resultando la realización de auditorías o seguimientos menos compleja.

Otro de los componentes a destacar es el vShield Edge, el cual proporciona seguridad de red y servicios de puerta de enlace, aislando las máquinas virtuales en un subconjunto virtual de puertos lógicos, un switch distribuido virtual (vDS) o un Cisco Nexus 1000V. Este componente pude conectar redes locales aisladas, denominadas *stub*[13] o *pocket* networks, con otras redes compartidas, proporcionando servicios comunes como DHCP, VPN, NAT y balanceo de carga. Las implementaciones comunes de vShield Edge incluyen DMZ, VPN, y la base para los entornos *multi-tenant* en la Cloud proporcionando seguridad perimetral en los centros de datos virtuales (VDC) [30].

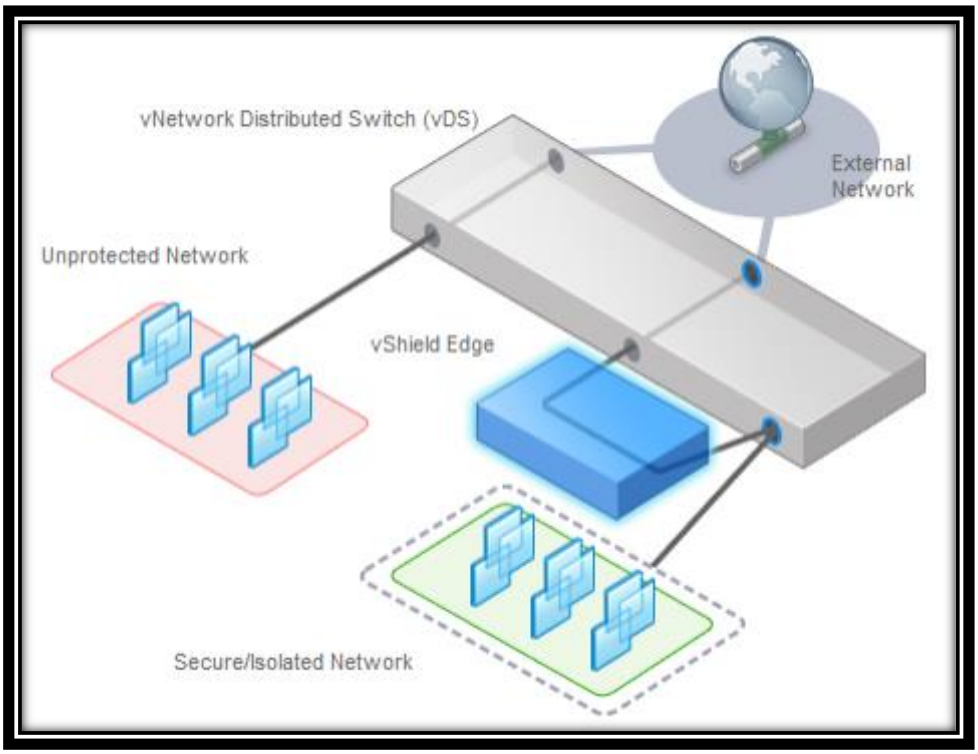


Figura 20: vShield Edge desplegado para securizar un vDS. VMware Inc.

vShield, por una estrategia empresarial de VMware es discontinuado, y sustituido a finales de 2013 por vCloud Security and Networking, que a diferencia de vShield, no es OpenSource. Posteriormente, este producto es englobado dentro

[13] Redes stub
https://www.techopedia.com/definition/9558/stub-network

de NSX; suite actual de redes y seguridad de VMware que se detalla a continuación.

3.5.2 NSX

NSX es un producto de VMware para virtualización de redes y seguridad. Permite la implementación de redes virtuales en su red física y dentro de su infraestructura de servidor virtual, además, ofrece el modelo operativo de una máquina virtual, en este caso, específico para la red. NSX se puede categorizar como una solución de redes definidas por software (SDN), que permite a los administradores de red inicializar, controlar, modificar, y administrar de manera dinámica el comportamiento de la red y la seguridad.

VMware menciona las siguientes premisas de NSX[14] : “Active su red virtual para conectar y proteger aplicaciones en su centro de datos, múltiples nubes, hipervisores *baremetal e* infraestructura de contenedores. VMware NSX Data Center ofrece una plataforma completa de virtualización de seguridad y redes L2-L7…”

Con este producto se observa como VMware extiende las tecnologías de virtualización a toda la infraestructura del centro de datos físico. NSX se complementa con vSphere, clave para una arquitectura SDDC, aportando a las redes lo que ya se ofrecía en términos de capacidad de procesamiento y almacenamiento. De manera muy similar al modo en que la virtualización del servidor, mediante programación, crea, elimina y restaura máquinas virtuales basadas en *software*, la virtualización de redes con NSX, mediante una programación similar, crea, elimina y restaura redes virtuales. El resultado es un concepto de redes evolucionado, que no solo permite que los administradores del centro de datos obtengan mayor agilidad y menor inversión, sino que también permite la implementación de un modelo operativo muy simplificado para la red física subyacente. Debido a que se puede implementar en cualquier red IP, incluidos los modelos de redes tradicionales existentes, y las arquitecturas de última generación de cualquier proveedor.

Con el fin de entender conceptos posteriores de seguridad, y de estos nuevos entornos de redes, se describen a continuación los componentes y los planos del NSX.

[14] VMware products portfolio NSX
https://www.vmware.com/products/nsx.html

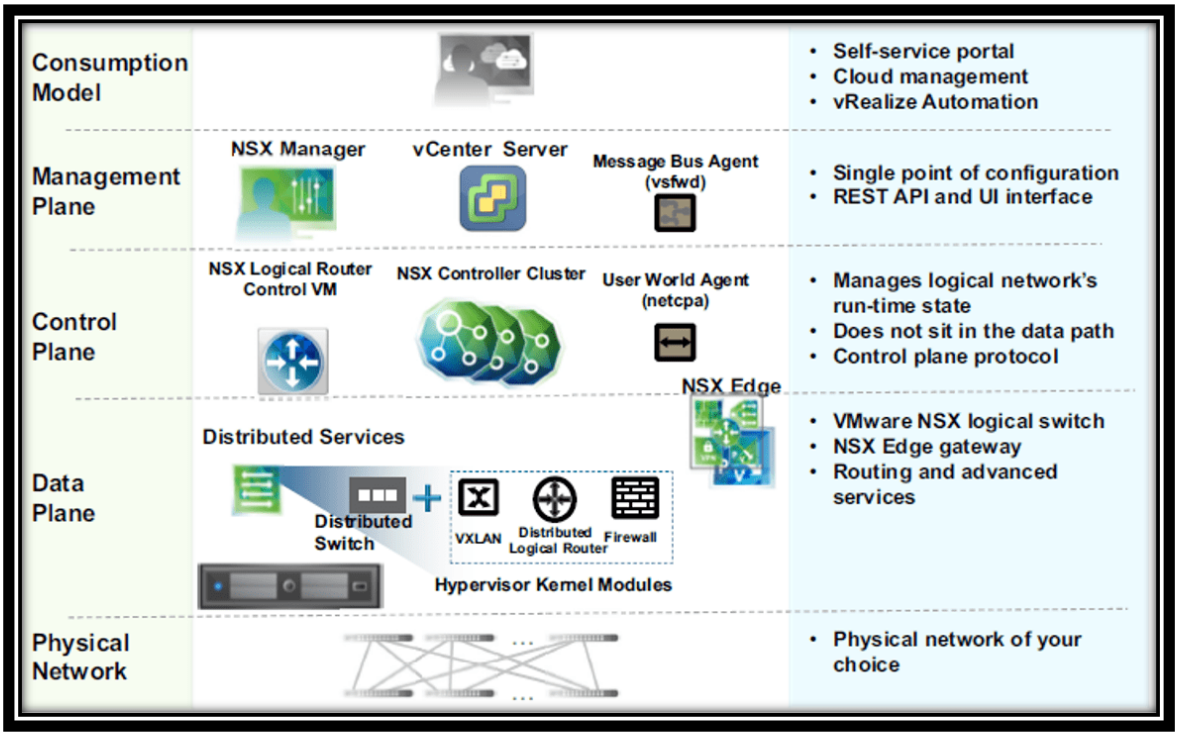


Figura 21: Planos del NSX y componentes. [31]

Se podría describir un equipo de red cualquiera dividiendo en tres planos distintos sus funciones. Estos planos, al igual que en NSX, son el plano de gestión, el plano de control, y el plano de datos. En algunos equipos modulares, como pueden ser los Catalyst de Cisco o los EX de Juniper, estos planos están físicamente definidos, una controladora o supervisora es la responsable del plano de control y gestión, mientras que otras tarjetas son los módulos de I/O del plano de datos.

El plano de gestión, por norma general, tiene la responsabilidad de permitir el acceso al equipo por una red o canal dedicado de este plano. Algunos equipos disponen de interfaz web, línea de comandos, etc. NSX permite, como se ha identificado en otros productos de VMware, el soporte de API REST. Esto facilita gestionar el equipo a través de orquestadores propios como el vCloud Director o de terceros como Cloudforms, CloudOpera u otras soluciones. En NSX el plano de gestión es responsabilidad del NSX Manager, y la principal interfaz de gestión es el cliente web, sin olvidar API REST.

El plano de control, por ejemplo, incluye tareas como averiguar la topología de la red, enrutamientos dinámicos, caminos lógicos, etc. Esta tarea es responsabilidad de ciertos protocolos según el tipo de equipo. En el caso de un *switch,* se podría hablar de STP, MPLS, tablas MAC, BPDUGuard, etc., mientras que en un *router* se podrían identificar OSPF, BGP, ACLs, etc. [32].

El plano de control, dentro de NSX, es responsabilidad del componente NSX Controller. Esta función del plano de control debe realizarse por un cluster de, al menos, tres VMs entre las cuales se distribuyen las diferentes tareas de control. El número de tres *controllers* o VMs se define así en las *best-practice*[15] de implantación de VMware. La ventaja de varias instancias del NSX Controller, además de HA y reducir aspectos como *split-brain,* es intentar distribuir la carga de control de manera equilibrada, utilizando una técnica denominada *slicing*[16]*.*

Por último, el plano de datos. En los equipos convencionales recae la responsabilidad de conmutar tramas, recibirlas en un puerto, analizarlas, y tomar una decisión en base a información del plano de control. Esa tarea puede ser ejecutada por un circuito electrónico (ASIC) o por una procesadora del equipo. Sin embargo, en NSX existen varios componentes responsables de gestionar las tramas de manera centralizada en una VM como es el caso de NSX Edge router o distribuida; vDS (virtual Distribute Switch), DLR (Distributed Logical Router), etc.

Aunque se esté haciendo foco en productos de VMware, en escenarios de *cloud* hibrida, con proveedores de virtualización diferentes se deben comprobar las matrices de compatibilidad de los productos. Sí la plataforma de virtualización es heterogénea, respecto a fabricante, se debe tener en cuenta que VMware dispone de NSX-T, con soporte para múltiples hipervisores y plataformas de Cloud; vSphere ESXi, KVM, OpenStack, Pivotal, Openswift, Kubernetes, Docker, etc. En resumen, ha sido diseñado con la idea de soportar aplicaciones emergentes, arquitecturas heterogéneas, y adaptadas a la tendencia del uso de contenedores.

Una vez se ha detallado la evolución de la virtualización, dentro del centro de datos, se pretende presentar la transición a la nube que, aunque aquí se refleja posteriormente, ha sido adoptada por múltiples compañías, cronológicamente hablando, antes que tecnologías de virtualización de red como NFV o SDN.

3.6 Transición a la nube y seguridad

3.6.1 Transición a la nube

Como se ha ido describiendo, el término computación en la nube es un concepto que abarca diferentes tecnologías y, en definitiva, diversos aspectos del mundo TI. Esta arquitectura, que ha dejado de ser novedad pero que sigue

[15] Implementar clúster de NSX Controller https://docs.vmware.com/es/VMware-NSX-Data-Center-for-vSphere/6.3/com.vmware.nsx.install.doc/GUID-ADAED74E-4796-4826-B138-2F9EFF0AB427.html

[16] https://www.vstellar.com/2016/08/27/learning-nsx-part-3-deploying-nsx-controllers/

consolidándose, permite distribuir la carga de trabajo y procesos de forma ágil, abriendo una nueva puerta a los servicios distribuidos descentralizados y con consumo bajo demanda. Este nuevo modelo emerge como un nuevo paradigma capaz de proporcionar recursos de cálculo y de almacenamiento que, además, resulta especialmente apto para la explotación comercial de las grandes capacidades de cómputo de proveedores de ISP.

Tal y como se puede ver en el informe de Cloud Computing en España de 2020 [33], en artículos de medios de Cloud [34] o en algún cuadrante mágico de la consultora Gatner, el concepto Cloud se establece en el escenario de las plataformas TI. En España, por norma general, las grandes empresas han ido por delante de las PyMES en la utilización de servicios en la nube. No obstante, en líneas generales y como se puede ver en la Figura 22, la estrategia de *cloud* debe seguir madurando y evolucionando.

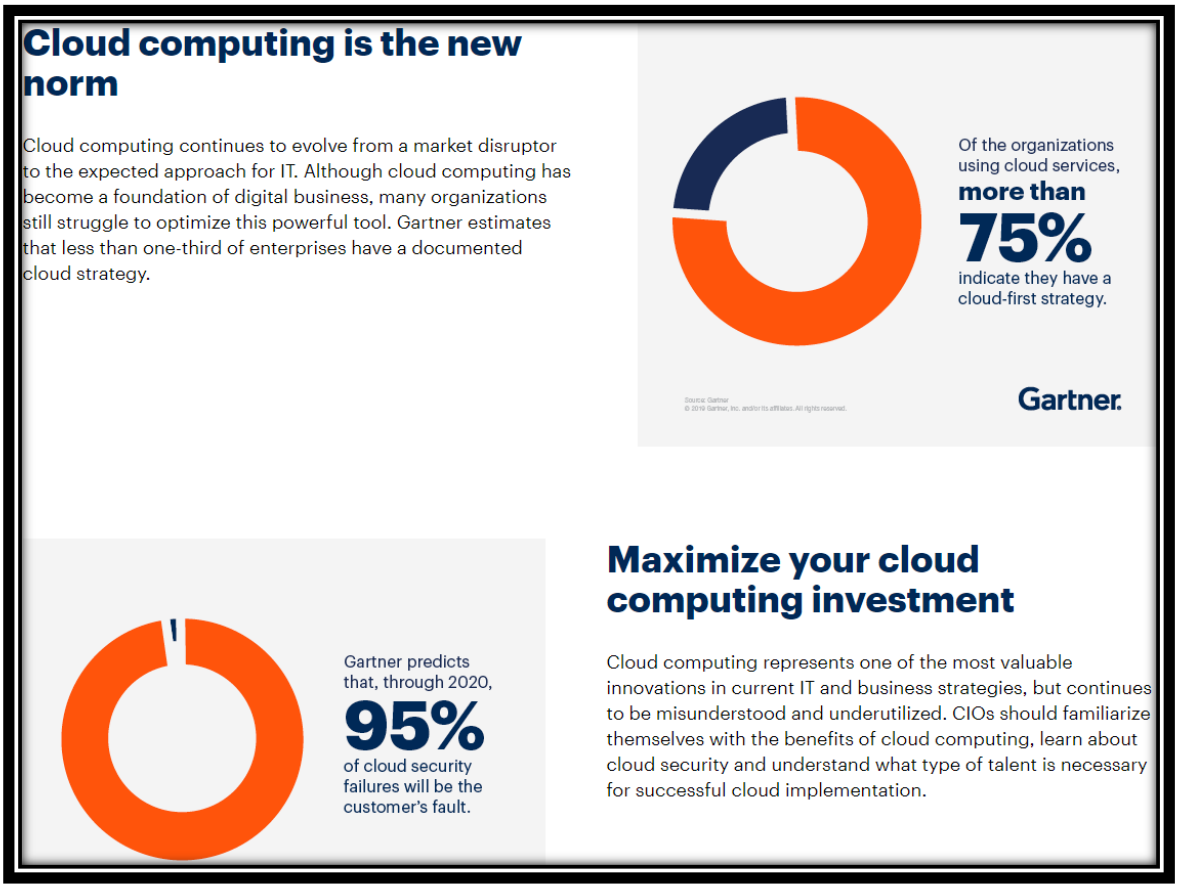


Figura 22: Advanced Cloud Computing Gartner [35]

La principal causa del crecimiento en los últimos años, y de la predicción de las diversas consultoras, son los beneficios que obtienen las empresas al implementar este tipo de soluciones: movilidad total, ya no solo dentro del centro de datos sino una descentralización y deslocalización de la información, reducción de fallos y costes, además de otros aspectos como la continuidad de

negocio en caso de desastre, y cuestiones como la privacidad y la integridad de la información.

Por lo tanto, aunque hoy se conocen muchos beneficios, no es requisito migrar todos los servicios o infraestructura a la nube, es más, se recomienda realizarlo de forma gradual, aunque cada empresa debe decidir su hoja de ruta en función de las características de su negocio, estrategia, y los servicios que demanda u ofrece. Para que la adopción de modelos *cloud* sea posible, debe establecerse una directriz en el proceso de provisión y gestión de todo recurso TI susceptible de ser migrado; aplicaciones, plataformas e infraestructuras.

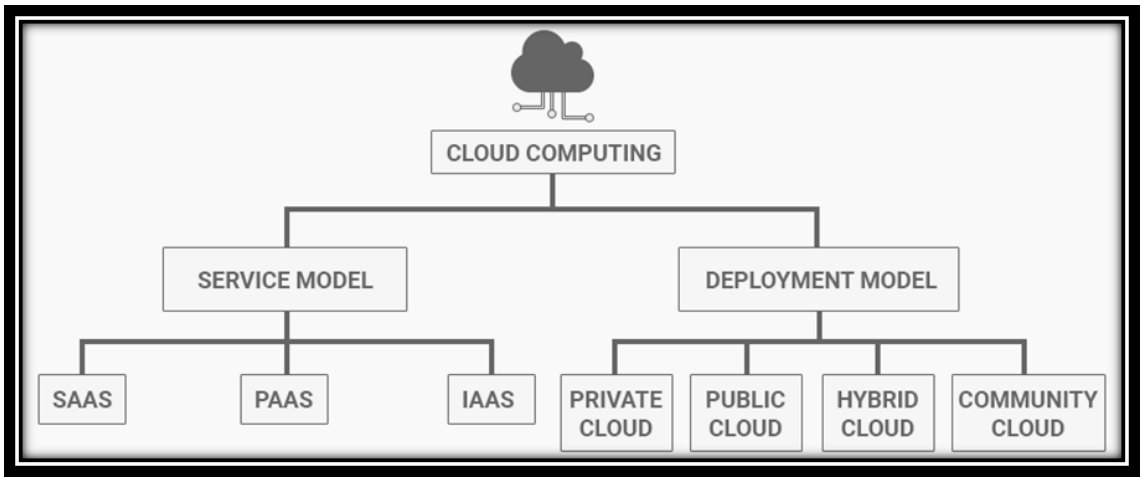


Figura 23: Tipos y modelos de Cloud. "Trending CC statistics" [36]

Al principio existían dos o tres tipos de infraestructuras *cloud* y varios modelos de servicio, aunque hoy en día se ha ampliado ese número, especialmente en los modelos de servicio. Los tipos, por ejemplo, pueden distinguirse según la titularidad de la infraestructura, es decir, pública, privada, comunitaria e hibrida. Por otro lado, hoy en día se utiliza el termino *multicloud*, que se refiere a la combinación de más de una implementación en la nube del mismo tipo, por ejemplo, en la utilización de dos proveedores públicos y uno privado se estaría dando una *multicloud* hibrida.

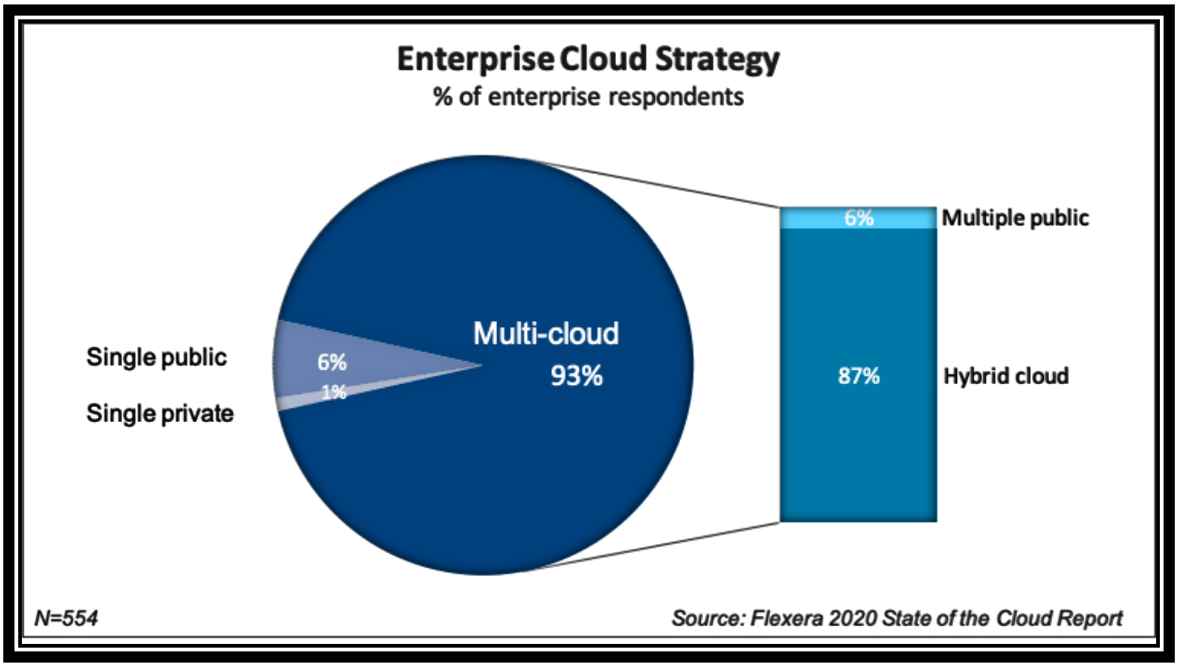


Figura 24: Estrategia empresarial Cloud 2020. Informe "State of the Cloud Report" Flexera 2020.

Como se ha indicado en otros puntos de la memoria, existen diferentes proveedores de *cloud* pública:

- Amazon EC2
- Microsoft Azure
- Google Cloud Platform
- IBM Cloud
- Alibaba Cloud

Se considera que no es objeto de este proyecto detallar los componentes y modelos de servicio de este tipo de proveedores, que además disponen de soluciones propietarias de seguridad y que, por norma general, son diferentes. El proveedor de servicios controla la infraestructura subyacente y el cliente no dispone de recursos dedicados para la implementación de una solución específica de seguridad. Esto obliga, en algunos casos, a intentar dar una capa extra de seguridad utilizando agentes en las máquinas virtuales, como si de un sistema tradicional se tratase o, por el contrario, a contratar los servicios adicionales de seguridad. No obstante, se deja el siguiente enlace de referencia para su consulta CompareCloud[17].

[17] http://comparecloud.in/

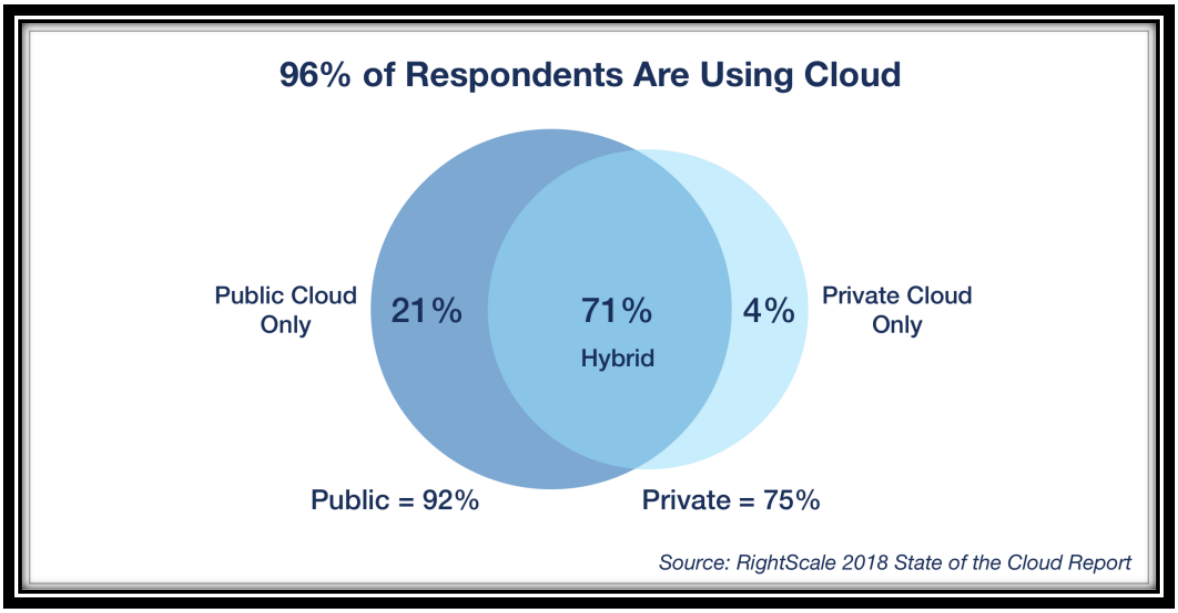


Figura 25: Tipos y modelos de Cloud [36]

En definitiva, se considera más relevante para este proyecto el análisis de la transición a la nube privada, ya que se ha realizado tanto por empresas grandes como medianas. Tal y como se puede observar en la Figura 25, prácticamente todas las empresas que han realizado el proceso de transición a la nube disponen de un entorno híbrido, es decir, utilizan tanto nube privada como pública. Con lo expuesto anteriormente sobre las soluciones de seguridad propietarias de las grandes empresas de *cloud,* se detallará en el punto cuatro las soluciones que se centran, principalmente, en entornos de nube privada.

Referente a los modelos de servicio, aunque existen muchos más actualmente, el comienzo se basó en tres: IaaS, PaaS y SaaS, como se puede ver en el siguiente enlace de Amazon "Tipos de informática en la nube"[18]. Estos modelos prácticamente cubren todas las necesidades, aunque existen términos como BaaS (Backup as a Service), EaaS (Email as a Service), PCaaS (Parallel Computing as a Service) o CaaS (Container as a Service), que se agrupan dentro del conjunto XaaS o Everything as a Service, conocidos también como modelos de *cloud* emergentes.

3.6.2 Seguridad en Cloud

En los inicios de la transición a la nube, una de las mayores preocupaciones se centra en aspectos como la gestión de los datos; fundamentalmente en la propiedad de estos y la forma de gestionarlos por parte de los proveedores, así como en la identificación y control de acceso a los recursos. Esto incluye la

[18] https://aws.amazon.com/es/types-of-cloud-computing/

protección de información crítica frente al robo, la filtración de datos y la eliminación de estos.

En este punto, se plantean las consideraciones de seguridad de infraestructuras y servicios en la nube, ya que afectan a la infraestructura de nuble pública y privada, con el objetivo de contrastarlos con las soluciones de seguridad. Por ejemplo, las amenazas identificadas por la organización CSA (Cloud Security Aliance), y aspectos clave de la seguridad según NIST (National Insitute of Standars and Technology.

La CSA se define como una organización internacional sin ánimo de lucro para promover el uso de mejores prácticas para garantizar la seguridad en cloud. Cada año publican un informe denominado “Top Threats to Cloud Computing” [37] , sobre las mayores amenazas de la infraestructura *cloud,* con el propósito de guiar a las diferentes organizaciones. Estas amenazas se actualizan regularmente buscando el consenso de los expertos. Se debe tener en cuenta que algunas amenazas descritas anteriormente, en el apartado 3.4 Seguridad en entornos virtualizados, están directamente relacionadas.

Por otro lado, el NIST dispone de varios informes y recomendaciones, distribuyendo las buenas prácticas por áreas.

Área	Recomendación
Arquitectura	Entender las tecnologías que sustentan la infraestructura del proveedor para comprender las implicaciones de privacidad y seguridad de los controles técnicos.
Aislamiento de software	Analizar el tipo de virtualización y otras técnicas de aislamiento que el proveedor emplee y valorar los riesgos implicados
Confianza	Incorporar mecanismos legales en el contrato que permitan controlar los procesos y controles de privacidad empleados por el proveedor.
Control de acceso	Asegurar las salvaguardas necesarias para hacer seguras la autenticación, la autorización y las funciones de control de acceso.
Cumplimiento	Comprender la legislación y las regulaciones, además de su impacto potencial en los entornos en la nube. Revisar y valorar las medidas del proveedor con respecto a las necesidades de la organización.

Disponibilidad	Asegurar que, durante un corte de servicio prolongado, las operaciones críticas se pueden reanudar inmediatamente y acto seguido, el resto de las operaciones, en un tiempo adecuado a cada servicio.
Gobernanza	Implantar políticas y estándares en la provisión de servicios *cloud*. Establecer mecanismos de auditoría y herramientas para que se sigan las políticas de la organización durante el ciclo de vida.
Respuesta ante incidentes	Gestionar los contratos de los proveedores. Entender los procedimientos externos e internos para la respuesta a incidentes requeridos por la organización.

Figura 26: Buenas prácticas de seguridad según el NIST[38]

Una vez planteado el escenario de amenazas, tanto en entornos virtuales como en entornos *cloud*, se introduce la evolución de los sistemas de seguridad; desde un agente de antivirus tradicional a las plataformas de gestión centralizada.

3.7 La evolución del antivirus convencional, EPP, EDR y XDR

El uso de antivirus sigue siendo fundamental hoy en día. No obstante, Internet ha aumentado de forma exponencial en los últimos 15 años, lo que ha propiciado también el crecimiento de forma progresiva del número de ataques e intrusiones en los sistemas informáticos, tanto a nivel empresarial como particular.

Este hecho constatado ha forzado que los antivirus hayan evolucionado hacia otro tipo de aplicaciones más avanzadas, que no sólo buscan detectar, bloquear y desinfectar virus informáticos, sino reconocer otros tipos de aplicaciones nocivas y detectar diferentes ataques. Para hablar de la evolución del antivirus tradicional, se debe mencionar, también, la evolución que ha tenido este tipo de aplicaciones mal intencionadas, es decir, el *malware.*

El término *malware* (*malicious software*), es un término amplio que hace referencia a todo aquel *software* que perjudica a un dispositivo o daña un sistema. Con el paso del tiempo ha ido evolucionando, presentándose en múltiples variedades según el objetivo que persigue. Hoy en día se pueden categorizar en diversas familias cuyo detalle, por ejemplo, puede consultarse en

los siguientes artículos “9 types of malware and how to recognize them” [19]y “What are the different types of Malware?”[20] .

Las motivaciones de los creadores de *malware* presentan una evolución clara en estos tipos, del reconocimiento personal hacia motivos económicos, como puede verse desde el dos mil quince hasta hoy en día. Este *software* es más sofisticado y difícil de detectar, presentando desarrollos más complejos y capacidades avanzadas para pasar inadvertido. Los ataques son espaciados y coordinados, y utilizan varios vectores simultáneamente, lo que se denomina APT (Advanced Persistent Threat). Estos ataques, cuyos fines pueden ser espionaje industrial, robo de tarjetas, cifrado de archivos sensibles, etc., están a la orden del día y pasan, prácticamente desapercibidos, bajo el radar de muchos antivirus.

El antivirus tiene un modo de operación simple, basado en un análisis regular de la máquina. Ofrece tres tipos de análisis para detectar y bloquear acciones o programas maliciosos:

- **Escaneo de firmas:** El AV detecta y lee el *hash* de cada programa, y lo comparará con los almacenados en su base de datos. Si la clave del producto de *software* coincide con la de un programa malicioso, se bloquea, elimina o se pone en cuarentena.
- **Análisis heurístico:** El análisis heurístico permite identificar nuevos virus que aún no están registrados en las bases de datos de los proveedores de AV. Este análisis se basa en el supuesto comportamiento de un programa. Al lanzar un programa, se lanza en paralelo en un *sandbox* y se analiza su comportamiento. Si algunas de sus acciones son sospechosas, como puede ser la eliminación de ficheros, inicialización de múltiples procesos, se envía una alerta.
- **Análisis de integridad**: Cuando se enciende la máquina, a intervalos regulares y tan pronto como se modifica un archivo, el antivirus lanza un nuevo análisis para verificar que ningún archivo haya sido modificado o dañado por *software* malicioso.

El antivirus es el programa de protección más conocido y extendido, y tal y como se ha indicado al inicio del apartado, sigue siendo necesario. Es un *software* que tiene un precio económico por dispositivo y que es relativamente sencillo de configurar y utilizar. Sin embargo, debido a su perenne modo de funcionamiento, tiene limitaciones. La protección proporcionada por un antivirus es básica y suele ser posible su anulación de manera sencilla, por ejemplo, la búsqueda de firmas

[19] https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html

[20] https://comtact.co.uk/blog/what-are-the-different-types-of-malware/

de productos solo es relevante si el *malware* está en la lista. Un usuario malintencionado pueda crear un script cuyo hash aún no se encuentre en la lista y realizar un ataque que no será detenido por el antivirus.

De la misma forma, hoy en día existen ataques sin archivos y, por tanto, sin firmas, que permiten atacar una máquina, aun estando protegida por un antivirus. Por otro lado, aunque sus funcionalidades han ido evolucionando con el tiempo, no se han adaptado al mismo nivel que los desarrollos indicados en el área del *malware*. De hecho, las nuevas funcionalidades se han ido agregando como diferentes módulos, en una superposición que proporciona agentes pesados y que consume recursos de manera notable, tanto en memoria como en CPU.

Estas nuevas funcionalidades, entre otros aspectos, dan lugar a la aparición de los EPP. El EPP es una solución que se implementa en sistemas o dispositivos finales para prevenir ataques basados en archivos, detectar actividades maliciosas, y proporcionar las capacidades de investigación y corrección necesarias para responder a incidentes de seguridad dinámica. Es decir, se mantiene el esquema de escaneo de firmas, pero se brindan nuevas funciones más avanzadas, por ejemplo:

- **Análisis de comportamiento:** Debido a la implementación de un motor de aprendizaje automático, el EPP puede identificar acciones y archivos que pueden considerarse maliciosos
- **Monitorización de la memoria:** El *software* de protección analiza en tiempo real, durante la ejecución de un programa, si este último corrompe la memoria del sistema o de otro programa.
- **Verificación de IOC o indicador de compromiso:** El EPP identifica en la máquina cualquier archivo o clave de registro que pueda estar vinculado a un ataque gracias a la inteligencia de amenazas, no tiene que mantener una base de datos local de todas las IOC conocidas, ya que puede verificar las últimas actualizaciones sobre objetos que no puede clasificar.

Por tanto, estas incorporaciones hacen que el EPP sea más apropiado que un AV para la protección de máquinas en un entorno empresarial, en la medida en que su espectro de protección es más amplio que el de su predecesor. No obstante, no es infalible. Puede detectar un volumen de *malware* superior al de un antivirus, pero no bloquea ni detecta ciertos tipos de ataques o intentos de corrupción del sistema o de los datos, lo que fuerza un siguiente paso; los EDR.

Los EDR o Endpoint Detection & Response, son el modelo siguiente de *software* de protección. Se trata de una revolución en toda la tecnología de protección contra virus, *malware* y ataques de usuarios malintencionados. El EDR incorpora nuevas herramientas para brindar una protección más completa. De hecho, a

diferencia de AV y EPP, los EDR pueden identificar y detener amenazas incluso antes del inicio de la corrupción del sistema, gracias a una recopilación de datos significativa en comparación con otras soluciones de protección. El conjunto de herramientas utilizado para lograr esto incluye, entre otros, lo siguiente:

- Un motor de detección, que utiliza técnicas como la estructura basada en aprendizaje automático. Utiliza IA (Inteligencia Artificial).
- Análisis y *sandboxing* emulativo para detectar y prevenir muestras de código. Defensa contra un amplio rango de *malware*, como *ransomware*, *botnets* y otras amenazas conocidas y desconocidas; accesos no autorizados, robo de datos, etc.
- Un motor de análisis en tiempo real, que monitoriza la memoria y busca patrones en comportamiento, lo que permite la detección de *exploits* y el diagnóstico rápido de código más complejo, y amenazas previamente desconocidas.
- Inteligencia de amenazas aplicada, que puede provenir de varias fuentes independientes.
- Visibilidad en todos los puntos finales; fundamental para detectar actividades maliciosas.
- Monitorización y registro de datos de eventos en tiempo real, así como su recopilación para su utilización posterior en diferido. Permite un bloqueo avanzado de amenazas
- Herramientas forenses para investigar infracciones pasadas y detectar amenazas, no identificadas, que podrían mantenerse inactivas en un *endpoint.*
- Respuesta a incidentes; generación de alertas y respuestas automáticas.
- Filtrado de incidentes para evitar falsos positivos y una sobrecarga de alertas innecesarias.

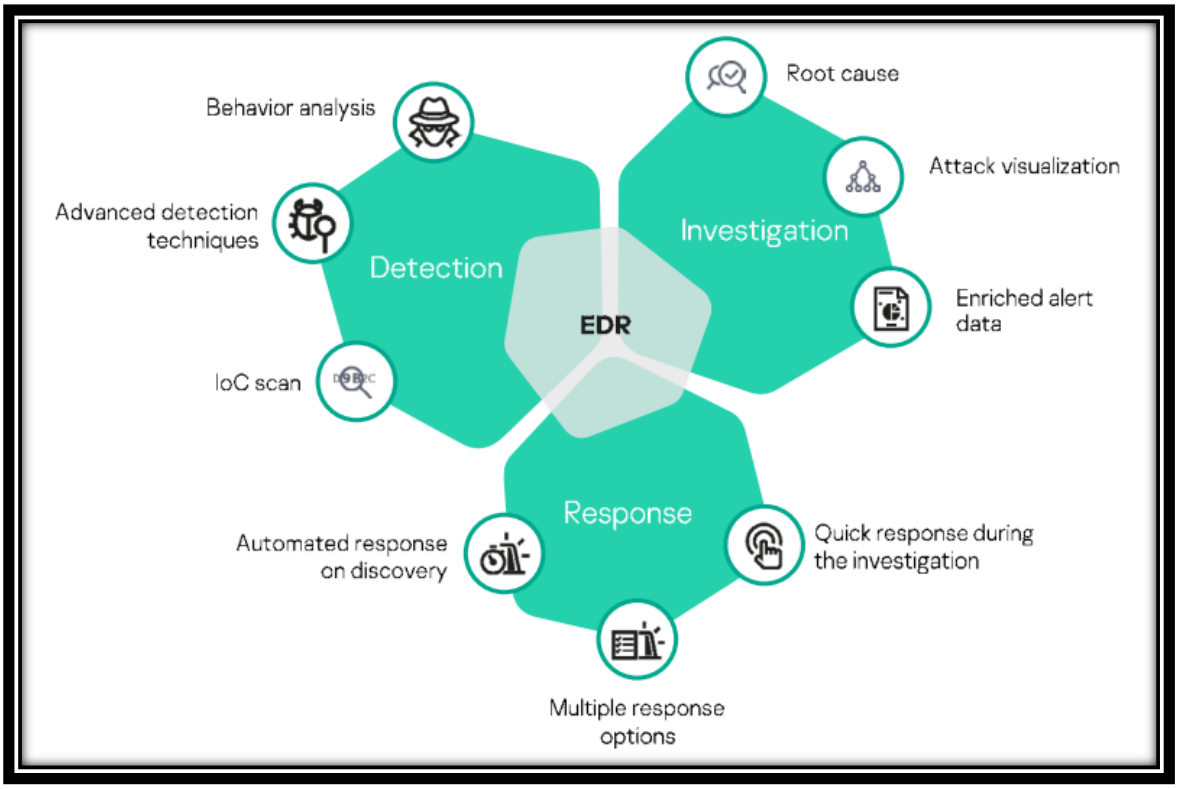


Figura 27: Capacidades principales de un EDR [39]

En resumen, el EDR está enfocado en amenazas avanzadas, las diseñadas para evadir la primera capa de defensa y que logran penetrar en la red. Por lo tanto, intenta prevenir esa actividad y contener el ataque antes de que pueda desplazarse transversalmente en el entorno o en la red, mejorando notablemente las siguientes áreas:

- Detección
- Contención
- Investigación
- Eliminación

Aunque existen otros términos como MDR/MTR o MSSP, se considera relevante mencionar XDR o Extended Detection and Response.

Básicamente, se puede definir como un concepto transversal dentro del modelo detallado de EDR, donde la "X" se refiere a la capacidad de detección de amenazas y respuesta a través de múltiples controles de seguridad, considerando tanto la actividad de la red como de los terminales. En resumen, se puede hacer referencia a XDR, también, como la convergencia de soluciones SIEM, DPI y EDR, es decir, se extienden modelos anteriores para agregar y correlacionar telemetría de controles de seguridad existentes, con otros adicionales, agregando capas de red, *cloud,* correo electrónico y otros servicios.

Por tanto, el alcance abarca tantos entornos físicos como virtuales, *cloud* privada o hibrida [40] , [41].

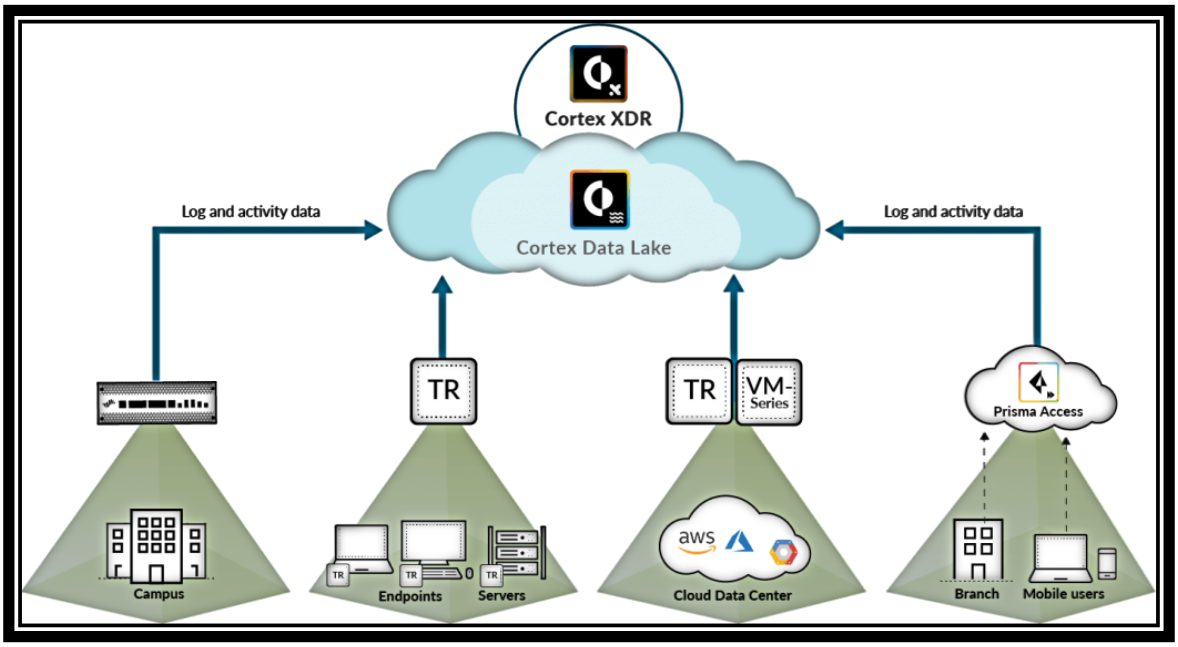


Figura 28: Cortex XDR Paloalto Inc.[42]

En dos mil veinte el mercado de soluciones EDR y XDR está en auge, además de las soluciones de seguridad integral para un modelo de centro de datos definidos por *software.* Estas soluciones se integran, según el tipo de empresa, con un SOC interno o externo, lo que da un valor añadido relevante.

Fabricantes como BitDefender, Kaspersky, Sophos, Trend Micro, Panda Security o Symantec han incorporado el EDR y XDR en su porfolio de productos, sin dejar de lado otros servicios que se detallan en el punto siguiente.

4. Soluciones de seguridad en virtualización

Históricamente, como se ha indicado en apartados anteriores, para proteger un sistema había que instalar una solución antivirus, sin embargo, se ha visto que actualmente estas aplicaciones únicamente protegen de un tipo de *malware* común, sin ciertas alteraciones. Como se ha detallado, esto se debe a que dicho término engloba muchos tipos de aplicaciones maliciosas, de ahí que los fabricantes de seguridad hayan ido desarrollando aplicaciones complementarias de *software* de protección o suites de seguridad con diferentes módulos, ya que no existía una herramienta específica que garantizase un entorno completamente libre de *malware*. Es decir, se considera que, con el rápido crecimiento de la virtualización y las amenazas en los últimos años, las medidas de seguridad para este tipo de entornos no han seguido el mismo ritmo de evolución. No obstante, muchas empresas existentes, y otras de nueva creación, han resuelto numerosos problemas, sin embargo, el campo de la virtualización continúa enfrentándose a desafíos de seguridad en muchas áreas, como la monitorización, la visibilidad, y la propia infraestructura que la sostiene.

La monitorización es la capacidad que tienen los centros de datos y las nubes de registrar datos confiables sobre las actividades en las máquinas virtuales o en los propios *hosts*. Por lo general, una empresa solo establece una defensa y monitorización en las redes perimetrales, que es una estrategia insuficiente ya que tienen una protección mínima contra las amenazas internas. Sin embargo, incluso para las empresas que brindan una monitorización interna, las características de la virtualización hacen que esta sea compleja. La capa de administración creada en la virtualización está destinada a abstraer los recursos subyacentes de las VM y, como se ha visto, debido a esta nueva capa, parte de la información se abstrae de los monitores de red perimetrales, lo que genera datos insuficientes para determinar amenazas potenciales. Además, los mecanismos de alta disponibilidad generan estados variables y movilidad de las máquinas virtuales, algo que los monitores o sondas no controlan.

La visibilidad se refiere a cuánto pueden ver los sistemas de detección y prevención de intrusiones en una red virtualizada. Es un tema relacionado directamente con la monitorización del tráfico; sin monitorización del mismo extremo a extremo, no habrá detección ni prevención. Este aspecto también es un problema para los propios proveedores de *software* de virtualización. Empresas líderes como VMware proporcionan una visión limitada del hipervisor y de la red virtual. Su implementación está desarrollada con la intención de proteger los *hosts* y la red de máquinas virtuales infectadas, sin embargo, esta característica también hace que disminuya dicha visibilidad en los sistemas

operativos de los *hosts* y las redes virtuales, dificultando la prevención de intrusiones mal intencionadas o la detección de máquinas virtuales infectadas.

La infraestructura no deja de ser la forma en que se instala, despliega y configura la virtualización en un centro de datos o en la nube. Numerosas empresas utilizan *software* de virtualización, de seguridad, y de servicios, de varios proveedores. Las configuraciones de esos centros de datos dependen, en gran medida, del *software* de los proveedores que han utilizado. Como resultado, la estructura de seguridad dentro de un centro de datos virtualizado debe ser muy específica para el centro de datos o la nube en particular, de ahí que cada empresa debe parametrizar sus servicios de una forma adecuada. Esto, a su vez, hace que la seguridad entre las bases de datos y las nubes se debilite debido a posibles malas praxis de configuración, incompatibilidades u otros problemas potenciales. Además, las diferentes medidas de seguridad para máquinas virtuales y *hosts* dentro de un centro de datos pueden causar incidencias o problemas imprevistos en la operativa de los servicios.

Los productos analizados, que se describen en el punto 4.3 Productos de seguridad en entornos virtuales, han cambiado la forma de concebir las aplicaciones de seguridad clásicas, orientando las mismas hacia el estudio de los patrones de comportamiento del sistema, es decir, una monitorización activa y detallada de las acciones que desencadenan las aplicaciones en los equipos. Por otro lado, se ha añadido el análisis global de usuarios o entidades, utilizando técnicas de inteligencia basadas en Data Mining y Big Data, además, la fortificación y securización de los sistemas operativos, impidiendo o minimizando la ejecución de cualquier proceso sospechoso de peligro, alertando y registrando toda actividad anómala.

Independientemente de la solución de seguridad adoptada, se debe seguir teniendo presente que numerosos problemas pueden provenir de las múltiples formas en las que se puede configurar una infraestructura de virtualización. Además, no es de extrañar que la forma más obvia de atacar un centro de datos virtualizado sea la de obtener acceso al hipervisor, pieza que controla todas las máquinas virtuales que se ejecutan en el *host o* incluso en el centro de datos, sí el ataque consigue salir del mismo. Por ello, se ha hecho foco, durante varios apartados de este trabajo, en el hipervisor. Incluyendo el acercamiento práctico en el punto 5. Caso práctico. Implantación, despliegue y securización**.** [43] [44]

4.1 Soluciones basadas en arquitectura de virtualización

Las soluciones basadas en la arquitectura de virtualización tienen como objetivo resolver vulnerabilidades mediante el empleo de medidas de seguridad en los

componentes y en las diferentes parametrizaciones del entorno virtual. Los tres enfoques principales son la seguridad del hipervisor, la seguridad del sistema operativo invitado, y la seguridad de la gestión de las imágenes.

- **Seguridad en el hipervisor:** La seguridad del hipervisor consiste en la aplicación de medidas de seguridad tradicionales. Este componente, como se ha ido referenciando durante el desarrollo del trabajo, es un activo básico de la seguridad de la virtualización. El hipervisor es una pieza clave de la capa de gestión de un sistema virtualizado. Por lo tanto, si el hipervisor está comprometido, también lo están todas las máquinas virtuales creadas o controladas por dicho hipervisor, además, podrían estar comprometidos otros elementos de la capa de virtualización u otros hipervisores. Siempre que la seguridad del hipervisor sea lo suficientemente fuerte, comprometer todas las máquinas virtuales será difícil para el atacante, de ahí que se dedique un apartado entero en este trabajo al *hardening* del hipervisor. Para la arquitectura de virtualización nativa, existen muchas formas físicas de garantizar el control de acceso al hipervisor. Un ejemplo sería un token de *hardware* que posee el administrador para lanzar el hipervisor. Para la arquitectura de virtualización alojada, las formas tradicionales de proteger los procesos en ejecución en un sistema operativo se implementan actualmente para proteger el hipervisor. Las medidas de seguridad como el control de acceso, la actualización automática, las redes y la introspección en los sistemas operativos invitados son todas formas de proteger el hipervisor del acceso no autorizado. Estos elementos de seguridad generalmente se implementan en software y se pueden actualizar fácilmente para mantener actualizadas las características de seguridad del hipervisor **¡Error! No se e ncuentra el origen de la referencia.**[45] .
- **Seguridad en el sistema operativo:** La seguridad del sistema operativo invitado es la aplicación de medidas de seguridad tradicionales a los sistemas operativos invitados. Esto puede parecer un proceso redundante para la seguridad del hipervisor, pero en la virtualización, cada componente o capa debe ser seguro para que el sistema virtualizado en conjunto sea seguro. Dado que los sistemas operativos invitados, que se ejecutan dentro de una máquina virtual, se comportan como un sistema operativo real en una máquina física, se deben implementar medidas de seguridad para estos sistemas en cada uno de ellos. Además, cada sistema operativo invitado debe tener suficiente aislamiento para que una VM comprometida no lleve a que otras VM en la misma máquina se vean comprometidas. Más importante aún, dado que los sistemas operativos invitados pueden utilizar los periféricos físicos disponibles en la máquina, la comunicación entre los sistemas operativos invitados y el hipervisor debe ser segura, y la abstracción proporcionada por el hipervisor debe aplicarse. Actualmente, muchas empresas de seguridad de virtualización están utilizando la supervisión del

sistema operativo invitado para detectar y poner en cuarentena los sistemas operativos invitados infectados o revertirlos a un estado anterior con imágenes almacenadas.

- **Seguridad de la gestión de imágenes:** Es la protección de cómo se almacenan, transportan y gestionan las imágenes de VM en un centro de datos virtualizado o en la nube. Este es un aspecto importante de la seguridad en la virtualización debido a la movilidad y al estado variable en cada VM, y cómo los atacantes aprovechan el hecho de que las medidas de seguridad son más débiles en la red o en los centros de datos de respaldo. Se debe tener presente que estas imágenes pueden almacenarse en formatos y medios, desde discos locales y NFS, hasta cabinas de almacenamiento FC y SAN, incluso en herramientas de respaldo como Avamar, Networker, NetBackup, etc. Por lo tanto, para lograr la seguridad de la gestión de imágenes, se debe aplicar un cifrado de almacenamiento sólido con el fin de que no se filtren datos confidenciales de las imágenes. Por otro lado, debe existir una sólida seguridad de red para garantizar el transporte seguro de las imágenes de las máquinas virtuales. Además, otro aspecto para tener en cuenta es que las imágenes de VM se pueden crear de forma rápida y sencilla, lo que puede generar muchos clones, copias y, en definitiva, muchas distribuciones innecesarias de la misma VM, vulnerabilidad generalmente conocida como expansión de VM. Para controlar la distribución innecesaria de imágenes de VM, se debe implementar un control de acceso en el despliegue o administración de imágenes. Las empresas de software de VM generalmente implementan diferentes niveles de autoridad para controlar cómo se puede administrar cada imagen para garantizar la seguridad de la administración de imágenes. Por ejemplo, en el caso de VMware se podría realizar desde el hipervisor, desde el vCenter o el vCloud, no obstante, siempre con la posibilidad de una granularidad de permisos muy exhaustiva.

Las soluciones descritas anteriormente son enfoques genéricos y transversales con el objetivo de lograr la seguridad en la virtualización, no obstante, la implementación real o el detalle práctico puede diferir según el tipo de empresa, servicios utilizados e infraestructura virtual. Es decir, además de proteger los componentes en la virtualización, las medidas de seguridad en la propia infraestructura pueden reducir en gran medida la posibilidad de ataques

4.2 Soluciones basadas en infraestructura de virtualización

Las soluciones basadas en la infraestructura de virtualización tienen como objetivo resolver las vulnerabilidades de seguridad mediante la creación de interfaces seguros en la infraestructura de virtualización. Este conjunto de soluciones se da principalmente para centros de datos de cierta envergadura y

nubes, tanto privadas como híbridas, ya que la infraestructura es una parte integral del proceso de despliegue. Las dos áreas donde se hace foco son la seguridad en la capa virtual y en la capa física:

- **Seguridad en la capa virtual:** Se consigue asegurando cómo las máquinas virtuales y los hipervisores se comunican entre sí dentro de la red virtual. Para aprovechar al máximo la infraestructura de virtualización, las redes privadas virtuales (VPN) se crean comúnmente para administrar diferentes niveles de autoridad en las VM. Debido a la naturaleza virtual de la red, las características como monitorización, controles de acceso, integridad, cifrado, autenticación, y movilidad de las máquinas virtuales se pueden implementar directamente en la red. Esto resuelve muchas de las vulnerabilidades presentes en una virtualización, ya que la seguridad en la capa virtual aislará diferentes redes de administración virtual, plano de control y datos, facilitando la implementación y operación de VMs en diferentes autoridades o centros de datos.
- **Seguridad en la capa física:** Se trata del diseño de la estructura de los sistemas físicos. Una de las características más notables en esta área es la detección y prevención de intrusiones en el *host*, que permite que el sistema se asegure de que, al menos, la capa física no se vea comprometida fácilmente por otros medios. La estructura del centro de datos o la nube también juega un papel importante; accesos físicos a los centros, conexionado, control de los servidores de consolas, etc. Otro aspecto es cómo las máquinas que ejecutan las VM interconectadas físicamente pueden determinar las posibles medidas de seguridad que se pueden utilizar. Además, la inspección de rutinas para detectar fallos de *hardware,* y *firmware* desactualizado, forman parte de la seguridad en la infraestructura física que tiene un papel relevante en la seguridad global del entorno virtualizado.

Está fuera del alcance de este proyecto detallar cómo se implementan las diferentes soluciones de seguridad que hay en el mercado. No obstante, los siguientes apartados presentan algunos de los productos actuales, para entornos virtualizados, que utilizan estas soluciones generales de seguridad que se han comentado en este punto.

4.3 Productos de seguridad en entornos virtuales

Como se ha ido analizando existen, hoy en día, una gran variedad de soluciones de seguridad, no obstante, este volumen no facilita la elección de una solución de protección. En gran parte, debido a que cada una de estas soluciones tiene funcionalidades muy específicas. Sin embargo, aunque es importante hacer esta elección a conciencia, es importante también en base al conocimiento de las necesidades de cada empresa o entorno. Por eso conviene conocer las

soluciones de protección presentes en el mercado, su modo de funcionamiento, sus ventajas, y también su alcance.

Algunos de los productos de referencia, en el mercado actual, son de los proveedores reconocidos históricamente: Kaspersky, Eset, Fortinet, TrendMicro, Symantec, etc. destacando algún otro proveedor como CrowdStrike, Cylance o F-Secure.

Algunas de las soluciones identificadas son:

- Trend Micro Cloud/Apex One
- Trend Micro Deep Security
- Sentinel One EPP
- VMware Carbon Black Cloud
- Kaspersky Endpoint Security for Business
- Checkpoint Endpoint Security
- F-Secure PSB Computer Protection 2.0
- Sophos Intercept X Advanced
- Cylance Protect
- ESET Endpoint Security

De las cuales, se presentan a continuación, cinco diferentes; en base a las evaluaciones por Gartner, el instituto AV-Test[21], y presencia del fabricante en el mercado. Como se puede ver en la Figura 29, algunas de estas soluciones han obtenido la puntuación general más elevada. Además, se adelanta que cualquier de estas soluciones que se presentan permiten programar o concertar una demo o prueba de concepto desde cualquiera de las páginas del producto.

[21] https://www.av-test.org/es/vista-general-de-productos-de-seguridad-it/

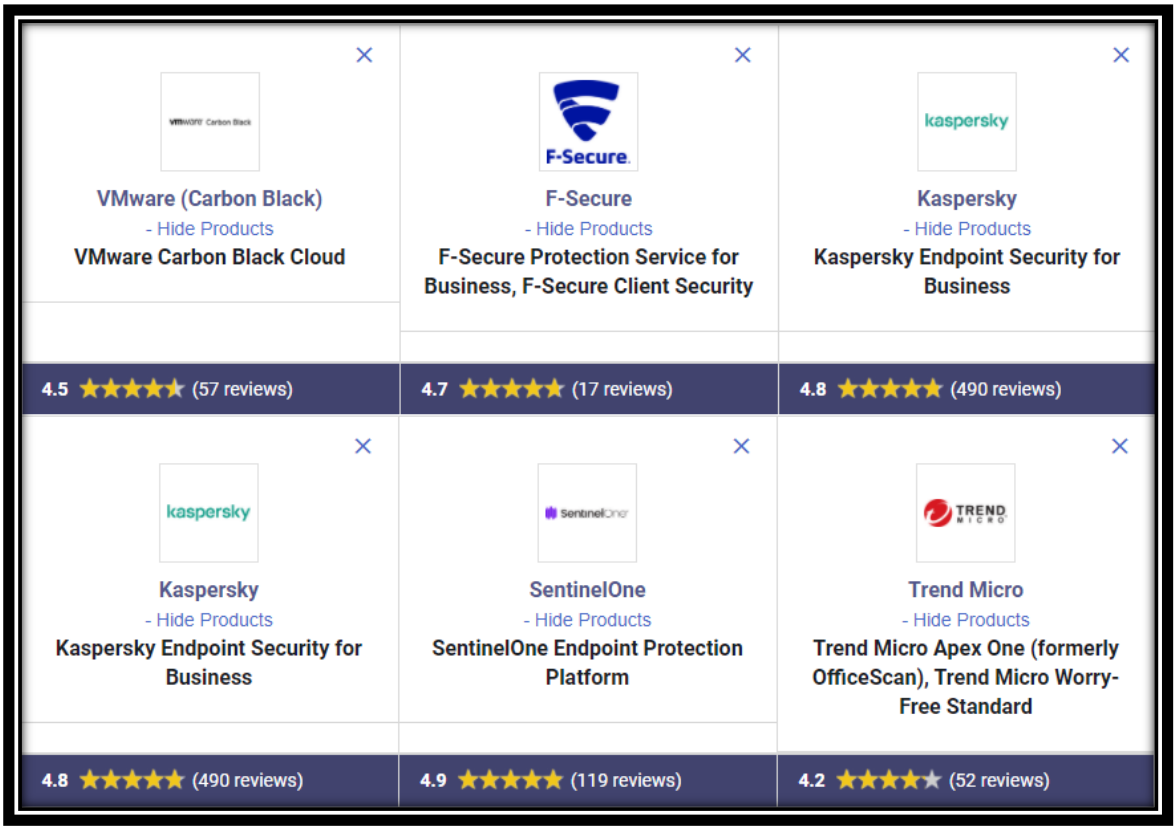


Figura 29: Gartner Overall Peer Rating [46]

4.3.1 Trend Micro Cloud One

La solución Hybrid Cloud Security de Trend Micro, dentro del producto comercial Apex One, utiliza tecnología propietaria XGen™, y hace referencia a una protección de servidores que ejecutan aplicaciones en entornos físicos, virtuales, y cargas de trabajo en la nube o en contenedores. Esta solución se presenta, por tanto, como una protección de sistemas, aplicaciones y datos, especialmente en las VMs, evitando interrupciones por análisis de patrones y facilitando el cumplimiento normativo, es decir, no solo protección a nivel técnico sino, también, dentro del marco legal. Los niveles de seguridad avanzados para una nube híbrida se ofrecen a través de Trend Micro™ Deep Security™.

Deep Security, que se incorpora como un servicio de Cloud One, engloba y proporciona varias técnicas desde una consola central, lo que facilita y agiliza la implementación de la gestión de la seguridad, simplificando la gestión de entornos físicos, virtuales, así como la transición la nube. En las últimas versiones también incluye compatibilidad con arquitecturas de microservicios y protección de contenedores de anclajes, salvaguardando de manera sistemática la evolución del centro de datos. Incluye, como se ha indicado, gestión centralizada, y aprovechando la integración con diferentes plataformas; VMware, AWS y Microsoft Azure, detección automatizada de servidores y protección frente a diversas vulnerabilidades.

Considera, como se ha visto durante el desarrollo del trabajo, que el *malware* puede acceder al entorno desde varios niveles de la infraestructura de virtualización. De ahí que tiene en cuenta la operativa de aplicaciones que se ejecutan en los sistemas operativos invitados, aplicaciones en los sistemas operativos *host* y los propios hipervisores. Por lo tanto, se implementan varios niveles de seguridad en la capa virtual para proteger todo el sistema. Por ejemplo, su solución consiste en un monitor, en forma de *virtual appliance*, en el nivel del hipervisor, que resuelve los problemas de monitorización y ataques al hipervisor desde el sistema operativo *host* en caso de entornos con hipervisor de tipo dos, y desde el propio hipervisor si se trata de entornos tipo uno. Esta solución también consta de módulos de detección de intrusiones en cada una de las VM. Esto resolverá el problema de la vulnerabilidad debido a la concentración ya que cada VM tiene sus propios mecanismos de autodefensa desde el hipervisor.

Dejando de lado la parte más comercial, se podría definir este producto como una plataforma automatizada de respuesta y detección de amenazas para dispositivos terminales o *endpoints*. Su objetivo es proteger a las empresas, especialmente en los entornos que se han ido viendo, de la creciente variedad de amenazas y tipos de *malware*; como los *ransomware*. Esta solución ofrece múltiples opciones de implementación y soluciones híbridas, lo que la posiciona como una buena opción para grandes organizaciones con una estrategia mixta, basada en una arquitectura compuesta por soluciones locales y basadas en la nube.

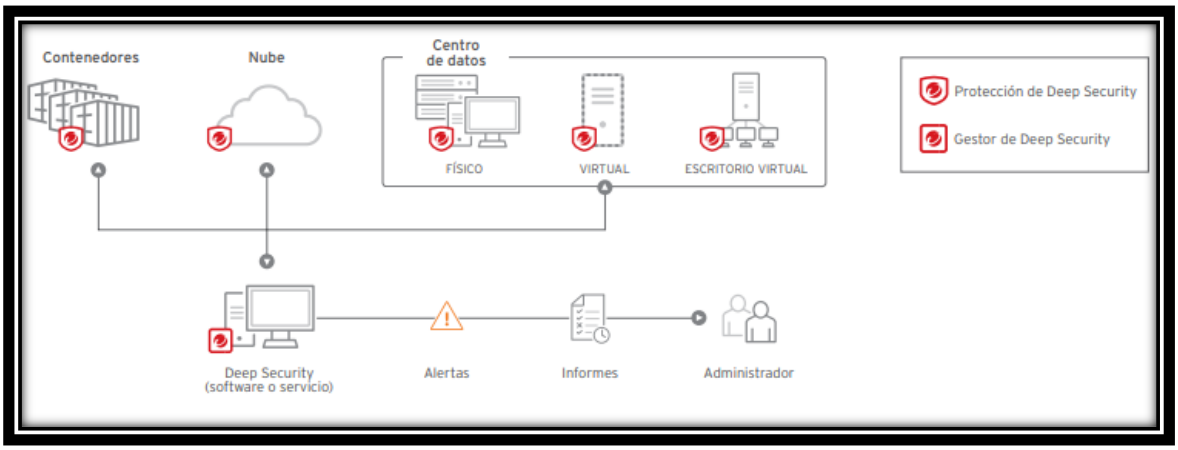


Figura 30: Deep Security overview. Trend Micro Inc.

La infraestructura de la solución, a alto nivel, se muestra en la Figura 30. En ella se puede ver el enfoque con el que Deep Security aborda la seguridad, por ejemplo, de la virtualización. Esta securización se considera mejor que en otros productos debido a la integración que tiene Deep Security a nivel de hipervisor.

Esta integración facilita que se implemente automáticamente sin periodos de inactividad, eliminando la necesidad de instalar y gestionar un agente separado en cada VM. Esto también implica que los servidores y VM individuales no presenten un exceso de bibliotecas de firmas y motores de detección, lo que propicia mejoras en la gestión y uso de la red, velocidad de análisis, y consumo de otros recursos del *host* como memoria, CPU e IOPS. Es decir, unas de las amenazas vistas en entornos virtuales, como tormentas o duplicaciones, se eliminan con esta solución que se integra con VMware NSX, y anteriormente con vShield.

Este enfoque centralizado permite el uso de una caché de exploración de *malware* eficiente, ya que elimina la duplicación en la exploración a través de VM similares, lo que mejora el rendimiento de forma notable, por otro lado, los números que presenta Trend Micro son de una mejora en las exploraciones completas de hasta veinte veces más rápido, análisis en tiempo real hasta cinco veces más rápido, e incluso se garantiza que los inicios de sesión para VDI sean más ágiles.

Hasta aquí, la solución descrita de seguridad sería una solución *agentless* ideal, pero los escenarios reales son heterogéneos y, por normal general, difieren de ser ideales. La solución, como se refleja nuevamente en la Figura 30, contempla este tipo de escenarios de centros de datos físicos, virtuales, y con diversos servicios soportados por diferentes sistemas, es decir, se podría dar el caso de una mezcla de sistemas físicos y virtuales como HP-UX, Windows 2003 Server, Red Hat Linux Enterprise 6.X, Red Hat Linux Enterprise 7.X, Windows 2019 Server, etc. En este caso, como se puede ver en la Figura 31, se podría disponer de una solución combinada; con agente y sin agente, y dependiendo de la versión de Cloud One y el sistema, se tendrían unas funcionalidades u otras, como se puede ver en la web del producto Cloud One.[22]

Se han indicado ejemplos de sistemas como Windows 2003 o Windows 7 por encontrarse fuera de soporte, ya que esta solución tiene un servicio conocido anteriormente como Virtual Patching, y ahora dentro de Workload Security, que crea reglas de prevención de intrusiones que parchean los sistemas a nivel virtual en base a las CVE. Puede utilizar la API para determinar qué regla de prevención de intrusiones protege contra un CVE específico y aplicar la regla si es necesario. Esta funcionalidad es especialmente útil en sistemas que se han dejado de evolucionar o que por necesidades del servicio no se pueden

[22] Trend Micro Cloud One https://cloudone.trendmicro.com/docs/workload-security/supported-features-by-platform/

actualizar, normalmente debido a una aplicación de terceros que no está certificada con un nivel de parcheado diferente.

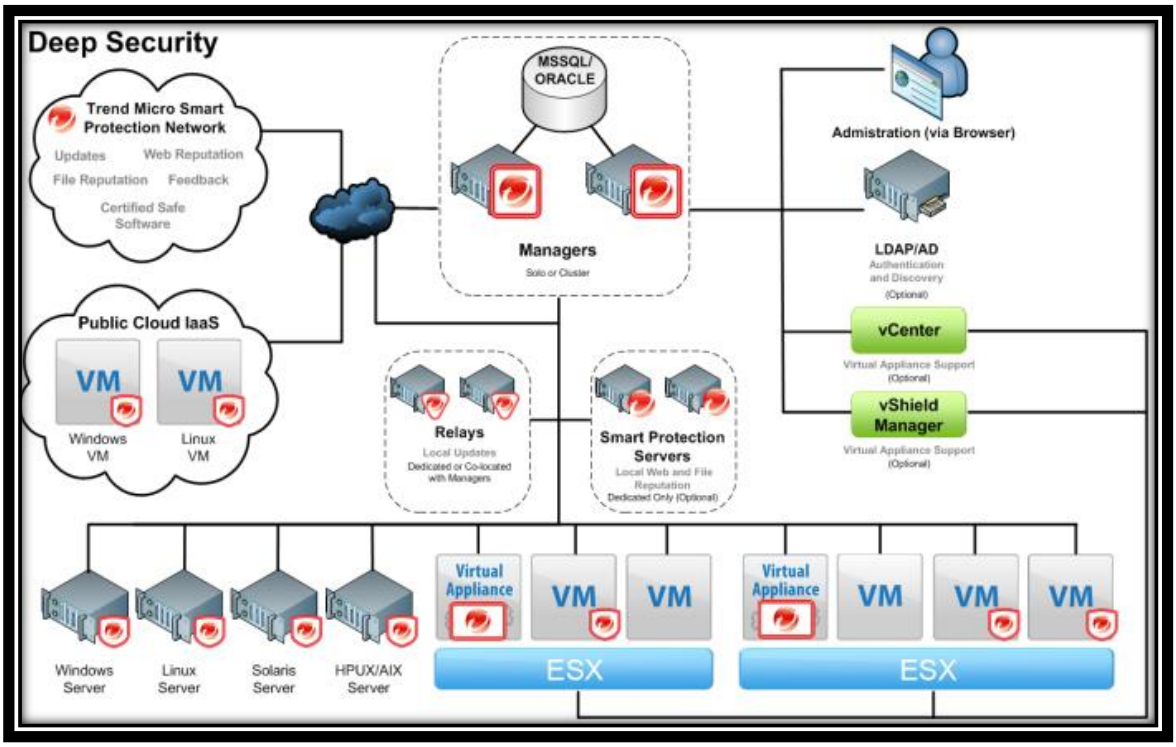


Figura 31: Deep Security componentes en el centro de datos. Trend Micro Inc.

Respecto a la operación o administración, se utiliza una única consola de para revisar todos los informes de amenazas de los *endpoints*, y controlar las políticas de respuesta y los controles de dispositivos. Además,

Un punto importante es el aspecto legal, el producto está alineado para el cumplimiento con normativas destacadas como PCI DSS, HIPAA, NIST, SSAE-16 y GDPR, abarcando desde el centro de datos a la nube. Cloud One ayuda con:

- Informes detallados y auditables que documentan las vulnerabilidades evitadas, los ataques detectados y el estado de cumplimiento de las políticas.
- Automatización, lo que incide en un consumo menor de tiempo y esfuerzo en auditorías mediante controles centralizados de seguridad y generación consolidada de informes.
- Respaldo para iniciativas internas de cumplimiento a fin de aumentar la visibilidad de la actividad de red interna.
- Tecnología certificada según Common Criteria EAL2.

En resumen:

- Seguridad basada en aprendizaje automático con análisis de comportamiento para garantizar que los puntos finales estén protegidos contra amenazas avanzadas.
- Funciones de detección y respuesta automatizadas que detienen y detectan amenazas al tiempo que ayudan a reducir la carga de los departamentos de TI.
- Seguridad avanzada contra ransomware que protege contra archivos sospechosos, actividades maliciosas y puede recuperar archivos perdidos si es necesario.
- Implementación flexible con soluciones híbridas, locales y en la nube
- Dispone en las últimas versiones de protección para dispositivos móviles, mediante un agente específico.
- Disponible tanto en la web de TrendMicro como en AWSmarketplace y MS Azure.

Las diferentes funcionalidades de la solución y, en concreto, del agente, se pueden consultar en la web de Cloud One[23] directamente.

4.3.2 Kaspersky Endpoint Security for Business

Kaspersky Endpoint Security es un producto que ofrece a las pequeñas y medianas empresas una protección contra amenazas conocidas y desconocidas, entre ellas, *malware* tipo *ransomware*. Este producto, al igual que Cloud One, incorpora diferentes componentes como los virtual appliance que se integran en los *hosts* e interactúan con el hipervisor y NSX. En este caso son los SVA, mientras que en Cloud One son los DSVA.

[23] https://cloudone.trendmicro.com/docs/workload-security/supported-features-by-platform/

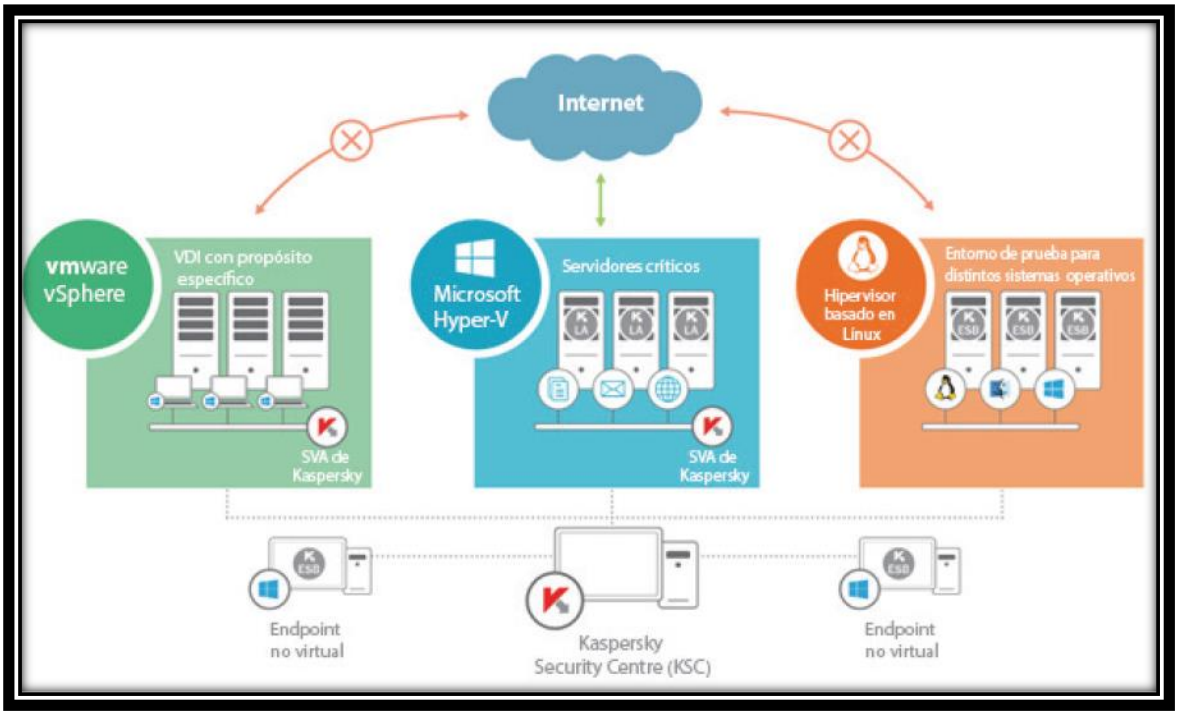


Figura 32: Kaspersky Endpoint Security for Business. Kaspersky Inc.

Kaspersky Endpoint Security for Business (KESB), está diseñado para entornos de TI mixtos, al igual que el producto anterior de Trend Micro, e incorpora una consola web junto con un paquete integrado de tecnologías certificadas, por ejemplo, por el instituto AV-Test GmbH. Esta consola se conoce como KSC, tal y como se puede observar en la Figura 32, sobre la arquitectura del producto. Por otro lado, también se puede observar que es multiplataforma, es decir, soporta tanto ESXi de VMware como Hyper- de MS, no obstante, al contrario que Cloud One, es necesaria la solución “Kaspersky Hybrid Cloud Security for AWS”, para integrar con la nube de Amazon.

Como se puede ver en la Figura 33 incorpora una serie de características, según se utilice la solución sin agente, agente ligero o integral. Estas características, como la comentada anteriormente de multiplataforma, se pueden cruzar con los casos de uso que propone Kaspersky, a modo de ejemplo, o las necesidades específicas de cada empresa u organización.

Por ejemplo, en servidores de bases de datos o back-end, que no tengan acceso externo, y la única condición externa sea alguna conexión puntual de un administrador y los agentes de copias de seguridad periódicas, Kaspersky recomienda utilizar la solución *agentless,* mientras que en la infraestructura de procesamiento de datos de clientes o los servidores de *front-end* recomiendan solución de agente ligero o agente de la solución integral. Teniendo en cuenta premisas como el valor de los datos, acceso y condiciones externas, además de la categorización del servicio.

Característica	Kaspersky Security for Virtualization | Agentless	Kaspersky Security for Virtualization | Light Agent	Kaspersky Endpoint Security for Business
Plataformas de virtualización compatibles	VMware	VMware, Microsoft Hyper-V, Citrix	Cualquiera excepto a nivel de sistema operativo[1]
Sistema operativo invitado compatible	MS Windows	MS Windows	MS Windows, Mac OS X, Linux
Indice de consolidación dentro de un único host	* * *	* */* * *2	*
Gestión centralizada mediante Kaspersky Security Center	+	+	+
Funcionalidad de KSN	+	+	+
Protección de máquinas virtuales nuevas sin instalaciones adicionales	+	+/-3	-
Antimalware	* *	* * *	* * *
Firewall	-	+	+
Prevención de intrusiones basada en host (HIPS)	-	+	+
Network Attack Blocker	+	+	+
Control de aplicaciones con marcado dinámico en la lista blanca y compatibilidad con denegaciones predeterminadas	-	+	+
Control web	-	+	+
Control de dispositivos	-	+	+
Gestión de sistemas	-	+4	+4
Cifrado	-	-	+

Figura 33: Kaspersky lista comparativa de funciones. Kaspersky Inc [48]

En el porfolio de servicios Kaspersky Endpoint Security for Business[24], se pueden encontrar todos los servicios que ofrece en base al tipo de empresa y necesidades de cada una, basándose en tres tipos de licencia o extensiones del producto. Mediante el registro de una cuenta, se puede realizar una estimación del coste por número de dispositivo e incluso instalar agentes en los *endpoints* [48] .

En resumen:

[24] https://media.kaspersky.com/en/business-security/kaspersky-security-products-for-small-and-medium-business.pdf

- Al igual que Cloud One la seguridad está basada en aprendizaje automático con análisis de comportamiento.
- Funciones de detección y respuesta automatizadas que detectan y detienen amenazas según el tipo de solución implementada.
- Seguridad avanzada contra *ransomware* en base a modificación de ficheros de datos y de sistema, monitorización de actividades maliciosas, recuperación de archivos según solución y sistema.
- Implementación flexible con soluciones multiplataforma local. Necesario otro producto para soluciones en la nube o híbridas.
- Disponible tanto en la web de KasperskyLab como en AWSmarketplace.

4.3.3 VMware Carbon Black Cloud

Este producto de seguridad, referencia en entornos *cloud*, es adquirido por VMware en 2019[25], es decir, actualmente pertenece a un fabricante de virtualización y no de seguridad, a diferencia de los otros cuatro.

VMware acuerda la compra de Carbon Black con el objetivo de mejorar la seguridad en la nube y mejorar la privacidad de los datos de cliente, a través de Big Data, analítica de conducta e Inteligencia Artificial. Desde un punto de vista técnico, esta compra refleja que se necesitaba un producto para proteger diferentes aspectos como la gestión de las cargas de trabajo en la nube o la mejora de la privacidad, así como el cumplimiento con las normativas de protección de datos. Por lo tanto, es un producto adquirido para complementar sus componentes de seguridad del centro de datos y nube privada, incluidos en NSX, de cara a extender y mejorar esta seguridad en nubes híbridas y públicas.

Tal y como anunció el CEO de Vmware[26], Pat Gelsinger, con este posicionamiento se convertían en la única compañía capaz de entregar soluciones de *software* que permitan a los clientes crear, ejecutar, gestionar, conectar y proteger cualquier aplicación en cualquier *cloud* y en cualquier dispositivo; “es también una oportunidad para cambiar todo el mercado de seguridad”.

No obstante, volviendo al producto, Carbon Black es un referente en el mercado de seguridad de nueva generación. Se considera una plataforma de seguridad nativa de las nubes basadas en VMware, al contrario que los otros productos, detallando la capacidad de análisis de datos y comportamiento para proporcionar una protección integral de *endpoint* incluso contra los ciberataques más avanzados. Tal y como adelantábamos, VMware ofrece la combinación de las

[25] https://www.vmware.com/es/company/carbonblack-announcement.html
[26] https://www.itdigitalsecurity.es/actualidad/2019/08/vmware-compra-carbon-black-y-pivotal

soluciones de Carbon Black con otros productos de seguridad, incluidas AppDefense, Workspace ONE, NSX y SecureState, lo que describe como “una plataforma moderna de nube de seguridad para cualquier aplicación, que se ejecuta en cualquier nube y en cualquier dispositivo”, [49] [50]

VMware Carbon Black Cloud utiliza una consola centralizada y un agente de tipo ligero, además, está compuesto de los siguientes módulos o componentes:

- **Endpoint (NGAV):** Es el antivirus de nueva generación (Next-generation anti-virus). Permite la configuración y manipulación de la protección NGAV, además de analizar el comportamiento EDR en los puntos finales que ejecutan el agente ligero; VMware Carbon Black Cloud Endpoint Sensor. Antes de la compra por VMware se conocía como Carbon Black Defense.
- **Enterprise EDR:** Permite el análisis de datos avanzados, sin filtrar, a través de un elemento de interfaz de usuario específico. No obstante, refleja dicha información, de todos los puntos finales administrados, en la consola centralizada lo que permite administrador tener una vista amplia y poder aplicar acciones de detección y respuesta. Anteriormente conocido como Carbon Black ThreatHunter.
- **Audit & Remediation:** Habilita los elementos de la interfaz de usuario de Live Query y permite la gestión de vulnerabilidades, así como la reparación de servicios con consultas programadas o bajo demanda de todos los dispositivos en el entorno. Por otro lado, posibilita la capacidad de aprovechar un *shell* o consola remota para resolver cualquier problema. Anteriormente conocido como Carbon Black LiveOps.

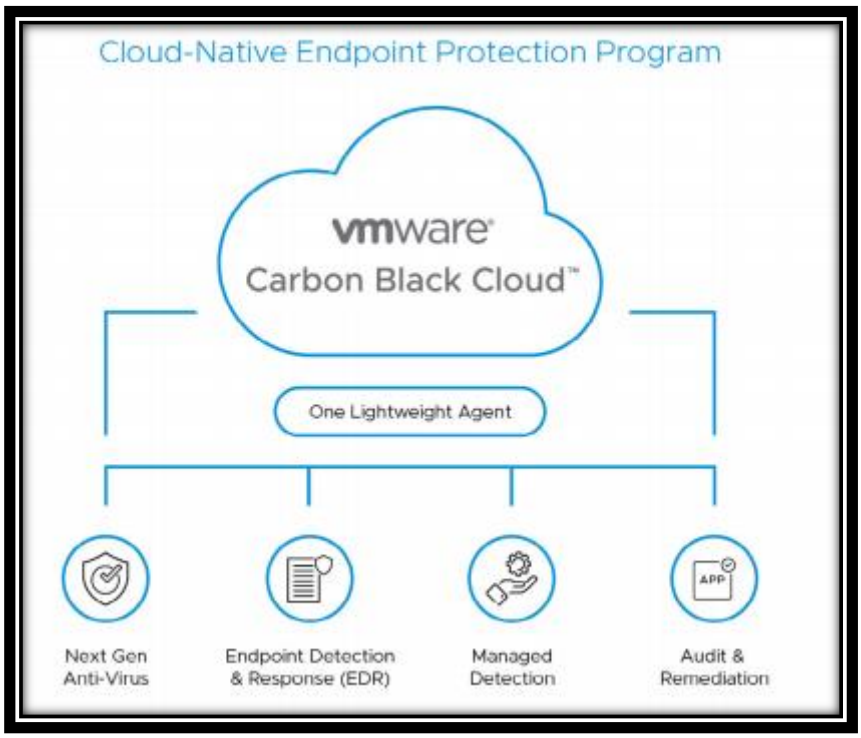


Figura 34: Arquitectura VMware Carbon Black Cloud. VMware Inc.

En resumen:

- Al igual que los anteriores, la seguridad está basada en aprendizaje automático con análisis de comportamiento. VMware indica que analiza billones de eventos para obtener políticas de comportamiento normal de servicios y sistemas.
- Funciones de detección y respuesta automatizadas que detectan y detienen amenazas según el tipo de solución implementada, monitorizando comportamientos como escalado de privilegios no autorizado o uso de herramientas legítimas.
- Integración en consola única con el fin de que los departamentos de TI de seguridad y de infraestructura virtual dispongan de la misma fuente de información.
- Implementación nativa en soluciones de nube de VMware, no obstante, necesarios otros productos para securización de centro de datos, por ejemplo, NSX.
- Gestión y monitorización remota o externa de la nube, se necesita comunicación TCP 80 y 443 con diferentes servidores que VMware detalla según zona geográfica.
- Disponible en la web de VMware.

4.3.4 Sentinel One EPP

Esta herramienta integra las soluciones tradicionales de antivirus con agente *endpoint,* y les suma las funciones de un EDR; detección y respuesta automatizada, monitorización continua; análisis forense en tiempo real, además de incluir aspectos como la integridad de ficheros. Como el resto de los productos, aplica el *machine learning* y la automatización permitiendo clasificar cada aplicación de la organización de forma precisa haciendo que se ejecute únicamente lo que es lícito. Es decir, cambia totalmente el concepto de la solución clásica: elabora una base de datos de acciones y aplicaciones del usuario que son consideradas como buenas y, todo lo que se salga de ahí, entra en análisis.

Distribuye su actividad en cuatro pilares; protección, visibilidad, simplicidad y automatización. Por ejemplo, el sistema de protección multicapa es capaz de detectar las amenazas en un entorno real independientemente de su procedencia o del estado, es decir, incluso de un USB. Incluye asimismo un agente ligero proporciona la funcionalidad de EPP, EDR, HIPS, supervisión de la integridad de los archivos, etc. Por otro lado, la consola central puede estar

ubicada en la propia infraestructura local, en la nube o en ambas, bajo un modelo híbrido [51] .

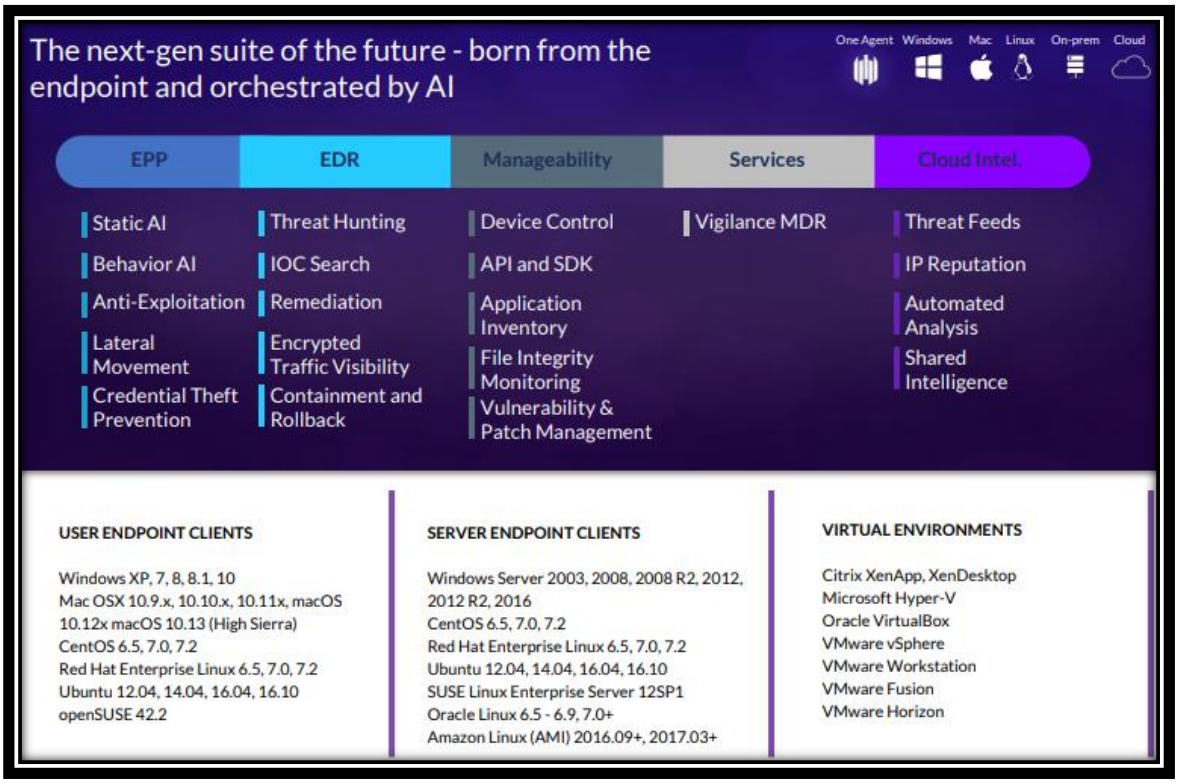


Figura 35: Componentes y soporte Sentinel One EPP

En resumen:

- Al igual que los anteriores, la seguridad EPP y EDR está en aprendizaje automático, aplicando inteligencia artificial para analizar comportamiento.
- Incorpora funciones para detección del movimiento lateral de *ransomware.*
- Integración en consola única; en la nube, centro de datos local o nube hibrida.
- Posibilidad de XDR y servicio SentinelOne MDR 24/7/265. Este aspecto es valorado por diferentes empresas u organismos. Disponer de un departamento externo o SOC (Security Operation Center)
- Foco en a la visibilidad. Especialmente de cualquier dispositivo que se conecte a la red o la nube sin autorización. El descubrimiento de dispositivos maliciosos se realiza vía Ranger® IoT, el cual proporciona visibilidad de todos los dispositivos de red administrados y no administrados y control sobre ellos.
- Análisis de los flujos o cargas de trabajo entre la nube pública y privada.
- Producto mejor valorado por Gartner.

4.3.5 F-Secure PSB Computer Protection

Este producto, otro de los mejores valorados por Gartner, es considerado también una suite de protección empresarial completa, diseñada para una integración fácil en la nube y una operación ágil desde cualquier navegador. Al igual que las otras soluciones, dispone de una consola central o portal de gestión unificada. El resto de las componentes, además del portal, son denominados de protección:

- **Computer** Protection: Cliente dedicado para estaciones de trabajo, principalmente Windows y MacOS.
- **Mobile** Protection: Protección específica de terminales móviles bajo el nombre de F-Secure Freedome (iOS y Android).
- **Server** Protection: Protección multiplataforma, a nivel de servidor y servicio (Windows y SharePoint, Exchange, etc., Linux, Citrix, etc.)

Permite la instalación de los clientes desde el portal mediante un flujo de correo, instalación local, vía *scripting* o fichero por lotes. También vía aplicaciones de gestión empresarial como SolarWinds, Kaseya, Datto o con un paquete MSI, opción recomendada para grandes entornos. Del mismo modo, los clientes de Mac se implementan como paquetes utilizando Instalador de macOS o herramientas de administración de dispositivos móviles, y se puede configurar con pasos de implementación adicionales en paquetes firmados y personalizados. La opción de correo incluye la clave de suscripción para que el usuario final solo tenga que ejecutar el enlace para que el proceso de instalación se inicie automáticamente.

Por otro lado, cada módulo incluye una serie de características que se focalizan en determinados aspectos de la solución, partiendo de la premisa de que la solución está diseñada para entregarse como un servicio basado en la nube; ya sea como un servicio autogestionado o por un proveedor de servicios certificado. Su agente, hace honor a su nombre (F-Secure Ultralight, ya que es considerado uno de los más ligeros. Además, se incluye XFENCE en el componente de F-Secure Computer Protection, específico para macOS.

A nivel comercial se diferencian tres tipos de licenciamiento: Standard, Premium y Advanced. El servicio de protección para las estaciones de trabajo basadas en MacOS y Windows están disponible dentro del nivel estándar, incluyendo *anti-malware* y gestión del nivel de parcheado en entornos Windows. Las funciones Premium y Advanced agregan una protección superior respecto a control de aplicaciones y *ransomwares,* añadiendo funcionalidades adicionales, si entrar en detalle técnico. No obstante, estas licencias proporcionan servicios profesionales

con F-Secure como soporte en horario laboral (Premium) o continuo a cualquier hora (Advanced), con diferentes SLAs [52] .

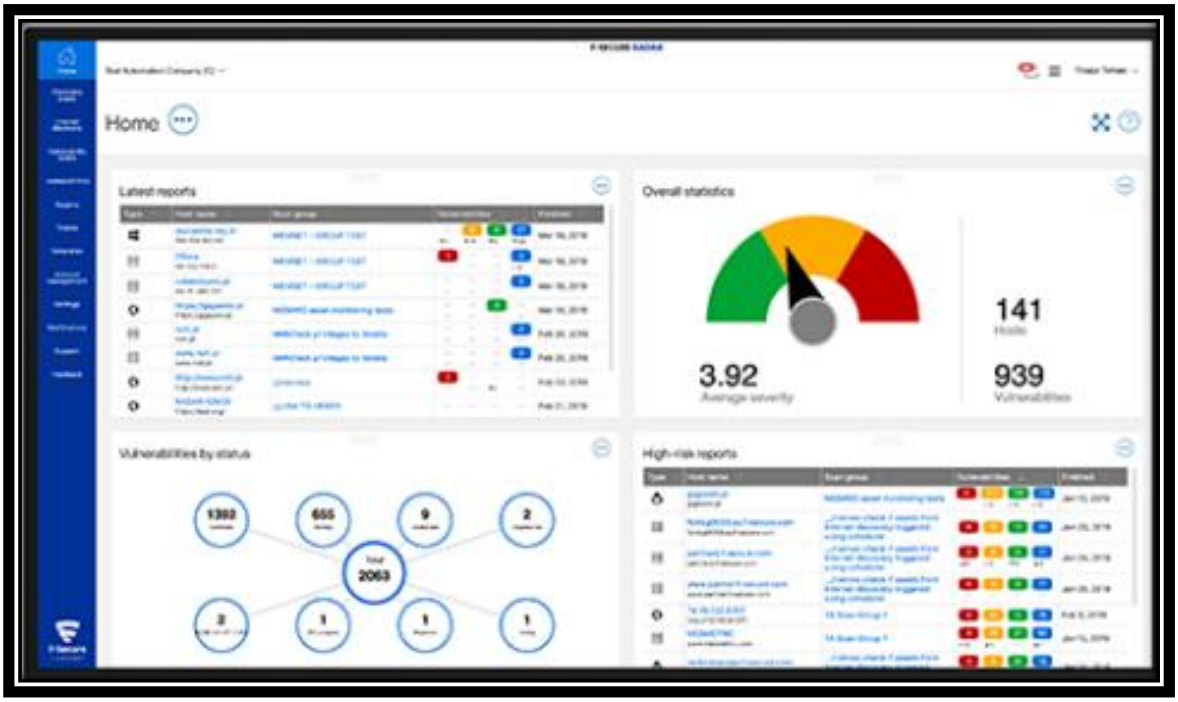


Figura 36: Consola centralizada o portal de gestión F-Secure PSB. F-Secure

En resumen:

- Al igual que los anteriores, la seguridad EPP/EDR mediante agente se basa en inteligencia artificial.
- Integración en consola única; en la nube. Utiliza la nube de Amazon (AWS) y no su nube privada.
- Foco en entornos en la nube. Control de dispositivos móviles con un componente, y agente específico, para terminales basados en Android e iOS.
- Análisis de los flujos o cargas de trabajo entre la nube.
- Control de actividad en uso de periféricos como llaveros USB, CD-ROM, micros o cámaras web.
- Producto mejor valorado por AV-Test. Ha recibido el premio a la mejor protección varios años consecutivos.

4.3.6 Adaptabilidad frente a nuevas amenazas

Llegados a este punto, y tras analizar las diferentes soluciones del mercado, se observa una notable mejoría en estas soluciones, categorizadas como *software* de seguridad de nueva generación, no obstante, se sigue considerando que no hay una solución única que pueda proteger, completamente, los entornos complejos actuales contra el amplio espectro de amenazas que existen.

Se ha visto que, gracias a la inteligencia artificial y al *machine learning*, estas soluciones de seguridad se entrenan y amplían su rango de detección, intentando adaptarse a los movimientos laterales del *malware.*

El concepto de movimiento lateral, dentro del contexto de incidentes de seguridad o ciclo de vida de un ciberataque, es un aspecto de gran importancia en la actualidad. Este tipo de ataque se debe a que, por norma general hoy en día, los *ransomware* es operado por personas, prácticamente de forma manual, es decir, se suelen tratar de ataques dirigidos a organizaciones específicas, en las cuales se intenta acceder mediante otro tipo de *malware,* campañas de *spear phishing*, y cuyo objetivo inicial no es el de extraer la mayor cantidad de información sensible, sino establecer un punto de entrada a la red. Cuando se compromete alguno de los equipos del entorno, sigue el ataque, comenzando el movimiento lateral. Puede ejecutarse un solo paso lateral o cientos de ellos para llegar al objetivo perseguido, ya sea la información crítica sensible o controlar un sistema foco, y para esto se suelen obtener credenciales de personas clave para moverse en la red corporativa.

En resumen, el movimiento lateral es un aspecto básico o una las etapas que se utilizan en un ataque dirigido, que típicamente son; la recolección de información y escaneo, acceso y escalamiento de privilegios, exfiltración, sostenimiento, asalto y ofuscación. Como se ha visto, los productos evaluados controlan aspectos como el comportamiento de usuarios legítimos, en busca de actividades fuera de los patrones regulares, pero quizás no todos los usuarios estén bajo monitorización o haya tenido información suficiente para conocer su comportamiento. Por otro lado, algunas de estas soluciones también realizan la gestión de parcheado de los componentes, pero un sistema de seguridad sigue siendo un sistema de terceros, que también necesita estar protegido, ya que sería un punto crítico muy interesante para un ataque. Además, el acceso desde cualquier tipo de dispositivo, tanto a la red de la organización como a la nube, requiere de medidas múltiple factor de autenticación o, al menos, doble factor de autenticación, ya que aplicar seguridad a la capa de acceso es esencial.

Por estos motivos, la seguridad debe implementarse en varias capas, y debe utilizarse más de una solución de seguridad si es necesario, evitando estos posibles movimientos laterales. Es decir, sí un componente de seguridad no puede identificar cierto tipo de amenazas o proteger la red, hay otros componentes, que pueden hacerlo. Por eso es importante, como se ha indicado anteriormente, elegir un producto adecuado en base a los servicios que la empresa proporciona y, además, implementar todas las medidas o recomendaciones de seguridad que estén disponibles, por ejemplo, aplicando medidas de seguridad a la capa virtualización o desplegar un entorno *sandbox;*

aislado, lo más seguro posible, para entornos de pruebas y desarrollo. No se debe dejar de lado que determinados servicios o aplicaciones se desarrollan continuamente, y pueden tener vulnerabilidades en el código. Estos servicios corporativos se integran contra el directorio activo y, por tanto, existe información como dominios, relaciones de confianza, etc. que pueden quedar al descubierto si no se protegen adecuadamente [53] .

4.4 Entornos virtuales seguros. Securización del hipervisor y *Sandbox*

Como se ha ido demostrando, la migración de recursos informáticos a un entorno virtualizado tiene poco efecto en la mayor parte de las vulnerabilidades y amenazas de los recursos. Por ejemplo, si un servicio tiene vulnerabilidades inherentes y se traslada de un servidor no virtualizado a un servidor virtualizado, el servicio sigue siendo igual de vulnerable a la explotación. Sin embargo, el uso de la virtualización puede ayudar a reducir el impacto, pero, por el contrario, la virtualización también puede proporcionar vectores de ataque adicionales, como las amenazas que se han visto del hipervisor, aumentando así la probabilidad de éxito. A continuación, se describen unas pautas para aplicar seguridad adicional en hipervisores de tipo uno y de tipo dos.

4.4.1 Securización del hipervisor

La seguridad de una solución de virtualización completa depende en gran medida de la seguridad individual de cada uno de sus componentes, incluido el hipervisor. Las organizaciones deben proteger todos estos elementos y mantener su seguridad, principios básicos como restringir el acceso a interfaces de administración, gestionar el ciclo de vida del *software y* aplicar las guías o recomendaciones de configuración de cada fabricante. Por último, tener presente que quizás estas recomendaciones no sean suficientes para asegurar un entorno de virtualización o hipervisor, por eso, se deberá monitorizar y controlar los registros y su comportamiento.

Las aplicaciones que gestionan el hipervisor deben protegerse mediante métodos similares a los utilizados para proteger otro *software* que se ejecuta en equipos de escritorio y servidores. La seguridad de toda la infraestructura virtual suele basarse en la seguridad del sistema de gestión de virtualización que controla los hipervisores, no obstante, este componente está más maduro respecto a la seguridad; incorpora más medidas que los hipervisores, como es el nivel de acceso por rol y dominio, y es monitorizado de manera más exhaustiva por las soluciones anteriormente indicadas.

Generalmente, los hipervisores solo utilizan contraseñas para acceso con privilegios y, en muchos entornos, suelen dejarse por defecto. Este aspecto, y otras recomendaciones, dan lugar a la guía que se presenta en el Anexo II "*hardening* de un hipervisor ESXi versión 6.7 U3" [54] , [55] [56]

Algunos puntos, del total que se detallan en la guía, se resumen a continuación:

Sección	Nombre	Descripción
Software	Parcheado ESXi	Un atacante capacitado puede aprovechar las vulnerabilidades conocidas al intentar obtener acceso o elevar los privilegios en un host ESXi. Se debe mantener actualizado el hipervisor.
Instalación	Perfil VIB	Un VIB (vSphere Installation Bundle) es una colección de archivos que se empaquetan en un archivo e incorporan un archivo de firma que comprueba el nivel de confianza. Se recomiendan los niveles del 1 al 3.
Logs	Persistencia de *logging*	El registro no persistente presenta un riesgo de seguridad porque la actividad del usuario registrada en el host solo se almacena temporalmente y no se conservará durante los reinicios.
Password	Configuración complejidad *passwords*	Se recomienda aplicar política de longitud mínima de caracteres, caracteres particulares y restringir el número de intentos de inicio de sesión fallidos consecutivos.
Password	Configuración sesión	Configurar el número máximo de intentos de inicio de sesión fallidos consecutivos para cada cuenta.
Password	Configuración baneo	Bloquear automáticamente después de que se alcanza el número máximo de intentos de inicio de sesión consecutivos fallidos.
Accesos	Deshabilitar Shell, SSH, etc.	Las actividades realizadas desde el shell ESXi omiten vCenter RBAC y los controles de auditoría, por lo que el shell ESXi solo debe habilitarse cuando sea necesario, al igual que el SSH.
Comunicación	NTP, SNMP, MOB, etc.	Hay que asegurar que todos los sistemas utilizan el mismo origen de tiempo relativo, deshabilitar SNMP si no se está utilizando, etc.
Red	Deshabilitar modo promiscuo en vSwitch	Deshabilitar el modo promiscuo en los switches virtuales.
Red	Activar filtro BPDU	BPDU Guard y Portfast se habilitan comúnmente en el *switch* físico. Si se envía un paquete BPDU desde una máquina virtual en el host ESXi puede ocurrir un bloqueo en cascada de todas las interfaces de enlace ascendente desde el host ESXi.

Figura 37: Resumen puntos guía de hardening ESXi

4.4.1 Despliegue de una *sandbox*

La *sandbox o* caja de arena originalmente se refería a la pequeña caja llena de arena donde los niños juegan y experimentan en un ambiente controlado. Pero poco a poco, el término ha ido adquiriendo nuevos significados en diversos sectores. En el mundo de la informática, una caja de arena es un entorno de prueba cerrado, utilizado como un mecanismo de seguridad para separar ciertos programas en ejecución, de entornos productivos. Con el fin de mitigar fallos del sistema y vulnerabilidades del *software* para que no se propaguen. A menudo se utiliza para ejecutar aplicaciones o código que no han sido testeados o que no son confiables. Suele darse en código nuevo proveedores o proveniente de terceros o sitios web no verificados o no confiables.

Una caja de arena, por norma general, proporciona un conjunto de recursos estrictamente controlado para que se ejecuten los programas invitados, como el almacenamiento y el espacio temporal de la memoria. El acceso a la red, la capacidad de inspeccionar el sistema *host* o leer desde dispositivos de entrada generalmente están prohibidos o restringidos, sin riesgo de dañar la máquina *host* o el sistema operativo.

Estas también se utilizan con frecuencia para analizar aplicaciones que puedan contener virus u otro código malicioso, con el fin de estudiar el comportamiento sin permitir que este código dañe el dispositivo host.

Prácticamente todos los fabricantes de seguridad disponen de este tipo de solución, por ejemplo, ESET incorpora un servicio de *sandbox* en la nube denominado ESET Dynamic Threat Defense.

Existen muchos tipos de *sandbox*, por ejemplo; Sandboxie[27] o Shade[28], incluso dispositivos o aplicaciones en ese modo de ejecución, ya que se trata de una de las formas más efectivas de asegurar que un sistema comprometido sufra la menor cantidad de daños posible. Esto se realiza aislando el espacio de ejecución de código malicioso dentro de su propia zona, y posibilitando su descarte completo una vez finalizada su ejecución. A continuación, de cara a no extender más el apartado, se resumen algunos pasos para desplegar una *sandbox*, los cuales se detallan en los siguientes artículos “Sandbox Deployment

[27] https://www.sandboxie.com/
[28] https://www.shadesandbox.com/

and Install Guide"[29], "Como crear un entorno seguro *sandbox* con VirtualBox"[30] y "Deploying Hortonworks Sandbox on VirtualBox"[31]:

- Desplegar la máquina virtual o sistema operativo.
- Aislar dicha máquina virtual de la red. Los hipervisores permiten crear redes locales específicas o desactivar los interfaces de red virtuales. Sí se quiere investigar un movimiento lateral o infección por red tendría sentido no deshabilitar el interfaz, pero sí crear una red dedicada y aislada.
- Aislar dicha máquina de periféricos. Se podría deshabilitar los controladores de USB, puertos serie, etc.
- Cerciorarse de la configuración de NAS, NFS u otro tipo de almacenamiento en red, como la posibilidad de "carpetas compartidas" de Virtual Box.
- Desplegar herramientas de investigación, analizadores de tráfico, *debbugers, honeypots* en la red aislada, etc.

[29] https://www.cloudera.com/tutorials/sandbox-deployment-and-install-guide/.html
[30] https://www.geeknetic.es/Guia/1758/Como-crear-un-Entorno-Seguro-Sandbox-con-VirtualBox.html
[31] https://www.cloudera.com/tutorials/sandbox-deployment-and-install-guide/1.html

5. Caso práctico. Implantación, despliegue y securización.

5.1 Instalación del hipervisor

En este apartado se realiza la instalación de un hipervisor, concretamente el hipervisor ESXi de VMware versión 6.7 U3. En primer lugar, se puede descargar y seguir los pasos desde el siguiente KB[32] de VMware, teniendo en cuenta que existe la versión gratuita limitada y diferentes versiones de pago según licencia.

Para licenciar el hipervisor de uso gratuito ESXi 6.7 y 7.x se debe:

- Inicie sesión en “My VMware”.
- Seleccionar “Productos” y, posteriormente, “Mi historial de descargas”.
- Seleccionar “+” o “>” debajo de “VMware vSphere Hypervisor” para abrir los detalles del producto.
- Ir a “descargas y licencias”. Alternativamente, se puede acceder a la clave de licencia siguiendo este enlace VMware vSphere Hypervisor 6.7[33].

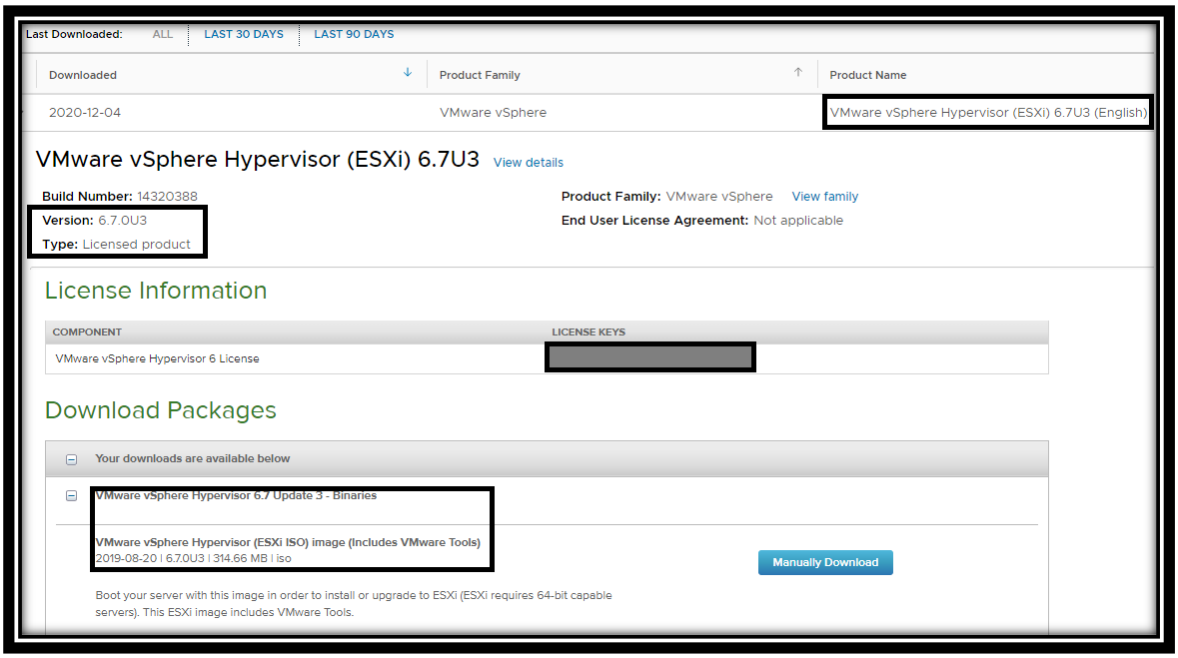


Figura 38: Obtención de licencia y registro ESXi

Los pasos de una instalación se pueden encontrar detallados en la siguiente guía[34] de VMware.

[32] https://kb.vmware.com/s/article/2107518?lang=en_US
[33] https://my.vmware.com/en/group/vmware/evalcenter?p=free-esxi6
[34] https://docs.vmware.com/es/VMware-vSphere/6.7/vsphere-esxi-67-installation-setup-guide.pdf

5.2 Configuración

Durante la instalación, el ESXi requiere el idioma del teclado y la contraseña de root, por lo tanto, el resto de la configuración se realiza una vez se haya instalado.

Desde la pantalla de inicio del hipervisor, la cual se puede visualizar en la Figura 40, se presiona “F2” y se accede al menú del ESXi como si fuese una BIOS de cualquier otro sistema. Desde este menú se pueden realizar configuraciones de red, por ejemplo; configuración específica IPv6. Añadir nuevas *vmnic* y activarlas para *teaming,* habilitar el ESXI Shell y el acceso por SSH, etc. Desde este modo del ESXi no se crean maquines virtuales ni se accede a la configuración de estas, de ahí que se haya insistido en su correcta configuración, ya que no se le da la importancia que requiere y suele dejarse de lado, normalmente utilizándose únicamente para la instalación y configuración inicial de red. También es utilizado para diagnóstico a través de la Shell.

En este apartado se incluye la configuración de la licencia obtenida en el apartado anterior:

- Ir a “Administrar”→ Licencias y seleccionar “Asignar licencia”.
- Añadir licencia en “Clave de licencia” → “Comprobar licencia”
- Finalmente, “Asignar licencia”, la fecha de caducidad debe modificarse de los 60 días a “Nunca”.

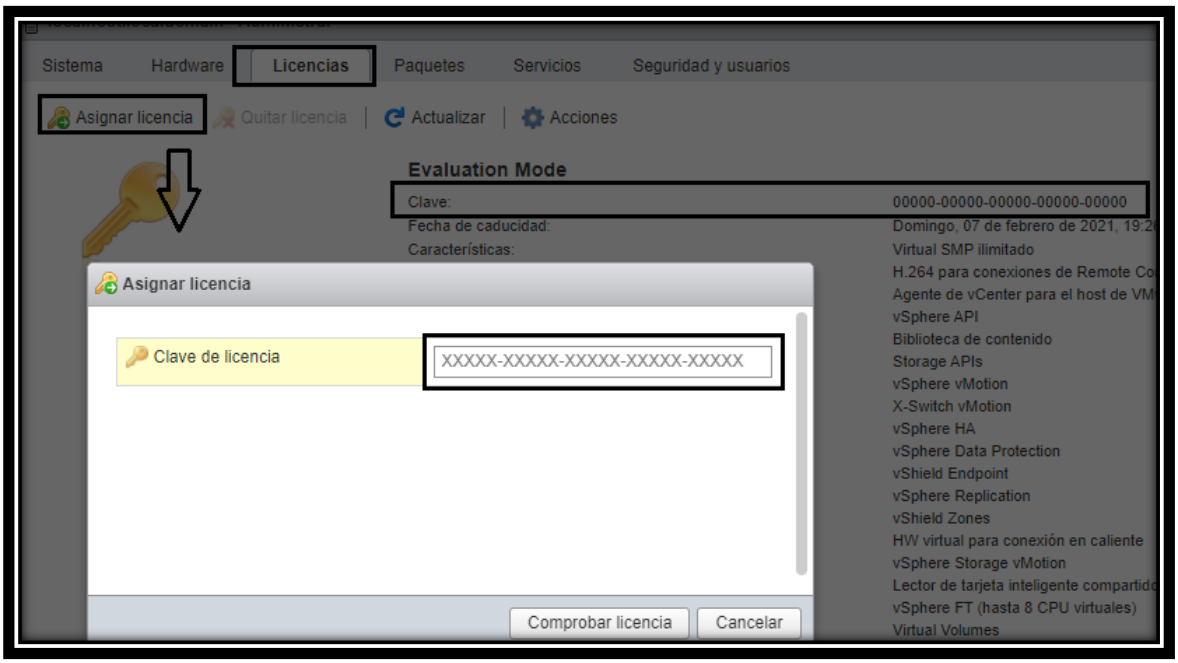


Figura 39: Configuración de licencia ESXi

Por un lado, se puede observar en la Figura 39 el acceso mediante cliente web, y en la Figura 40, la pantalla de inicio del hipervisor.

En la pantalla de inicio se indican la versión del ESXi, el parcheado exacto a nivel de *build*, y el procesador físico del servidor que lo soporta. Además, se muestran las IPs para acceder al mismo, tanto IPv4 como IPv6. En caso de que no exista un servidor DHCP válido en la red, la IP será la típica que se da cuando no se encuentra una válida: 169.254.X.X

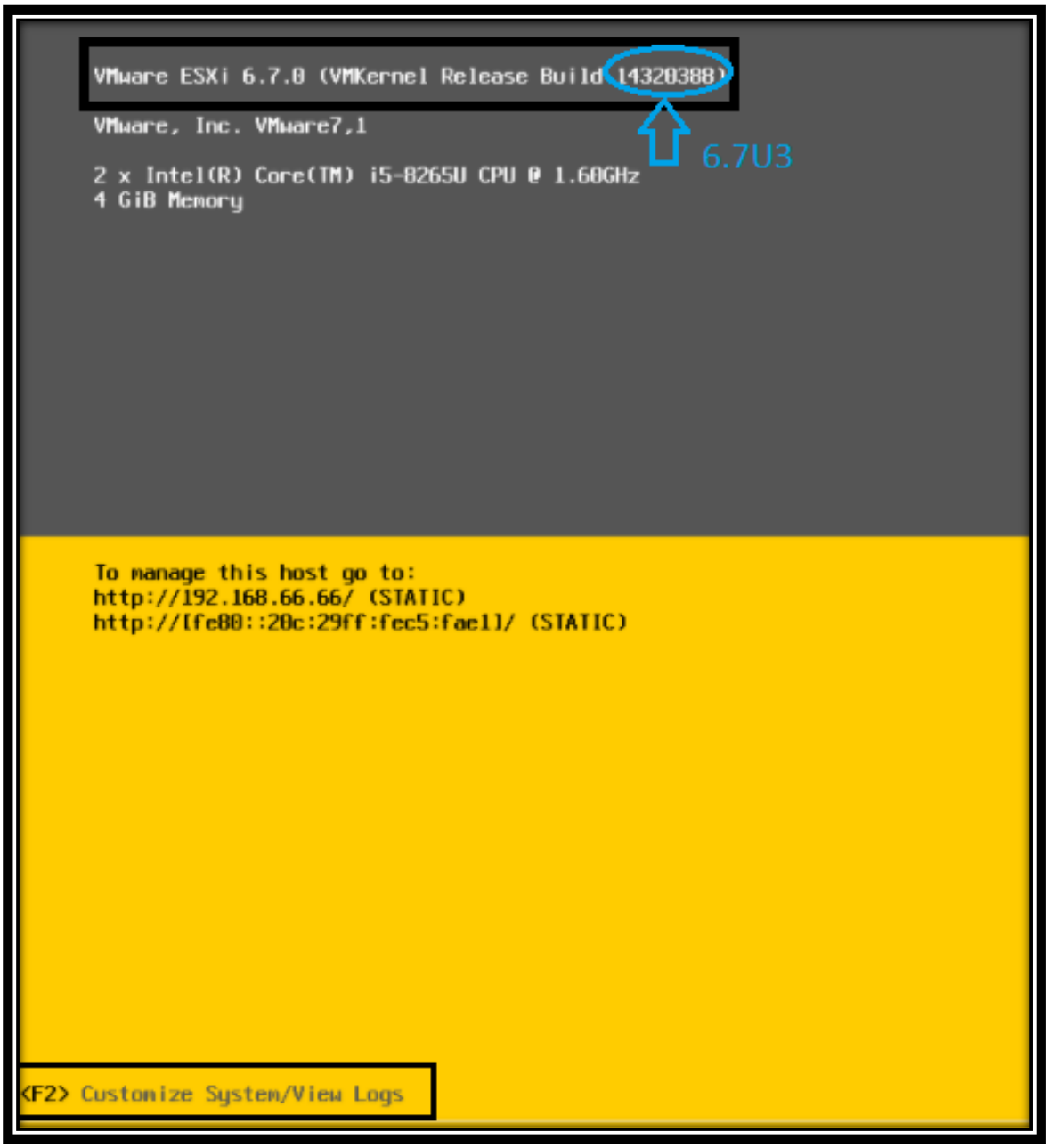


Figura 40: Inicio instalación ESXi 6.7U3

5.3 Medidas de seguridad en la configuración. *Hardening*

En el Anexo II se puede encontrar la guía de *hardening* para el ESXi de VMware elaborada durante el proyecto. Aunque se ha desarrollado y aplicado en la versión 6.7 U3, se basa en la experiencia personal y en las recomendaciones del

fabricante para todas las versiones de la 6.X. Las medidas de seguridad de esta versión han sido mejoradas respecto a versiones anteriores, por ejemplo, la política por defecto de contraseñas. Por otro lado, no ha sido probada en la versión 7.0 publicada en abril de este mismo año, no obstante, la base de securización es la misma.

En la Figura 41 se resumen los pasos de la guía referentes a la desactivación de las conexiones remotas por SSH y el acceso a la Shell de ESXi.

Además de analizar el detalle de estos puntos, se tratan otros aspectos como los tiempos de sesión para forzar una desconexión tras un periodo de inactividad, bloqueo de sesión tras un número consecutivo de intentos fallidos, filtros BPDU o configuraciones SNMP y NTP.

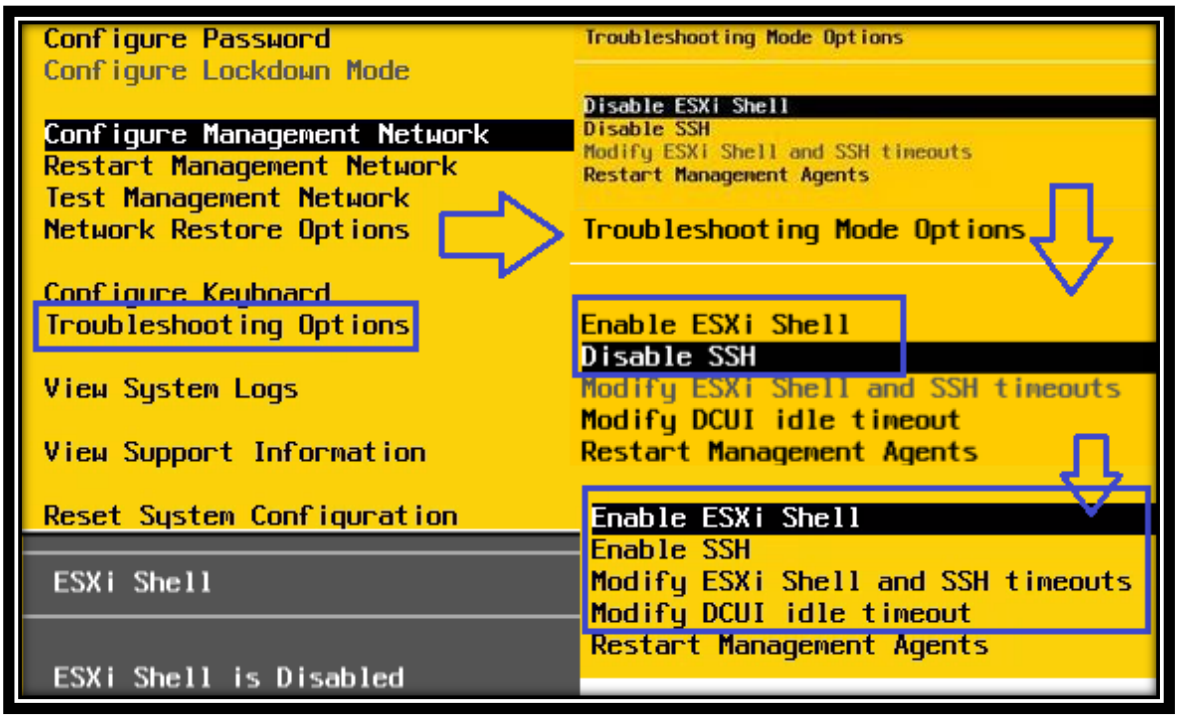


Figura 41: Deshabilitar servicios ESXi 6.7U3

Las opciones de configuración segura del ESXi pueden realizarse desde el cliente *web* o la consola del ESXi.

De cara a ataques de fuerza bruta, por diccionario o basados en reglas, es muy importante aplicar medidas de seguridad básicas a este tipo de accesos. Por ejemplo, se podría utilizar la herramienta Hydra para automatizar un acceso HTTPS o SSH contra el hipervisor. El configurar contraseñas de más de ocho caracteres, incluyendo alguno especial y, además, bloquear el inicio de sesión tras tres intentos fallidos, durante un tiempo limitado, hace que el ataque se vea penalizado notablemente o se frustre.

En el Anexo III se pueden encontrar algunos ejemplos detallados, no obstante, de cara a esquematizar un ejemplo claro, se utiliza un diccionario específico, y muy reducido, denominado “esxihack.txt”. En este diccionario se incluyen algunas contraseñas típicas, por otro lado, se utiliza un fichero denominado “users.txt”.

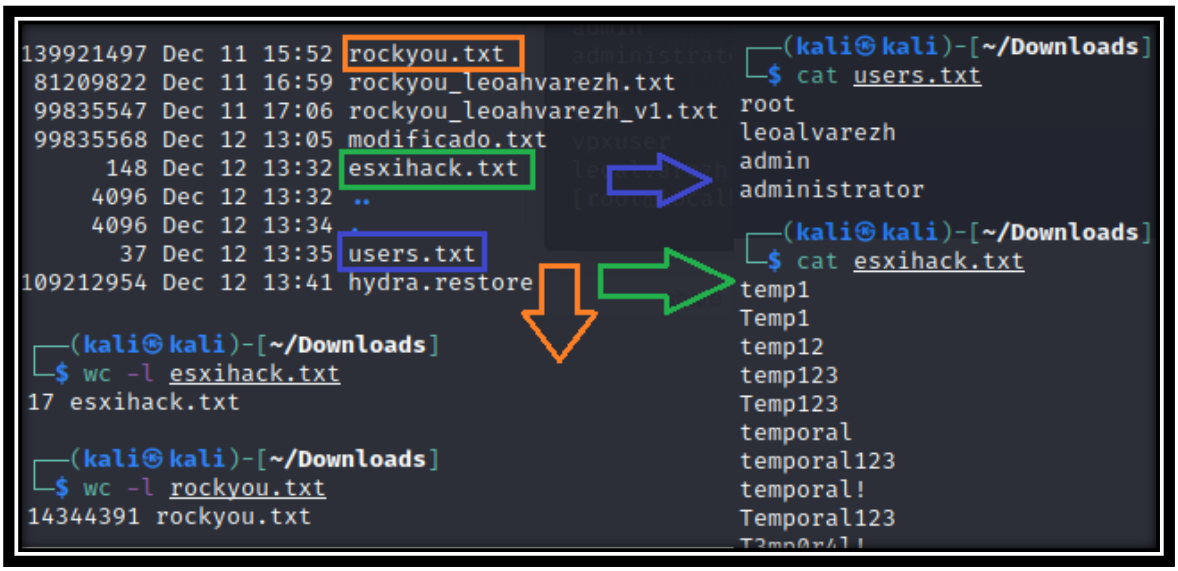


Figura 42: Diccionarios “rockyou.txt”, “esxihack.txt”, y lista de usuarios.

Se puede ver en la Figura 42 uno de los diccionarios más conocidos “rockyou.txt”, el cual se podría utilizar aumentando las posibilidades, pero también el tiempo de ataque.

En la Figura 43 se puede observar un ataque satisfactorio, mediante Hydra vía ssh, al usuario “administrator” del ESXi.

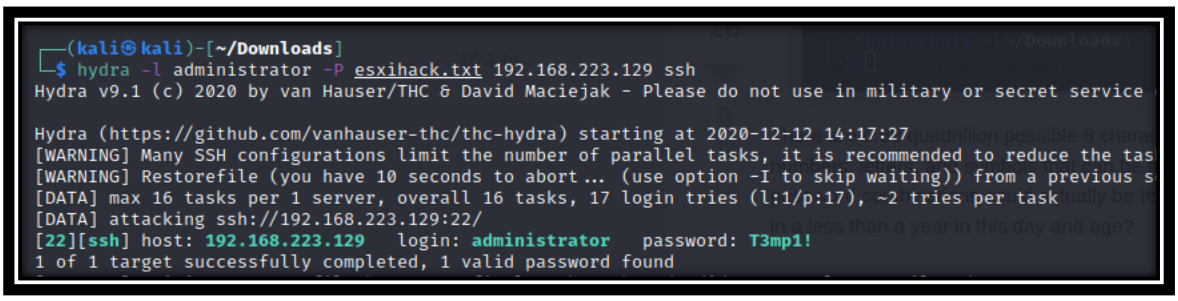


Figura 43: Ataque de diccionario con Hydra y usuario “administrator”

Hydra permite pasar, así como un fichero de contraseñas, un fichero de posibles usuarios con la opción “-L”.

hydra -L users.txt -P rockyou.txt ‘IP’ ‘protocolo’

Pudiendo utilizarse usuarios obtenidos de metadatos de la víctima o usuarios tipo; admin, administrator, root, administrador, etc.

A modo complementario en este apartado, se identifican también los puertos que utiliza un hipervisor ESXi, además de los opcionales según los servicios que se utilicen.

Puerto	Origen	Destino	Protocolo	Descripción
22	Cliente SSH	ESXi	TCP	Servidor SSH
53	ESXi	Servidor DNS	UDP	Consultas DNS
80	Cliente web	ESXi	TCP	Redirección HTTPS
123	ESXi	NTP	UDP	NTP
427	ESXi	CIM	UDP	Cliente CIM SLPv2
443	Clientes/vCenter	ESXi	TCP	Acceso HTTPS
902	ESXi	ESXi	TCP/UDP	Migración/provisión
902	Cliente	ESXi	UDP	Acceso consola VM
902	ESXi	vCenter	TCP	Heartbeat
5900-5964	ESXi	ESXi	TCP	Herramientas de gestión
5988	Servidor CIM	ESXi	TCP	Operaciones CIM
5989	vCenter/ESXi	ESXi/vCenter	TCP	CIM XLM sobre HTTPS
8000	ESXi	ESXi	TCP	Consultas vMotion
Servicios opcionales				
68	ESXi	DHCP	UDP	Servidor DHCP
161/162	ESXi	OSS	UDP	Servidor SNMP
514	ESXi	OSS	UDP	Servidor Syslog
1234/1235	ESXi	HBR	UDP	Host based replication

Figura 44: IPuertos ESXi 6.X

6. Conclusiones y trabajo futuro

6.1 Conclusiones

La inmediatez que demanda el negocio actual requiere que los despliegues TI, relacionados sobre todo con la parte de red, sean más rápidos que las implantaciones tradicionales basadas en modelos estáticos, añadiendo una complejidad real de convivencia heterogénea; entornos físicos, virtuales, y de computación en la nube. El hecho de que los entornos en la nube proliferen de forma exponencial obliga a las corporaciones a entender mejor estos entornos y sus principales problemáticas. Por consiguiente, a la hora de la elección de servicios *cloud* se ha de tener claro el tipo de infraestructura que lo soporta y el tipo de servicio que se ofrece.

La virtualización, como se ha analizado en este trabajo, soporta esta infraestructura o servicios en la nube, y se ha convertido en un campo cada vez más importante en los últimos años. Con las nuevas técnicas de virtualización, por ejemplo, las innovaciones en la virtualización de red han aparecido ventajas notables. Uno de los aspectos clave es, sin duda, la movilidad. Permitiendo el movimiento de las máquinas virtuales o servicios no solo entre diferentes equipos físicos, sino que posibilita su ubicación en diferentes centros de datos de distintos países, facilitando así la descentralización y la alta disponibilidad geográfica. No obstante, el crecimiento de la virtualización en los centros de datos también introduce vulnerabilidades en este tipo de entornos. Como se ha estudiado, algunas amenazas incluyen el ataque al hipervisor, directamente o a través del sistema operativo de la máquina virtual huésped. Otras formas de ataques que pueden comprometer potencialmente un sistema virtualizado son la extracción de bibliotecas virtuales, el ataque a los sistemas de migración de MVs, y el ataque de cifrado.

Con la evolución de este tipo de entornos, y las vulnerabilidades que han ido apareciendo en la virtualización, se han desarrollado diversas soluciones específicas para estos entornos, en muchos casos, híbridos y complejos. Estas soluciones implican la implementación de mecanismos de seguridad tradicionales como cortafuegos, detectores de intrusión y antivirus, sin embargo, desplegados dentro de la infraestructura virtual y, además, integrados con motores de *machine learning* propiciando el estudio de patrones de comportamiento y facilitando el aprendizaje automático del sistema de protección. Es decir, se incorporan mecanismos para aprender de manera automática cómo se comporta un usuario legítimo y disponer de la capacidad para discernir su comportamiento del de un *bot* o un ataque. Además, la seguridad sobre cómo se transportan, almacenan y administran las imágenes de

las VM es actualmente más relevante debido a la movilidad de las VM. Agregar una capa adicional de seguridad, implica proteger la infraestructura virtual directamente con algunas de las soluciones que existen en el mercado, se han visto algunos productos, a modo de ejemplo, que implementan estas soluciones.

Por lo tanto, tras los puntos que se han estudiado durante la ejecución de este trabajo, se considera que actualmente se puede mejorar notablemente la seguridad de un entorno virtualizado empleando las medidas que se describen en el documento. Sin embargo, el desarrollo continuo de la virtualización en los centros de datos y la nube, como el reciente crecimiento de la virtualización por contenedores, siguen generando nuevas vulnerabilidades. Sumado a la consolidación de grupos APT de ciberataques y campañas definidas como HOR (Human Operated Ransomware), presentan continuamente desafíos que deben resolverse. Sin olvidar el aspecto legal de propiedad y privacidad de los datos, que, sin haber profundizado, es relevante y también está presente. Dado que estas infraestructuras pueden gestionar los datos en múltiples países, lo que puede ocasionar conflictos en cuanto al marco legal en el que son tratados u objeto de fugas de información, ya sean intencionadas o fortuitas. Pero al mismo tiempo, hay un crecimiento en las empresas de seguridad informática, además de consolidar y evolucionar el catálogo de servicios, detectándose una mejoría en la resolución de este tipo de problemas.

En definitiva, tras el análisis realizado, se obtiene una visión global de este tipo de entornos donde la seguridad por capas sigue siendo uno de los aspectos clave. Es decir, sigue sin existir una solución o producto específico que garantice la seguridad y se debe, en la medida de lo posible, adoptar las medidas recomendadas por organizaciones como CSA, NIST, CCN-CERT, etc., y complementarlas con soluciones de seguridad. Sin olvidar las recomendaciones de cada fabricante que se utilice en el entorno, tanto de seguridad como de ciclo de vida del *software/firmware.*

Se logran, por consiguiente, los objetivos planteados al inicio del proyecto. Estableciendo, en primer lugar, el marco contextual de la evolución de los SSII y centros de datos, para posteriormente, ir definiendo y detallando una arquitectura de este tipo de entornos de nueva generación, basados en la definición de redes por *software.* Una vez se han sentado estas bases, se ha realizado el análisis de las amenazas existentes en los entornos virtuales, desde las vulnerabilidades a las rutas de ataque en base a la evolución del *malware* y los atacantes, además, se ha realizado un breve análisis de las soluciones de seguridad del mercado y diseñado una guía de recomendaciones de seguridad para el hipervisor ESXi de VMware.

Estos objetivos se han cumplido bajo la planificación establecida inicialmente, destacando un ligero desvío en la misma entre la entrega de la PEC2 y la PEC3. Este desvío se ha debido a una ejecución en paralelo de tareas de investigación de la PEC2, con tareas de diseño y de instalación de la PEC3, lo que ha propició este desalineamiento en las entregas parciales.

6.2 Trabajo futuro

Se han identificado una serie de aspectos que podrían tenerse en cuenta de cara acciones futuras. Por un lado, se prevé un crecimiento aún mayor de la virtualización por contenedor, y la migración de estas a CaaS; Container as a Service. Existen amenazas reales específicas destinadas a contenedores, como imágenes maliciosas en Docker Hub, ataques de DDoS como CoinMiner o las vulnerabilidades identificadas recientemente en Kubernetes[35]. Además, se debe tener en cuenta el despliegue de 5G y el crecimiento de redes IoT, las cuales aumentaran aún más el volumen de generar y transmitir información.

Por otro lado, se han evaluado de manera breve las diferentes soluciones de seguridad del mercado, tanto por falta de tiempo como de medios, ya que la mayoría de las demos ofrecidas requerían de un contacto con el proveedor y una acción comercial asociada. No obstante, alguno de los fabricantes proporciona la posibilidad de desplegar una demo temporal en un servicio de nube tipo AWS que también dispone de opción de demo gratuita, por ejemplo, de Workload Security Cloud One[36] de TrendMicro. En definitiva, se deberían estudiar términos como *threat hunting* y *threat intelligence,* los cuales se integran en alguna de las soluciones analizadas, con la transición del EPP a EDR.

Por último, otro de los aspectos que se han considerado importantes son la identidad y el control de acceso. La mayoría de las infraestructuras, por norma general, son compartidas por múltiples departamentos o empresas, y la mala definición de los controles de acceso puede derivar en accesos no autorizados a datos confidenciales. Por tanto, queda pendiente el análisis para la implementación de un modelo basado en *zero-trust* en la capa de acceso de este tipo de entornos descentralizados, y accesibles desde cualquier parte. La definición de una política de identidad y control de acceso basada en políticas de mínimo privilegio es esencial en este tipo de entornos. Este modelo requiere una verificación de identidad estricta para cada persona y/o dispositivo que intente acceder a los recursos de una red, aplicando técnicas como 2FA o MFA. Ya que gran parte de los ataques a la capa virtual se producen directamente por robo de credenciales o uso de contraseñas inseguras.

[35] https://www.tigera.io/blog/kubernetes-q3-2020-threats-exploits-and-ttps/
[36] https://cloudone.trendmicro.com/docs/workload-security/demo/

7. Glosario

ACL: Access Control List. Instrucciones que controlan que en un equipo de red se permita o bloquee el paso de determinado tráfico.
API: Acrónimo de Aplicación Programming Interface. Es un conjunto de rutinas que se proporcionan para proveer acceso a funciones determinadas de una plataforma o *software*.
AV: Acrónimo de antivirus.
BPDU: Bridge Protocol Data Unit. Tramas de capa dos utilizadas para el Spanning Tree Protocol.
BPDUGuard: La función BPDU Guard se utiliza para proteger la topología del Protocolo de árbol de expansión (STP) de capa dos de los ataques relacionados con BPDU.
CPD: Acrónimo de Centro de Procesamiento de Datos. Equivalente a DC (datacenter).
CLI: Es la interfaz de línea de comandos o Command Line. Método que permite dar instrucciones a algún sistema operativo o aplicación por medio de expresiones de texto.
Clúster: Conjunto de dos o más nodos que pueden compartir recursos de computación, almacenamiento o servicios. Los nodos de un clúster se monitorización entre sí mediante un heartbeat [57] .
DSVA: Deep Security Virtual Appliance. Máquina virtual de TrendMicro destinada a proteger un host físico, esencial para el tipo de protección *agentless.*
Edge Computing: Arquitectura de TI abierta y distribuida que cuenta con potencia de procesamiento descentralizada, base para las tecnologías de Internet de las cosas (IoT). Los datos son procesados por el propio dispositivo o por una computadora o servidor local, en lugar de ser transmitidos a un centro de datos lejano.
EP: Cualquier dispositivo conectado a una red se considera un punto final o EP. Actualmente son considerados EP dispositivos móviles, *smartwatches,* y otros dispositivos inteligentes habilitados para IoT.
DMZ: Red desmilitarizada o Demilitarized Zone es una red que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras las conexiones desde la red externa solamente se permitan a al DMZ [57] .
Fog Computing: Este modelo de computación se basa en el concepto de una estructura de red que se extiende desde el lugar donde se crean los datos hasta donde finalmente se almacenarán, ya sea en la nube o en el centro de datos de un cliente.

IoT: Internet of Things. Internet de las cosas es un término que hace referencia a la interconexión de objetos cotidianos con los sistemas de información o Internet.

IoE: Internet of Everything. El Internet de todo (IoE) es un concepto que extiende el énfasis de la internet de las cosas (IoT), en las comunicaciones de máquina a máquina (M2M). Tiene el objetivo de describir un sistema más complejo que también abarca personas y procesos además de los dispositivos.

MDR: Acrónimo de Managed, Detection and Recovery. Servicio de seguridad avanzado que proporciona inteligencia sobre amenazas, búsqueda de las mismas y monitorización en tiempo real, análisis de incidentes y respuesta a los mismos

MPLS: Multiprotocol Label Switching. mecanismo de transporte de datos estándar creado por la IETF que opera entre la capa de enlace de datos y la capa de red del modelo OSI [57] .

MSSP: Managed Security Service Provider. Proveedor servicios de TI que proporciona a una organización cierta cantidad de recursos de monitorización y administración relativa a la ciberseguridad. Puede incluir la gestión de *software* específico; bloqueo de virus y spam, detección de intrusiones, firewalls y administración de redes privadas virtuales (VPN).

MTR: Managed Threat Response. Similar a un MDR, pero respaldado por un equipo de *threat hunting.*

SSII: Sistemas de Información. Conjunto de elementos interrelacionados que sirven para recoger, procesar, almacenar y distribuir información dentro de una organización. Sirven, entre otros puntos, de apoyo a los procesos de análisis, visualización, coordinación y control de las actividades de la organización.

STP: Spanning Tree Protocol. Protocolo de red de capa 2 del modelo OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes [57]

SVA: Security Virtual Appliance. Appliance virtual que suelen utilizar los fabricantes de seguridad para suministrar su solución *agentless* o monitorizar el entorno virtual.

TI: Tecnologías de la información. De las siglas en Inglés IT (Information Technology). Proceso que utiliza una combinación de medios y métodos de recopilación, procesamiento y transmisión de datos para obtener nueva información de calidad sobre el estado de un objeto, proceso o fenómeno.

VDI: Virtual Desktop Infrastructure. Tecnología de virtualización que consiste en proporcionar un escritorio virtual a un usuario de forma remota.

VM: Virtual Machine. Una máquina virtual (VM) es un entorno que funciona como un sistema virtual con su propia CPU, memoria, interfaz de red y almacenamiento, pero el cual se crea en un sistema de hardware físico.

XDR: Extended Detection and Response. Nuevo enfoque para la detección y respuesta de amenazas, un elemento clave para defender la infraestructura y los datos de una organización contra daños, acceso no autorizado y uso indebido.

8. Bibliografía

- [1] “Gartner Top9 Security and Risk Trends for 2020”. Christy Pettey, Sep 2020. https://www.gartner.com/smarterwithgartner/gartner-top-9-security-and-risk-trends-for-2020/

- [2] “The 2020 State of Virtualization Technology”, Sep 2020. https://www.spiceworks.com/marketing/reports/state-of-virtualization/

- [3] “What is Virtualization and its types & Techniques.What is hypervisor and its types with Diagrams?” Shashi Soni, 22nd Aug 2018. https://www.slideshare.net/sonishashi/what-is-virtualization-and-its-types-techniqueswhat-is-hypervisor-and-its-types-with-diagrams

- [4] “Virtualization Technology for Computing System: Opportunities and …” 2012. 11 Jul. 2016 http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=4637673&gt

- [5] “Evaluación de plataformas virtuales: Estudio comparativo – RiuNet.” Gimeno Martínez, S. 2011. Oct. 2020 https://riunet.upv.es/bitstream/handle/10251/13177/tesina.pdf?sequence=1&gt

- [6] “Mainframe (big iron)” Margaret Rouse. Oct. 2020 https://searchdatacenter.techtarget.com/definition/mainframe

- [7] Scott Lowe. “Mastering VMware vSphere 5”. Sybes, John Wiley & Sons, Inc. Indianapolis, 2011.

- [8] “Los seis riesgos de la Seguridad en los entornos virtuales”. Oct. 2020 https://cso.computerworld.es/actualidad/los-seis-riesgos-de-la-seguridad-en-los-entornos-virtuales

- [9] “Security in hardware assisted virtualization for cloud computing” Dic. 2020 https://www.sciencedirect.com/science/article/pii/S1389128618302998#tbl0001

- [10] “State-of-the-Art of Virtualization, its Security Threats and Deployment Models” Dic. 2020 https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-3-2013/State-of-the-Art-of-Virtualization-its-Security-Threats-and-Deployment-Models.pdf

- [11] “Securing Cloud Hypervisors: A Survey of the Threats, Vulnerabilities, and Countermeasures” Dic. 2020. https://www.hindawi.com/journals/scn/2018/1681908/

- [12] “Informes CCN-CERT públicos” Oct. 2020 https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/?limit=25&limitstart=0

- [13] “Virtualización de red” Oct. 2020 https://www.vmware.com/es/topics/glossary/content/network-virtualization.html

- [14] “Introducción al Cloud Computing con OpenStack y OpenShift” Sesión 3 – Virtualización de redes. Oct. 2020 http://iesgn.github.io/cloud3/curso/u4/

- [15] “Virtualización de Funciones de Red y SDN” Nov. 2020 https://www.eoi.es/blogs/mtelcon/2014/02/03/virtualizacion-de-funciones-de-red-y-sdn/

- [16] “Virtualización de redes y SDN” Nov. 2020 https://www.orbit.es/virtualizacion-de-redes-y-sdn/

- [17] “VMware Validated Design Reference Architecture Guide”. Vmware Inc. Oct. 2020 https://www.vmware.com/pdf/vmware-validated-design-20-reference-architecture-guide.pdf

- [18] “¿Qué es un hypervisor?”. Red Hat Inc. Nov. 2020 https://www.redhat.com/es/topics/virtualization/what-is-a-hypervisor

- [19] “¿What is a hypervisor?”. Vmware Inc. Nov. 2020 https://www.vmware.com/topics/glossary/content/hypervisor.html?SRC=WWW_US_GP_bare-metal-hypervisor_SiteLink

- [20] “¿What is a bare metal hypervisor?”. Vmware Inc. Nov. 2020 vmware.com/topics/glossary/content/bare-metal-hypervisor

- [21] “vSphere Hypervisor”. Vmware Inc. Nov. 2020 https://www.vmware.com/es/products/vsphere-hypervisor.html

- [22] “Virtualization Technologies and Cloud Security…”. Nov. 2020 https://www.researchgate.net/publication/326696873_Virtualization_Technologies_and_Cloud_Security_advantages_issues_and_perspectives/figures?lo=1

- [23] “Terminology and Architecture”. Vmware Inc. Nov. 2020 https://communities.vmware.com/docs/DOC-5501

- [24] “Venom, una nueva amenaza con Servicios de virtualización en la mira”. Dic 2020. https://www.welivesecurity.com/la-es/2015/05/14/venom-nueva-amenaza-virtualizacion/

- [25] “Gestión de la seguridad en ambientes virtualizados”. Jan 2016. Oct 2020

https://www.welivesecurity.com/la-es/2016/01/20/seguridad-en-ambientes-virtualizados-agente/

- [26] Daniel Reis “Seguridad para la nube y la virtualización”. John Wiley & Sons, Inc. Indianapolis, 2013. Edición especial de Trend Micro.

- [27] “Protección contra virus y malware para tu entorno de virtualización”. Gary Barnett, Junio 2012. Batwick Group. Kaspersky https://media.kaspersky.com/documents/business/brfwn/sp/Proteccion-contra-virus-y-malware-para-tu-entorno-de-virtualizacion-es.pdf

- [28] “vShield Quickstart guide”. Vmware Inc. 2011. Nov. 2020 https://www.vmware.com/pdf/vshield_50_quickstart.pdf

- [29] “VMware vShield Endpoint”. Vmware Inc. Nov. 2020 https://www.vmware.com/content/dam/digitalmarketing/vmware/es/pdf/VMware-vShield-Endpoint-Datasheet.pdf

- [30] Gustavo A.A. Santana. “CCNA Cloud CLDFND 210-451 Official Cert Guide”. Cisco Press, Indianapolis, 2016

- [31] “VMware NSX - Introduction”. Nov. 2020 https://diyvirtualization.com/2018/10/03/vmware-nsx-introduction/

- [32] Chad Hintz, Cesar Obediente, Ozden Karakok. “CCNA Data center DCICN 200-150 Official Cert Guide”. Cisco Press, Indianapolis, 2017.

- [33] “Informe Cloud Computing en España 2020”. Quint Group. Nov. 2020 https://www.quintgroup.com/es-es/insights/informe-cloud-computing-espana-2020

- [34] “Inversión en Cloud se triplicará en España”. IDC Spain. Nov. 2020 https://www.blog-idcspain.com/la-inversion-en-cloud-se-triplicara-en-espana-hasta-2023-segun-idc-research-espana/

- [35] “Advanced Cloud Computing Technology”. Gartner. Nov. 2020 https://www.gartner.com/en/information-technology/insights/cloud-strategy

- [36] “12 Trending Cloud Computing Statistics & Facts 2020”. Nov. 2020 https://hostingtail.com/cloud-computing-statistics

- [37] “Top Threats to Cloud Computing: Egregious Eleven Deep Dive”. Nov. 2020 https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/

- [38] “Security Recommendations for Server-based Hypervisor Platforms”. NIST Nov. 2020 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-125Ar1.pdf

- [39] “EDR - The case for automation …”. Kaspersky Inc. Nov. 2020 https://media.kaspersky.com/en/business-security/enterprise/endpoint-detection-and-response-optimum-whitepaper.pdf

- [40] “EPP y EDR: EL futuro de la ciberseguridad endpoint”. Nov. 2020 https://www.kaspersky.es/blog/epp-edr-importance/16154/

- [41] “Antivirus, EPP and EDR. What differences?”. Nov. 2020 https://nucleon-security.com/security-insights/antivirus-epp-and-edr-what-differences/#:~:text=EPP%20is%20next%20generation%20endpoint,attempted%20system%20or%20data%20corruption

- [42] “Cortex XDR – MDR 24/7 Service”. Nov. 2020 https://paloaltofirewalls.co.uk/cortex-xdr-managed-detection-and-response/

- [43] “Virtualization and Security Boundaries”. Mike Lococo. Nov. 2020 https://mikelococo.com/files/2009/virtualization-and-security-boundaries.pdf

- [44] “Virtualization Security and Best Practices”. Rob Randell. Nov. 2020 http://www.cpd.iit.edu/netsecure08/ROBERT_RANDELL.pdf

- [45] “Guide to Security for Full Virtualization Technologies”. NIST. Nov. 2020 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

- [46] “Gartner peer Insights – Endpoint Protection Platforms”. Nov. 2020 https://www.gartner.com/reviews/market/endpoint-protection-platforms/compare/carbon-black-vs-f-secure-vs-kaspersky-vs-sentinelone-vs-trend-micro

- [47] “Seguridad en la Virtualización: Comprender la diferencia”. Kaspersky Security for Virtualization. 2014 Kaspersky Lab Iberia. Kaspersky Inc. Nov. 2020 https://media.kaspersky.com/es/business-security/KSV.%20Maximize%20Consolidation%20Ratio.pdf

- [48] “Effortless Cybersecurity for growing businesses” Kaspersky Inc. Nov. 2020 https://www.kaspersky.com/small-to-medium-business-security

- [49] “VMware Carbon Black Cloud EP” VMware Inc. Nov. 2020 https://www.carbonblack.com/products/vmware-carbon-black-cloud-endpoint/

- [50] “Audit and Remediation” VMware Inc. Nov. 2020 https://cdn.www.carbonblack.com/wp-content/uploads/VMWCB-Datasheet-VMware-Carbon-Black-Cloud.pdf

- [51] “Sentinel One Singularity Platform” SentinelOne. Dic. 2020 https://www.sentinelone.com/platform/

- [52] “F-Secure. Protection Service for Business” F-Secure. Dic. 2020 https://www.f-secure.com/content/dam/f-secure/en/business/protection-service-for-business/collaterals/digital/f-secure-protection-service-for-business-solution-overview.pdf

- [53] B. Asvija, R. Eswari, M.B. Bijoy “Security in hardware assisted virtualization for cloud computing—State of the art issues and challenges”. Bengaluru 2019.

- [54] “Guide to Security for Full Virtualization Technologies” NIST. Dic. 2020 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf

- [55] “Security of the VMware vSphere Hypervisor” VMware Inc. Dic. 2020 https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/techpaper/vmw-white-paper-secrty-vsphr-hyprvsr-uslet-101.pdf

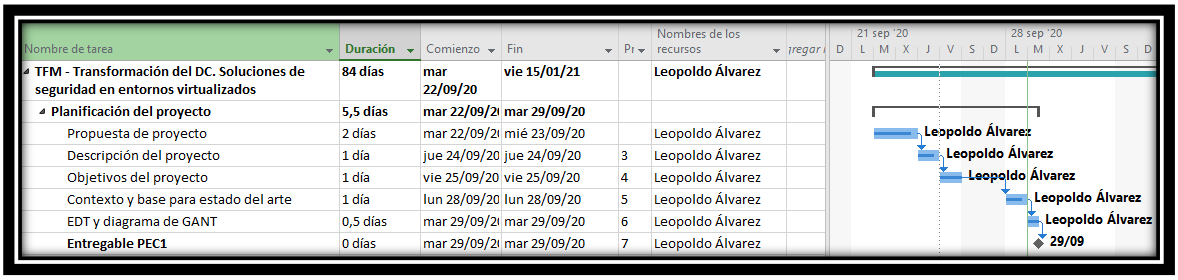
- [56] “VMware Security Hardening Guides” VMware Inc. Dic. 2020 https://www.vmware.com/security/hardening-guides.html

- [57] Harry Newton. “Newtons Telecom dictionary. 22nd edition”. Group West, Berkeley 2006.

9. Anexos

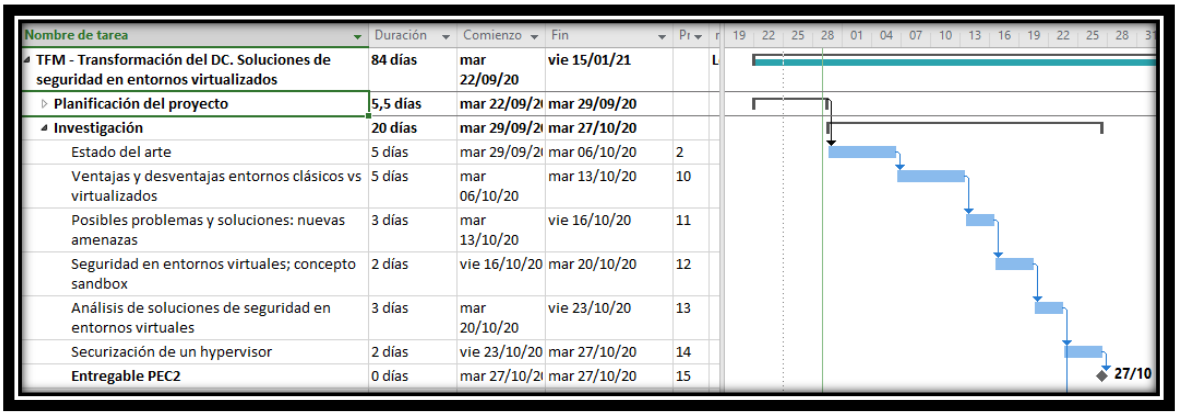
9.1 Anexo I. Planificación detallada por fases

La planificación contiene los hitos de entregas parciales; PEC1, PEC2, PEC3 y la entrega final.



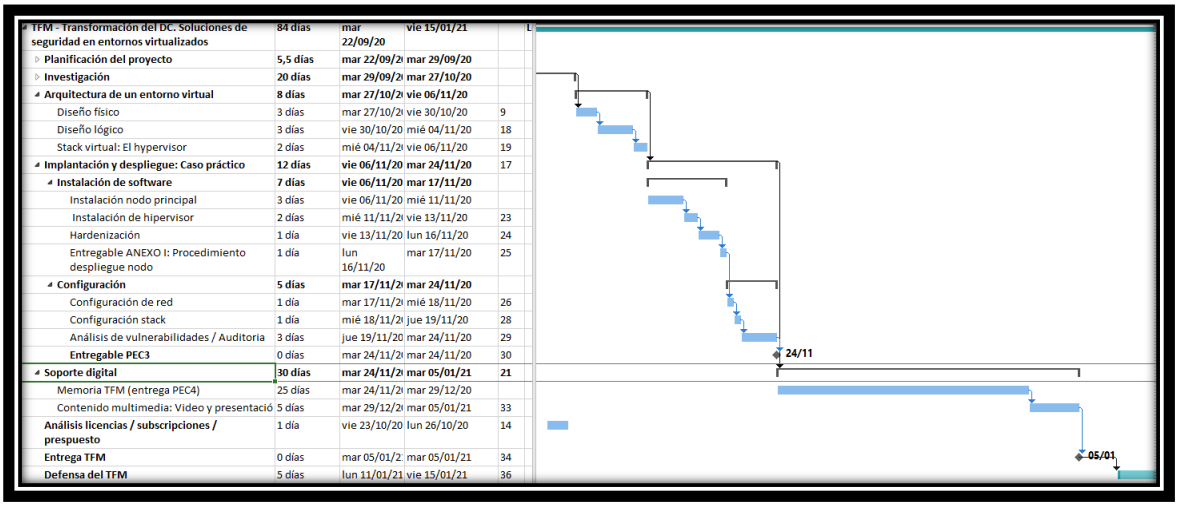
Nombre de tarea	Duración	Comienzo	Fin	Pr	Nombres de los recursos
TFM - Transformación del DC. Soluciones de seguridad en entornos virtualizados	84 días	mar 22/09/20	vie 15/01/21		Leopoldo Álvarez
Planificación del proyecto	5,5 días	mar 22/09/2	mar 29/09/20		
Propuesta de proyecto	2 días	mar 22/09/2	mié 23/09/20		Leopoldo Álvarez
Descripción del proyecto	1 día	jue 24/09/20	jue 24/09/20	3	Leopoldo Álvarez
Objetivos del proyecto	1 día	vie 25/09/20	vie 25/09/20	4	Leopoldo Álvarez
Contexto y base para estado del arte	1 día	lun 28/09/20	lun 28/09/20	5	Leopoldo Álvarez
EDT y diagrama de GANT	0,5 días	mar 29/09/2	mar 29/09/20	6	Leopoldo Álvarez
Entregable PEC1	0 días	mar 29/09/2	mar 29/09/20	7	Leopoldo Álvarez

Figura 45: Planificación detallada PEC1



Nombre de tarea	Duración	Comienzo	Fin	Pr
TFM - Transformación del DC. Soluciones de seguridad en entornos virtualizados	84 días	mar 22/09/20	vie 15/01/21	
Planificación del proyecto	5,5 días	mar 22/09/2	mar 29/09/20	
Investigación	20 días	mar 29/09/2	mar 27/10/20	
Estado del arte	5 días	mar 29/09/2	mar 06/10/20	2
Ventajas y desventajas entornos clásicos vs virtualizados	5 días	mar 06/10/20	mar 13/10/20	10
Posibles problemas y soluciones: nuevas amenazas	3 días	mar 13/10/20	vie 16/10/20	11
Seguridad en entornos virtuales; concepto sandbox	2 días	vie 16/10/20	mar 20/10/20	12
Análisis de soluciones de seguridad en entornos virtuales	3 días	mar 20/10/20	vie 23/10/20	13
Securización de un hypervisor	2 días	vie 23/10/20	mar 27/10/20	14
Entregable PEC2	0 días	mar 27/10/2	mar 27/10/20	15

Figura 46: Planificación detallada PEC2



TFM - Transformación del DC. Soluciones de seguridad en entornos virtualizados	84 días	mar 22/09/20	vie 15/01/21	
Planificación del proyecto	5,5 días	mar 22/09/2	mar 29/09/20	
Investigación	20 días	mar 29/09/2	mar 27/10/20	
Arquitectura de un entorno virtual	8 días	mar 27/10/2	vie 06/11/20	
Diseño físico	3 días	mar 27/10/2	vie 30/10/20	9
Diseño lógico	3 días	vie 30/10/20	mié 04/11/20	18
Stack virtual: El hypervisor	2 días	mié 04/11/2	vie 06/11/20	19
Implantación y despliegue: Caso práctico	12 días	vie 06/11/20	mar 24/11/20	17
Instalación de software	7 días	vie 06/11/20	mar 17/11/20	
Instalación nodo principal	3 días	vie 06/11/20	mié 11/11/20	
Instalación de hipervisor	2 días	mié 11/11/2	vie 13/11/20	23
Hardenización	1 día	vie 13/11/20	lun 16/11/20	24
Entregable ANEXO I: Procedimiento despliegue nodo	1 día	lun 16/11/20	mar 17/11/20	25
Configuración	5 días	mar 17/11/2	mar 24/11/20	
Configuración de red	1 día	mar 17/11/2	mié 18/11/20	26
Configuración stack	1 día	mié 18/11/2	jue 19/11/20	28
Análisis de vulnerabilidades / Auditoria	3 días	jue 19/11/20	mar 24/11/20	29
Entregable PEC3	0 días	mar 24/11/2	mar 24/11/20	30
Soporte digital	30 días	mar 24/11/2	mar 05/01/21	21
Memoria TFM (entrega PEC4)	25 días	mar 24/11/2	mar 29/12/20	
Contenido multimedia: Video y presentació	5 días	mar 29/12/2	mar 05/01/21	33
Análisis licencias / subscripciones / prespuesto	1 día	vie 23/10/20	lun 26/10/20	14
Entrega TFM	0 días	mar 05/01/2	mar 05/01/21	34
Defensa del TFM	5 días	lun 11/01/21	vie 15/01/21	36

Figura 47: Planificación detallada PEC3 y PEC4

9.2 Anexo II. Guía de *hardening* de un ESXi 6.7U3 (6.X)

A continuación, se anexa una guía de seguridad para hipervisores de VMware 6.X, de manera específica; 6.7 Update 3. Se incluye una columna ID para facilitar

la referencia en otros documentos o guías, sección donde recae la acción, nombre, descripción y procedimiento. Por ejemplo, VHI01-PA-02 se refiere a:

- "V" de infraestructura virtual
- "HI" de hipervisor
- "01" de *host* número uno
- "PA" de sección *password*
- "02" de segunda medida de esa sección

A esta guía se podrían añadir otras columnas de nivel o tipo de riesgo, y un *check* para que sirviese de control sobre que activos se aplica.

ID	Sección	Nombre	Descripción
VHI01-SW-01	Software	Parcheado ESXi	Mantener actualizado el ESXI en las diferentes versiones a nivel de revisión, mitiga las vulnerabilidades conocidas en el hipervisor. Un atacante capacitado puede aprovechar las vulnerabilidades conocidas al intentar obtener acceso o elevar los privilegios en un host ESXi.
	Procedimiento: Se debe mantener el ESXi actualizado a nivel de revisión. VMware dispone un ciclo de vida para cada producto y versión, no obstante, dentro de cada versión existen diferentes revisiones las cuales han de ser actualizadas ya que eliminan vulnerabilidades como 0-day. https://www.cvedetails.com/vulnerability-list/vendor_id-252/product_id-22134/Vmware-Esxi.html		
VHI01-INS-01	Instalación	Perfil VIB	Un VIB (vSphere Installation Bundle) es una colección de archivos que se empaquetan en un archivo. El VIB contiene un archivo de firma que se utiliza para comprobar el nivel de confianza. El perfil de imagen de ESXi admite cuatro niveles de aceptación de VIB: 1. VMware Certified: VIB creados, probados y firmados por VMware 2. VMware Accepted: vibraciones creadas por un socio de VMware, pero probadas y firmadas por VMware 3. Compatibilidad con partners: VIB creados, probados y firmados por un partner certificado de VMware 4. Compatibilidad con la comunidad: VIB que no han sido probados por VMware o un socio de VMware El perfil de imagen de ESXi solo debe permitir vibraciones firmadas (1-3) porque un VIB sin firmar (4) representa código no probado instalado en un host ESXi.
	Procedimiento: Para implementar el estado de configuración recomendado se debe ejecutar el siguiente comando de PowerCLI (en el código de ejemplo, el nivel es el 3, *partner*): # Establecer el nivel de aceptación de *software* para cada host Foreach ($ VMHost en Get-VMHost) { $ ESXCli = Get-EsxCli -VMHost $ VMHost $ ESXCli.software.acceptance.Set ("PartnerSupported")}		
VHI01-LOG-01	Logs	Persistencia de *logging*	El registro no persistente o permanente presenta un riesgo de seguridad porque la actividad del usuario registrada en el host solo se almacena temporalmente, por lo tanto, no se conservará durante los reinicios. Esto también puede complicar la auditoría y

			dificultar la supervisión de eventos y el diagnóstico de problemas. El registro del host ESXi siempre debe configurarse en un almacén de datos persistente
	Procedimiento: Para configurar el registro persistente correctamente, se debe realizar lo siguiente desde el cliente web vSphere: 1. Seleccionar el host e ir a "Configurar" → "Sistema" → "Configuración avanzada del sistema". 2. Introducir Syslog.global.LogDir en el filtro. 3. Configurar Syslog.global.LogDir en una ubicación persistente especificada como [datastorename] path_to_file donde la ruta es relativa al almacén de datos. Por ejemplo, [datastore1] / systemlogs. 4. Se debe asegurar de que el atributo esté resaltado, luego haga aplicar en el ícono del lápiz.		
VHI01-PA-01	Passwords	Configuración acceso	ESXi usa el complemento pam_passwdqc.so para establecer la seguridad y complejidad de la contraseña. Las opciones que proporciona incluyen establecer la longitud mínima de la contraseña, requerir que los caracteres de la contraseña provengan de conjuntos de caracteres particulares, y restringir el número de intentos de inicio de sesión fallidos consecutivos. La configuración debe hacer cumplir las políticas de contraseñas de la organización o de las buenas prácticas de seguridad. **Nota**: ESXi no impone restricciones a la contraseña de root. Las reglas de seguridad y complejidad de la contraseña solo se aplican a usuarios que no son root.
	Procedimiento: Para establecer los requisitos de complejidad de la contraseña se deben realizar los siguientes pasos: 1. Desde el cliente web vSphere, seleccionar el host. 2. Hacer *click* en "Administrar" → "Configuración" → "Sistema" → "Configuración avanzada del sistema" 3. Introducir "Security.PasswordQualityControl" en el filtro. 4. Establecer el valor siguiente o más restrictivo. "retry = 3 min = disabled, disabled, disabled, 8,8" El ejemplo requiere que todas las contraseñas tengan 8 o más caracteres y estén compuestas por, al menos, un carácter de tres a cuatro conjuntos de caracteres distintos. Además, únicamente se permite un máximo de intentos de inicio de sesión fallidos consecutivos durante 3 minutos.		
VHI01-PA-02	Passwords	Configuración acceso	La autenticación debe configurarse de modo que haya un número máximo de intentos de inicio de sesión fallidos consecutivos para cada cuenta. Superado ese número se bloquea la cuenta. Varios fallos de inicio de sesión para la misma cuenta posiblemente podrían ser un atacante que intenta adivinar la contraseña por fuerza bruta.
	Procedimiento: Para establecer correctamente el número máximo de intentos fallidos de inicio de sesión, realice los siguientes pasos: 1. En vSphere Web Client, seleccionar el host. 2. Seleccionar " Administrar" → "Configuración" → "Sistema" → "Configuración avanzada del sistema". 3. Introducir "Security.AccountLockFailures" en el filtro. 4. Hacer *click* en "Editar". 5. Establecer el valor de este parámetro en cinco o menos.		

	Alternativamente, se puede utilizar el siguiente comando de PowerCLI: Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures | Set-AdvancedSetting -Value 5 Complementado con el punto **VHI01-PA-01,** no se permitiría más de 5 intentos de sesión fallidos durante 3 minutos sin bloquear la cuenta.		
VHI01-PA-03	Password	Configuración baneo	Una cuenta se bloquea automáticamente después de que se alcanza el número máximo de intentos de inicio de sesión consecutivos fallidos. La cuenta debe desbloquearse automáticamente después de 30 minutos o más; de lo contrario, los administradores deberán desbloquear manualmente las cuentas a pedido de los usuarios autorizados.
	Procedimiento: Para configurar el bloqueo de la cuenta durante, al menos, 30 minutos, se debe realizar lo siguiente: 1. En vSphere Web Client, seleccionar el host. 2. Haga clic en "Configurar" → "Configuración" → "Sistema" → "Configuración avanzada del sistema". 3. Introducir "Security.AccountUnlockTime" en el filtro. 4. Seleccionar "Editar". 5. Establecer el valor de este parámetro en al menos 1800. Como alternativa, de cara a configurar en una planta considerable de *hosts,* se puede también utilizar el siguiente comando de PowerCLI: Get-VMHost | Get-AdvancedSetting -Name Security.AccountUnlockTime | Set-AdvancedSetting -Value 1800		
VHI01-AC-02	Accesos	Deshabilitar SSH	Se puede acceder al shell ESXi, cuando está habilitado, directamente desde la consola del host a través de la DCUI o de forma remota mediante SSH. Se recomienda desactivar Secure Shell (SSH) para cada host ESXi para evitar el acceso remoto al shell ESXi y solo habilite SSH cuando sea necesario para la resolución de problemas o el diagnóstico.
	Procedimiento: Para deshabilitar SSH, realizar lo siguiente: 1. Desde el cliente web vSphere, seleccionar el host. 2. Seleccionar " Administrar" → "Sistema" → "Perfil de seguridad". 3. Ir hasta “Servicios". 4. Hacer *click* en "Editar ...". 5. Seleccionar "SSH". 6. Seleccionar "Detener". 7. Cambiar la política de inicio a "Iniciar y detener manualmente". 8. Hacer *click* en "Aceptar". Como alternativa, se puede ejecutar vía PowerCLI: Get-VMHost | Get-VMHostService | Where {$ _. Key -eq "TSM-SSH"} | Set-VMHostService -Policy Of		
VHI01-AC-04	Accesos	DCUI *timeout*	La interfaz de usuario de consola directa (DCUI), incluida en las últimas versiones de ESXi, se utiliza para iniciar sesión directamente en un host y realizar tareas de administración. Esta configuración finaliza una sesión DCUI inactiva después de que haya transcurrido el número especificado de segundos. Terminar

			las sesiones inactivas de DCUI ayuda a evitar el uso no autorizado de DCUI que se origina en las sesiones de inicio de sesión sobrantes.
	Procedimiento: Para modificar la configuración del tiempo de espera de DCUI, se deben realizar las siguientes acciones: 1. En vSphere Web Client, seleccionar el host. 2. Haga clic en " Administrar" → "Configuración" → "Sistema" → "Configuración avanzada del sistema". 3. Introducir "UserVars.DcuiTimeOut" en el filtro. 4. Hacer *click* en "Editar". 5. Establecer el valor de este parámetro en 900 segundos o menos. Via PowerCLI: Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut | Set-AdvancedSetting -Value 900		
VHI01-COM-01	Comunicación	Deshabilitar MOB	El explorador de objetos gestionados (MOB) proporciona una forma de explorar el modelo de objetos utilizado por VMkernel para administrar el host, permitiendo cambiar las configuraciones. Esta interfaz está diseñada para usarse principalmente con el objetivo de depurar el SDK de vSphere. En 6.x está deshabilitado por defecto, no obsatnte, se incluye para que se cerciore de auditar este punto y confirmar que no haya sido activado.
	Procedimiento: Para comprobar el estado, sin modificar ningún dato: Desde ESXi Shell: vim-cmd proxysvc/service_list Desde PoweCLI: Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob Para deshabilitar MOB, se debe ejecutar el siguiente comando de shell de ESXi: vim-cmd proxysvc / remove_service "/ mob" "httpsWithRedirect" Además, se puede utilizar el siguiente comando de PowerCLI: Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.solo.enableMob | Set-AdvancedSetting -value "false" **Nota:** MOB no se puede desactivar mientras un *host* está en modo de bloqueo. Desactivar temporalmente el modo de bloqueo para desactivar MOB.		
VHI01-COM-02	Comunicación	Configuración NTP	La sincronización del Protocolo de tiempo de red (NTP) debe configurarse correctamente y habilitarse en cada host VMware ESXi para garantizar la hora exacta de los registros de eventos del sistema. Si no se utiliza una fuente de tiempo uniforme y centralizada, los eventos y las auditorías pueden ser inexactos. Al asegurarse de que todos los sistemas utilicen la misma fuente de tiempo relativo (incluido el desplazamiento de localización relevante), y que la fuente de tiempo relativo pueda correlacionarse con un estándar de tiempo acordado, es más sencillo rastrear y correlacionar las acciones de un intruso al revisar la información relevante. archivos de registro.

	Procedimiento: Para habilitar y configurar correctamente la sincronización NTP desde el cliente web: 1. Seleccione el host 2. Seleccionar " Administrar" → "Sistema" → "Configuración de hora". 3. Seleccionar en el botón "Editar". 4. Seleccionar en "NTP". 5. Proporcionar los nombres o direcciones IP de los servidores NTP. Separar los servidores con comas. 6. Si el estado del servicio NTP es "Detenido", hacer clic en "Iniciar". 7. Cambiar la política de inicio a "Iniciar y detener con el host". 8. Hacer clic en "Aceptar". Para implementar el estado de configuración recomendado de manera automatizada, se podría implementar mediante comando de PowerCLI: # Remplazar pool.ntp.org con la dirección IP o el Nombre de dominio completo (FQDN) del servidor NTP $ NTPServers = "pool.ntp.org", "pool2.ntp.org" Get-VMHost | Add-VmHostNtpServer $ NTPServers		
VHI01-COM-03	Comunicación	Configuración SNMP	Si no se está utilizando SNMP, debe permanecer deshabilitado. Sí se está utilizando, se debe configurar el destino y el resto de información adecuadamente y no mantener la información por defecto. Sí el servicio SNMP no está configurado correctamente, la información de supervisión se puede enviar a un host malintencionado que luego puede usar esta información para planificar un ataque, bien mediante obtención de datos sensibles o SNMPset. **Nota:** A partir de ESXi 5.1 se admite SNMPv3, lo que proporciona una mayor seguridad que SNMPv1 o SNMPv2c, incluida la autenticación y el cifrado de claves. Se recomienda utilizar, siempre que sea posible, la versión 3.
	Procedimiento: Según la versión de SNMP se deben ejecutar unas acciones u otras. Se añaden los enlaces para las 3 versiones: SNMPv3 (recomendada): https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-2E4B0F2A-11D8-4649-AC6C-99F89CE93026.html SNMPv1/2c: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-2A8FC3DC-53C3-4245-A4CF-CC5C7935D04B.html		
VHI01-RED-01	Red	Deshabilitar modo promiscuo en vSwitch	Cuando el modo promiscuo está habilitado para un *switch* virtual (vSwitch), todas las máquinas virtuales conectadas al dvPortgroup tienen el potencial de leer todos los paquetes que cruzan esa red. Esto podría permitir el acceso no autorizado al contenido de esos paquetes.
	Procedimiento: Para configurar la política para no permitir este modo promiscuo, se debe realizar lo siguiente: 1. En vSphere Web Client, navegar hasta el host. 2. Ir a "Hosts y clústeres" → "vCenter" → host. 3. En la pestaña “Configurar”, se debe seleccionar “Redes” y seleccionar “Switches virtuales”.		

	4. Seleccionar un “estándar” y editar la configuración seleccionando el icono del lápiz. 5. Seleccionar “Seguridad”. 6. Establecer el modo promiscuo en "Rechazar". 7. Hacer clic en "Aceptar". Se puede automatizar vía shell de ESXi: # esxcli network vswitch standard policy security set -v vSwitch2 -p false **Nota:** Se debe tener en cuenta que rechazar el modo promiscuo puede afectar a algunas sondas de análisis de tráfico, por ejemplo, de los productos de seguridad estudiados.		
VHI01-RED-02	Red	Política cambio de MAC	Si el sistema operativo de la máquina virtual cambia la dirección MAC, puede enviar tramas con una dirección MAC de origen suplantada en cualquier momento. Esto permite provocar ataques mal intencionados en los dispositivos de una red haciéndose pasar por un adaptador de red autorizado por la red receptora. Se debe asegurar de que la política de cambio de dirección MAC dentro del vSwitch esté configurada para rechazar. “Reject Mode”
	Procedimiento: Para configurar la política de rechazar el cambio de MAC, se debe realizar lo siguiente: 1. En vSphere Web Client, navegar hasta el host. 2. Ir a "Hosts y clusters" → "vCenter" → “host”. 3. En la pestaña “Administrar” → “Redes” y seleccionar “vSwitches” . 4. Seleccione un Std vSwitch de la lista y editar la configuración. 5. Seleccionar “Seguridad”. 6. Configurar los cambios de dirección MAC en modo *reject* "Rechazar". 7. Haer clic en "Aceptar". Se puede realizar vía shell ESXi: # esxcli network vswitch standard policy security set -v vSwitch2 -m false		
VHI01-RED-03	Red	Activar filtro BPDU	BPDU Guard y Portfast se habilitan comúnmente en el *switch* físico al que el host ESXi está conectado directamente para reducir el retraso de convergencia de STP. Si se envía un paquete BPDU desde una máquina virtual en el host ESXi al *switch* físico así configurado, puede ocurrir un bloqueo en cascada de todas las interfaces de enlace ascendente desde el host ESXi. Para evitar este tipo de bloqueo, el filtro BPDU se puede habilitar en el host ESXi para descartar cualquier paquete BPDU que se envíe al conmutador físico. Se debe revisar la infraestructura, ya que ciertas VPN SSL pueden generar legítimamente paquetes BPDU. El administrador debe verificar que no haya paquetes BPDU legítimos generados por máquinas virtuales en el host ESXi antes de habilitar este filtro. Si el filtro BPDU está habilitado en esta situación, habilitar 'Reject Forged Transmits’ en el PG del vSwitch agregando protección contra los bucles de STP. **Nota:** Verificar que no se requieran máquinas virtuales para enviar BPDU en el host ESXi.

	Procedimiento: Para habilitar el filtro BPDU en el host ESXi se deben realizar los siguientes pasos desde vSphere Client: 1. Con vSphere Client, cambiar a la vista “Hosts and Clusters”. 2. Seleccionar el host deseado de la vista de árbol de inventario en el panel izquierdo. 3. Seleccionar en la pestaña “Configuración” y luego en “Configuración avanzada”. 4. Seleccionar en “Red” y luego buscar la opción “Net.BlockGuestBPDU”. 5. Cambiar el valor a 1, que habilita el filtrado BPDU. 6. Hacer clic en Aceptar. **Nota:** Antes de habilitar el "Filtro BPDU" en el host ESXI, verificar que no se requieran máquinas virtuales (GuestVM) para enviar BPDU legítimas en el host ESXi. Sí alguna de las VMs requiere generar tráfico BPDU legítimo, activar el filtro BPDU en todas las máquinas virtuales excepto en la afectada. Se puede parametrizar de manera específica. Los pasos para hacerlo son los siguientes: Habilitación del filtro BPDU en máquinas virtuales individuales donde no se requiere VPN / Bridging: 1. Apagar la máquina virtual (solo aquellas que no requieran VPN / Bridging) siguiendo el procedimiento adecuado específico del sistema operativo. 2. Seleccionar con el botón derecho en <máquina virtual invitada> en el árbol de navegación. 3. Ir a “Editar configuración” → “Opciones” → “Avanzado” → “General”. 4. En el panel Configuración, hacer *click* en “Parámetros de configuración”. 5. En el panel Parámetros de configuración, doble *click* en cualquiera de las configuraciones que se muestran a continuación para cambiar el valor en el campo valor para que coincida con el estándar de la organización Si la configuración no está presente, hacer *click* en el botón “Agregar” para crear una nueva configuración de “Nombre” y “Valor” de la siguiente manera: Net.BlockGuestBPDU 1 6. Reiniciar la VM.

9.3 Anexo III. Evidencias de ataques y contramedidas de la guía

Se realiza un escaneo mediante Nmap del hipervisor y se obtiene algún puerto más de los indicados por VMware.

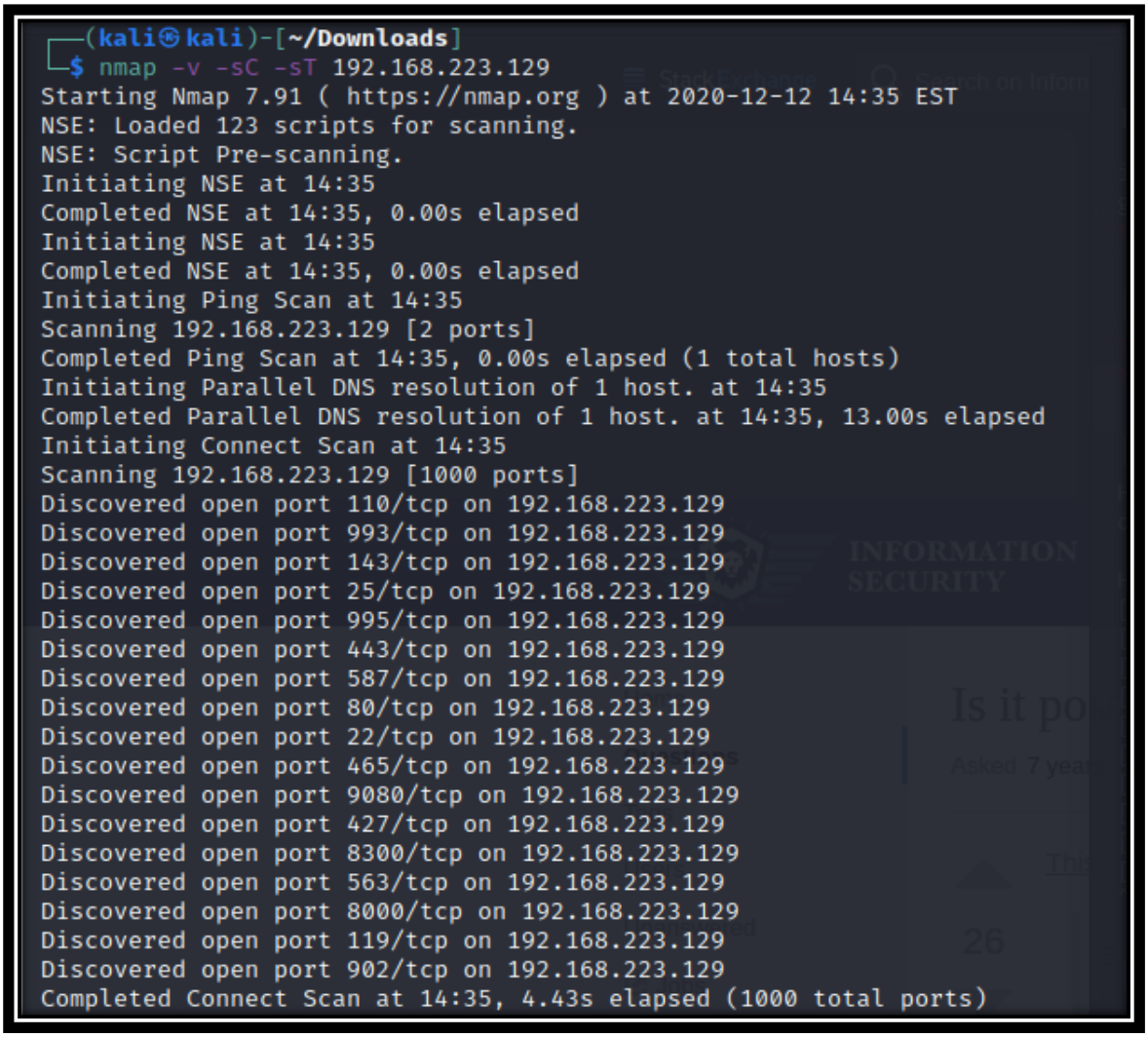


Figura 48. Nmap del ESXi 6.7U3

PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.9 (protocol 2.0)
25/tcp open smtp?
80/tcp open http VMware ESXi Server httpd
110/tcp open pop3?
119/tcp open nntp?
143/tcp open imap?
427/tcp open svrloc?
443/tcp open ssl/https VMware ESXi SOAP API 6.7.0
465/tcp open smtps?
546/tcp closed dhcpv6-client
563/tcp open snews?
587/tcp open submission?
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
993/tcp open imaps?

```
995/tcp  open   pop3s?
5988/tcp closed wbem-http
5989/tcp closed wbem-https
8000/tcp open   http-alt?
8300/tcp open   tmi?
9080/tcp open   ssl/soap       gSOAP 2.8
Service Info: Host: localhost.localdomain; CPE: cpe:/o:vmware:esxi,
cpe:/o:vmware:ESXi:6.7.0
```

En esta versión de ESXi 6.7 U3 no viene por defecto configurado el servicio SNMP:

```
$ snmpwalk -v 2c -c public 192.168.223.129
Timeout: No Response from 192.168.223.129
```

Hipervisor

```
[admin@localhost:~] esxcli system snmp test
Must first configure at least one v1|v2c|v3 trap target
[admin@localhost:~] esxcli system snmp get
   Authentication:
   Communities:
   Enable: false
   Engineid:
   Hwsrc: indications
   Largestorage: true
   Loglevel: info
   Notraps:
   Port: 161
   Privacy:
   Remoteusers:
   Syscontact:
   Syslocation:
   Targets:
   Users:
   V3targets:
```

De lo contrario, como se puede ver en diferentes sistemas, se podría consultar, por defecto, lectura con la comunidad “public” y escritura con “private”.

A continuación, se lanza un ataque basado en diccionario. Para ello se emplean diccionarios conocidos como “fastrack.txt” o “rockyou.txt”, además de alguno modificado. La nueva política de VMware para su hipervisor 6.7 y 7.0 hace que la contraseña de root sea, por defecto, de mínimo siete caracteres, por lo tanto,

se puede realizar una modificación del “rockyou.txt” excluyendo palabras con menos de siete caracteres, además, se puede realizar un diccionario a medida con la herramienta Crunch. Se debe tener presente, a la hora de elaborar un diccionario, las tendencias actuales, por ejemplo:

Sustitución de vocales por números
a → 4
e → 3
i → 1
o →0
Inclusión de caracteres especiales como “.”, “@”, “!” o “#” en las claves, inicio o al final de estas
hola → H0l4!
Inclusión de palabras relacionadas con el sistema al que se accede
4dm1nvc3nter
H1p3rv1s0r!

En la Figura 49 se muestran algunos de los diccionarios y algunas palabras relacionadas con la contraseña “temporal” del contenido de uno de ellos, además, se lanza un ataque con Hydra al usuario “administrador”.

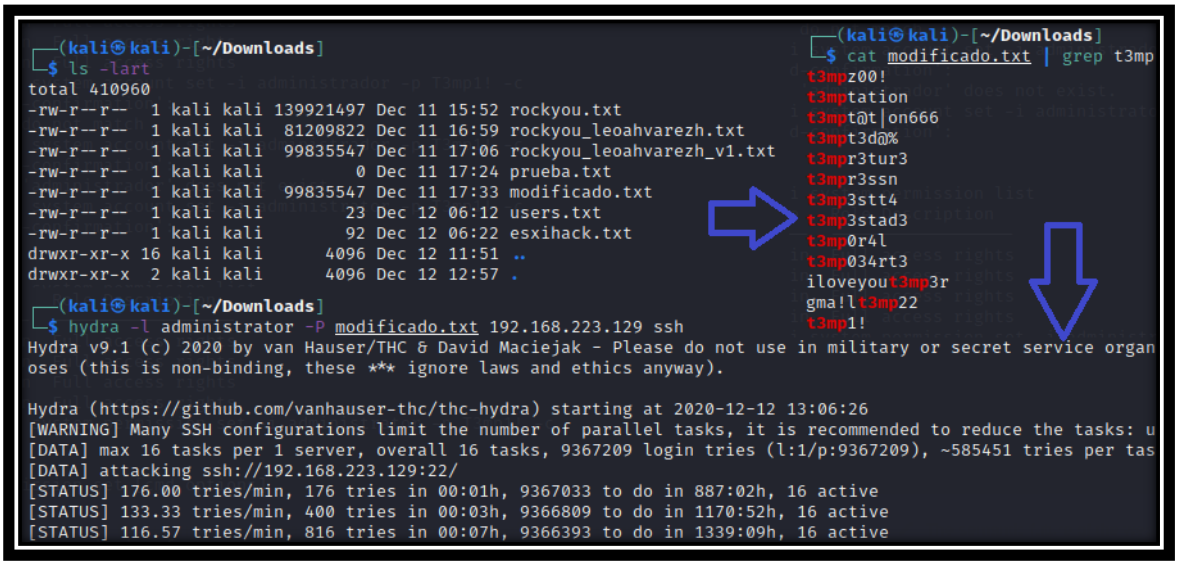
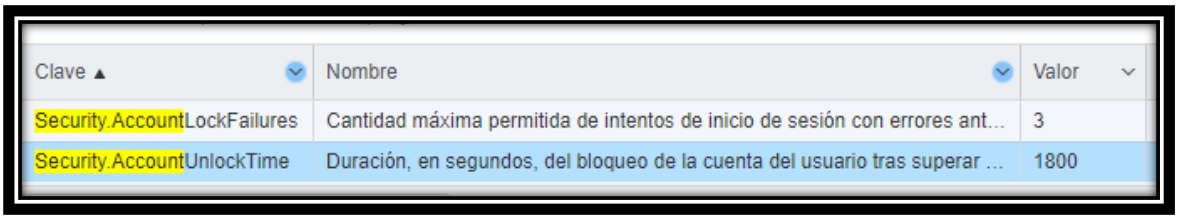


Figura 49. Diccionarios, muestra de contenido e Hydra

Sí se observa la salida de Hydra con el diccionario modificado se puede ver que dispone de nueve millones de intentos de *login*, y la salida por pantalla va indicando el número de intentos por minuto, el acumulado, y los hilos activos en paralelo. Tal y como se desarrolló en el trabajo, un ataque basado en diccionario o fuerza bruta puede ser efectivo si se utilizan contraseñas típicas, débiles o

cortas, a partir de ahí, el tiempo y los recursos juegan un papel clave. No obstante, si se aplican contramedidas como las que se han desarrollado en la guía, como el bloqueo de un usuario tras tres intentos de sesión fallidos, se verá que la efectividad de estos ataques tiende a desaparecer.



Clave ▲	Nombre	Valor
Security.AccountLockFailures	Cantidad máxima permitida de intentos de inicio de sesión con errores ant...	3
Security.AccountUnlockTime	Duración, en segundos, del bloqueo de la cuenta del usuario tras superar ...	1800

Figura 50. Número máximo de intentos 3 fallidos y 30 mins de bloqueo.

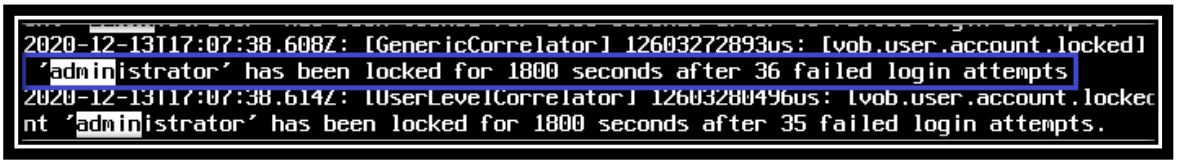


Figura 51. Bloqueo tras aplicar política de seguridad y ataque con Hydra

En la Figura 51 se puede observar como el usuario "administrador" ha sido bloqueado durante 30 minutos, tal y como se recomienda en la guía que se ha desarrollado. Se pueden ver los intentos fallidos, que ha provocado el ataque por diccionario, propiciando el bloqueo de la cuenta durante el tiempo establecido. Por otro lado, desactivando ESXi Shell, SSH y DCUI, prácticamente se obtiene poca información desde el exterior, desde el servicio HTTPS.

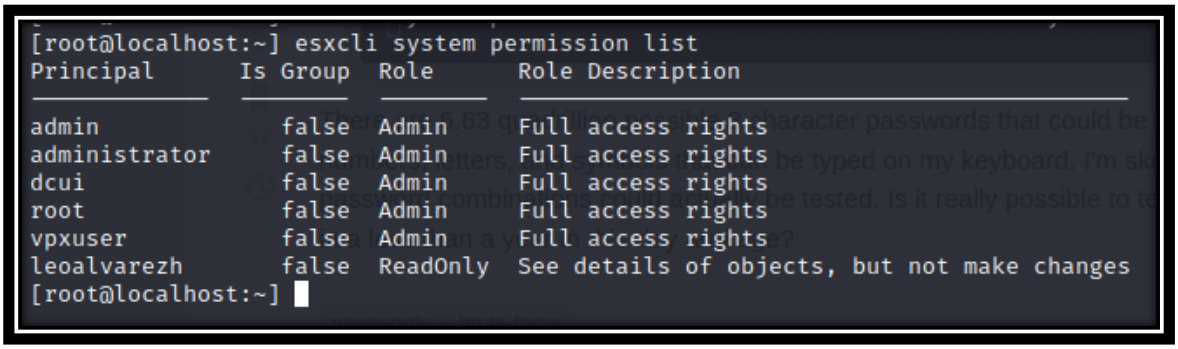


Figura 52. Usuarios del ESXi. Root, vpxuser y dcui por defecto.

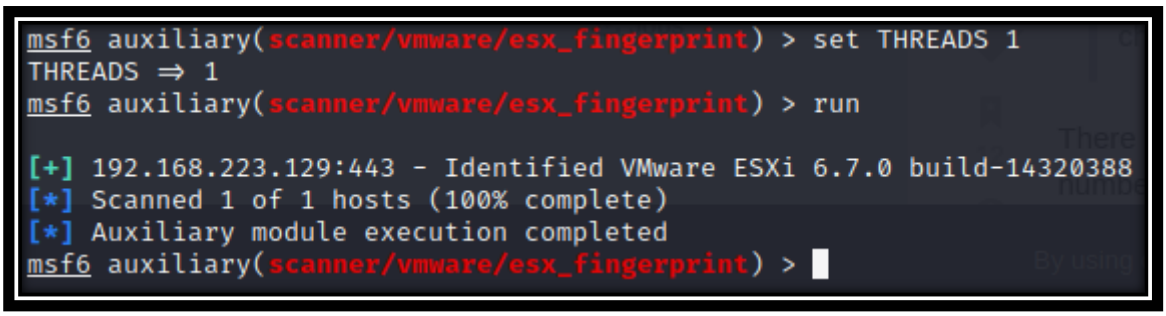


Figura 53. Fingerprinting del ESXi desde metasploit

```
SaltStack Salt Master Server Root Key Disclosure
VMware vCenter Server vmdir Information Disclosure
MS15-034 HTTP Protocol Stack Request Handling HTTP.SYS Memory Information Disclosure
Directory Traversal in Spring Cloud Config Server
VMWare ESX/ESXi Fingerprint Scanner
VMWare Authentication Daemon Login Scanner
VMWare Authentication Daemon Version Scanner
VMWare Enumerate Permissions
VMWare Enumerate Active Sessions
VMWare Enumerate User Accounts
VMWare Enumerate Virtual Machines
VMWare Enumerate Host Details
VMWare Web Login Scanner
VMWare Screenshot Stealer
VMware Server Directory Traversal Vulnerability
VMWare Update Manager 4 Directory Traversal
Cisco UCS Director Cloupia Script RCE
F5 BIG-IP TMUI Directory Traversal and File Upload RCE
VMware Workstation ALSA Config File Local Privilege Escalation
VMWare Setuid vmware-mount Unsafe popen(3)
SaltStack Salt Master/Minion Unauthenticated RCE
VMware VDP Known SSH Key
VMware Hyperic HQ Groovy Script-Console Java Execution
Novell NetWare LSASS CIFS.NLM Driver Stack Buffer Overflow
OS X VMWare Fusion Privilege Escalation via Bash Environment Code Injection (Shellshock)
VMware Fusion USB Arbitrator Setuid Privilege Escalation
Foswiki MAKETEXT Remote Command Execution
VMWare OVF Tools Format String Vulnerability
Tom Sawyer Software GET Extension Factory Remote Code Execution
VMWare OVF Tools Format String Vulnerability
VMware vCenter Chargeback Manager ImageUploadServlet Arbitrary File Upload
```

Figura 54. Algunos módulos en Metasploit relacionados con VMware

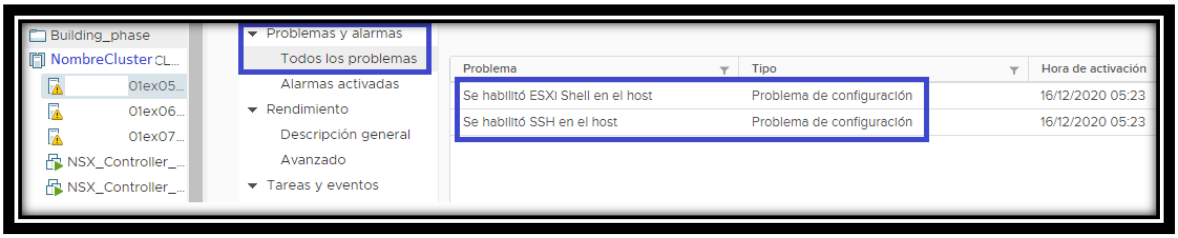


Figura 55. Alarma vCenter ESXi Shell y SSH

Es importante no desactivar la monitorización de los servicios en el ESXi para que, si se habilita el SSH o el ESXishell, aparezcan los avisos y alarmas en el vCenter o en el interfaz web del ESXi, como se puede ver en la Figura 55.

Por último, se ha observado que cuando se hace un “Reset System Configuration” al hipervisor este pierde la contraseña de “root” y se puede acceder con contraseña en blanco. Importante volver a configurar una nueva.