ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE LAS NORMAS DE SEGURIDAD DE DATOS (DSS) DE LA INDUSTRIA DE TARJETAS DE PAGO (PCI) VERSIÓN 2.0, PARA EL MEJORAMIENTO DE LAS POLÍTICAS DE SEGURIDAD EN UNA INFRAESTRUCTURA VIRTUALIZADA DE UNA INSTITUCIÓN EMISORA DE TARJETA DE CRÉDITO."

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

EDDIE GUILLERMO CARRASCO RIVERA

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

Primeramente quiero agradecer a Dios por llenarme de bendiciones, a mis padres por el apoyo incondicional y en especial a mi amada esposa por estar siempre a mi lado dándome fortaleza e inspiración para mi crecimiento profesional.

DEDICATORIA

Dedico este trabajo en especial a mi amada Madre Petita Rivera Cabrera por haber sido quien me supo guiar por el camino del éxito y del crecimiento como profesional, a mi padre por el apoyo incondicional, a mi amada esposa y a mi hijo por ser el motor de mi vida para seguir adelante y así poder culminar mi objetivo trazado, y a mi querida familia.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

DIRECTOR MSIA

MGS. NÉSTOR ARREAGA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

MGS. ROBERT ANDRADE

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El objetivo de este trabajo es Implementar mejoras a los políticas de seguridad de una infraestructura virtualizada, basado en los requerimientos y medidas de seguridad que establece la norma de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) versión 2.0, utilizando las directrices y las herramientas que garanticen el cumplimiento de la misma en ambientes virtualizados, y como objetivo principal reducir los fraudes relacionados con las tarjetas de crédito y aumentar la seguridad de los datos.

Los requisitos de la norma PCI DSS tienen como objetivo asegurar que el software y la infraestructura de las instituciones generadoras de tarjeta de crédito se alineen a las buenas prácticas de seguridad recomendadas para proteger los datos de los titulares de tarjetas.

Estos requisitos se aplican a todos los componentes del dentro de la infraestructura, tales como red, servidores, o cualquier aplicación que este dentro del entorno de los datos del titular de la tarjeta. Estos componentes incluyen además todo lo que conforma un entorno de virtualización, tales como Switches o routers virtuales, dispositivos virtuales e hipervisores.

Se propone implementar los requisitos que indica la norma en una infraestructura virtualización con Vmware Vshpere 5.5, donde obtendremos mejoras en los controles de acceso, políticas de seguridad, y además en base a las buenas prácticas que indica el fabricante, se cumplirán los requisitos que indica PCI DSS Versión 2.0 para ambientes virtualizados.

La propuesta apunta no solo a cumplir con los requisitos que indicar la norma PCI DSS sino además proporcionar una orientación de los pasos que se deben seguir para el cumplimiento de la norma en una infraestructura virtualizada. Este trabajo está realizado en una infraestructura Vmware Vsphere 5.5 y se deja abierta la posibilidad de ser utilizado para su implementación.

ÍNDICE GENERAL

ABREVIATURAS

CDE	Cardholder data environment
PCI DSS	Payment Card Industry Data Security Standard
RBAC	Acceso Basado en Roles.
VMM	Virtual Machine Monitor

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En la actualidad las entidades emisoras de tarjeta de crédito, guardan o gestionan los datos de los titulares de las tarjetas de crédito y deben garantizar la seguridad de esta información, debido a que su infiltración por ataques informáticos podría conllevar a fraudes informáticos. Con el fin de combatir estos tipos de fraudes las entidades como "*American Express, JCB International, Discover Financial Services, MasterCard y Visa Inc.*[1]", [1] crearon el PCI Security Standard Council, estas empresas unificaron todos sus requisitos de seguridad con el objetivo de crear una norma para el cumplimiento de la seguridad y protección de los datos de la Tarjeta de crédito. Esto conlleva a las entidades emisoras de Tarjeta de crédito asegurar su infraestructura, para que así las transacciones de sus clientes se realicen en un entorno seguro y por tal motivo es fundamental el cumplimiento de la normativa PCI DSS. [1]

Cuando se habla de un entorno de seguridad y del cumplimiento de la norma no solo se trata de proteger de fraude o ataques informáticos a los datos de los titulares de las tarjetas de crédito (CDE), sino que además se obtendremos grandes oportunidades para el crecimiento del negocio, tales como seguridad en los sistemas de información, incrementar la confianza de los clientes con la

[1] https://es.pcisecuritystandards.org/security_standards/role_of_pci_council.php

entidad, diseñar estrategias de seguridad para prevenir que la infraestructura se vulnerada y obtener la certificación PCI DSS. De esta manera se genera dentro de la entidad una cultura de seguridad de la información.

Es muy importante indicar que los requerimientos de la normativa PCI DSS ayudarán a incrementar la seguridad a los datos de los titulares de las tarjetas de crédito, y con una mejora constante se van realizando lanzamientos de nuevas versiones, con nuevos requisitos que las entidades emisoras de tarjeta de crédito deben adoptar con rapidez, ya que el incumplimiento de la normativa podría originar afectación a los datos de los titulares de las tarjetas de crédito siendo vulnerados por una persona malintencionada. Este efecto provocaría una mala imagen y reputación de la entidad, ya que se puede generar fuga de información. Como las entidades se enfrentan auditorias severas, un incumplimiento de las mismas puede acarrear una cuantiosa multa. [1]

En éste trabajo nos enfocaremos en implementar los requistos en una infraestructura virtualizada con Vmware Vsphere 5.5, utilizando las herramientas y buenas prácticas que indica el fabricante y las normas PCI DSS para entornos virtuales.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

En la actualidad las instituciones que emiten tarjeta de crédito implementan soluciones de infraestructura virtualizada, la misma que está compuesta de hosts, máquinas virtuales, aplicaciones, interfaces de administración, consolas centrales, hypervisores, etc. y además algunas medidas de control para garantizar la seguridad del ambiente.

Para éste caso, la institución tiene como solución de virtualización Vmware vSphere 5.5, la cual cuenta con sus hosts y máquinas virtuales incluyendo plantillas de servidores con sistema operativo Microsoft Windows y Linux. La infraestructura de servidores posee procedimientos de seguridad donde realizan aplicaciones de parches de seguridad de sistema operativo y los equipos poseen protección de Antivirus.

Para validar si cumplimos con los requerimientos que indica la norma, se realizó una evaluación de la infraestructura Virtual con la herramienta VMware Compliance Checker for PCI[2]. El resultado que presentó la herramienta nos demostró que la infraestructura virtual actual no cumplía con todos los requerimientos que la norma PCI DSS[3] exige para el ambiente de virtualización. El análisis destaca los puntos en los cuales existe incumpliendo y lo que se debe corregir en el ambiente virtualizado en vmware vsphere 5.5.

El incumplimiento de los requerimientos puede originar la terminación inmediata de las licencias y de los privilegios de generación de Tarjetas de crédito para la institución.

1.2 SOLUCIÓN PROPUESTA SOLUCIÓN PROPUESTA.

Debido que las instituciones emisoras de tarjetas de crédito requieren garantizar que su infraestructura cumple con los estándares de seguridad exigidos por los organismos de control, por tal motivo se realizará mejoramiento en la infraestructura virtual basado en las directrices de implementación de PCI DSS y las buenas prácticas recomendadas por el fabricante Vmware Inc[4].

---

[2] http://www.vmware.com/products/pci-compliance-checker/overview
[3] Payment Card Industry Data Security Standard
[4] http://www.vmware.com/

Con información obtenida de la herramienta VMware Compliance Checker for PCI, se realizarán los debidos ajustes en configuración de los Host, máquinas Virtuales, y otros cambios que la infraestructura virtual requiera, para el cumplimiento de todos los requerimientos que indica PCI DSS versión 2.0.

Finalizado los ajustes en la infraestructura virtual Vmware vSphere 5.5 obtendremos la mejora en los controles de acceso, políticas de seguridad en base a las buenas prácticas que indica el fabricante y el cumplimiento de los requerimientos que indica PCI Dss Versión 2.0 para ambientes virtualizados.
En resumen los beneficios que ofrece esta solución son:

Tener una infraestructura Virtual que cumpla con los requerimientos que indica la norma PCI DSS versión 2.0, se mejorarán las políticas de Seguridad para el ambiente virtual y se obtendrá una infraestructura virtual ajustada a las buenas prácticas de Vmware Inc.

CAPÍTULO 2

METODOLOGÍA Y DESARROLLO DE LA SOLUCIÓN.

2.1 METODOLOGÍA PARA LA IMPLEMENTACIÓN DE REQUERIMIENTOS PCIDSS VERSIÓN 2.0 PARA INFRAESTRUCTURA VIRTUAL EN VMWARE VSPHERE 5.5.

La metodología que se utilizará se basará en lo indicado por la documentación que proporciona la "PCI Security Standards Compliance[5]", sobre los requisitos y procedimientos de evaluación de seguridad versión 2.0, además con lo indicado en la exploración de PCI DSS sobre la comprensión del objetivo de los requisitos enfocados a los ambientes virtuales.

Como guías principales se utilizará la información suplementaria de PCI DSS para virtualización versión 2.0. Y Además como parte importante los documentos proporcionados por el fabricante sobre VMware "Solution Guide for Payment Card Industry (PCI)"[6]. Los documentos recogen los principales

[5] https://www.pcisecuritystandards.org/
[6] https://www.vmware.com/files/pdf/VMware-Payment-Card-Industry-Solution-Guide.pdf

aspectos relacionados con la tecnología de virtualización y básicamente, las guías incluyen:

- Una descripción de lo que es la virtualización en un nivel alto.
- Los principales riesgos de la implementación de ambientes virtuales.
- Las mejores prácticas y recomendaciones para su implementación, tanto con carácter general y los distintos niveles de riesgo que afectados o no por PCI DSS.
- Recomendaciones para ambientes implementados en la nube.
- Una pequeña guía para realizar una evaluación de riesgos en entornos virtuales.
- Finalmente, un detalle de cómo afecta la virtualización en cada uno de los requerimientos del estándar PCI DSS.

En los documentos se observan puntos importantes, como por ejemplo, si cualquier componente virtual está conectado o es parte del ambiente donde están los datos de los titulares de la tarjeta o CDE[7], entonces el hypervisor también está dentro del alcance de PCIDSS. Además sobre las recomendaciones propuestas se incluye orientación para asegurar el hypervisor, las máquinas y el resto de componentes virtuales.

[7] Cardholder data environment

Es importante mencionar una descripción general de las normas de seguridad de datos de la PCI DSS, ya que fueron creadas mejorar los entornos de seguridad de los datos del titular de la tarjeta y está norma aplica a todas las entidades emisoras de tarjeta de crédito o de pago. En la tabla adjunta se detalla los doce requisitos de la norma PCI DSS:

Tabla 1 Descripción general de los 12 requisitos de la Norma PCIDSS

Fuente: [1]

Normar de seguridad de datos de la PCI: descripción general de alto Nivel		
Desarrolle y mantenga redes y sistemas seguros	1.	Instalar y mantener una configuración de firewall para proteger los datos del titular de la tarjeta.
	2.	No utilizar contraseñas de sistemas y otros parámetros de seguridad provistos por los proveedores.
Proteger los datos del titular de la tarjeta	2.	Proteger los datos del titular de la tarjeta que fueron almacenados.
	3.	Cifrar la transmisión de los datos de las tarjetas a través de redes públicas abiertas.
Mantener un programa de administración de vulnerabilidad.	4.	Utilizar y actualizar con regularidad los programas o software antivirus.
	5.	Desarrollar y mantenga sistemas y aplicaciones seguras.
Implementar medidas sólidas de control de acceso	6.	Restringa el acceso a los datos del titular de la tarjeta según la necesidad de saber que tenga la empresa.
	7.	Identifique y autentique el acceso los componentes de sistema.
	8.	Restringir el acceso físico a los datos del titular de la tarjeta.
Supervisar y evaluar las redes con regularidad	9.	Rastree y supervise todos los accesos a los recursos de la red y a los datos de los titulares de las tarjetas.
	10.	Pruebe con regularidad los sistemas y procesos de seguridad.
Mantener una política de seguridad de información	11.	Mantenga una política que aborde la seguridad de la información para todo el personal.

Estos requisitos aplican a todo el entorno que conforma los datos de los titulares de tarjeta de crédito, los mismos que incluyen dispositivos de red,

aplicaciones o sistemas de seguridad, componentes de virtualización, servidores.

En un entorno virtualizado se debe cumplir con todos los requisitos, de tal manera que los sistemas virtualizados efectivamente pueden ser considerados como hardware separado, dado que debe haber una segmentación clara de las funciones y la segregación de las redes con diferentes niveles de seguridad. La segmentación debe impedir que se comparta el ambiente de producción con los ambientes de desarrollo o de certificación. La configuración de la infraestructura virtual deberían asegurar de tal manera que las vulnerabilidades no puedan afectar a la seguridad de otras funciones; y los dispositivos conectados, como los dispositivos USB o seriales, no deben ser accesibles por todas las instancias virtuales.

Es requerido que todos los protocolos que administran las interfaces virtuales deben incluirse en la documentación del sistema. Además se deben definir los roles y permisos para la administración de redes virtuales y los componentes dentro de ambiente virtual.

Las plataformas de virtualización deben tener la capacidad de hacer cumplir la separación de funciones y privilegios, para separar la administración de red virtual de la de administración del servidor virtual.

Para finalizar, es necesario que esté definida la aplicación de controles de autenticación para asegurar que los usuarios que se autentican a los componentes de virtualización se distingan entre el invitado VM (máquinas virtuales) y el hypervisor.

2.2 COMPONENTES DENTRO DE UNA INFRAESTRUCTURA VIRTUAL

Es importante tener en cuenta que dentro de un entorno virtual el alcance la norma PCIDSS abarca los componentes de sistemas que estén dentro del entorno de los datos de los titulares de la tarjeta de crédito o pago. Para determinar si un componente virtual es considerado dentro del alcance eso dependerá de la tecnología utilizada, y en qué ambiente este implementado.

2.2.1 HYPERVISOR

El hypervisor es el software o firmware responsable del alojamiento y de la gestión de máquinas virtuales, además también puede incluir el monitor de máquina virtual (VMM) encargado de administrar la abstracción de hardware de la máquina virtual, y se puede considerar como la función que gestiona la plataforma del hypervisor. El VMM administra el procesador, la memoria y otros recursos del sistema, para asignar lo que requiere el sistema operativo de máquina virtual.

Si algún componente virtual está conectado o alojado en el hypervisor está dentro del alcance de PCI DSS.

2.2.2 MÁQUINA VIRTUAL

Una máquina virtual en un ambiente autónomo se comporta como un equipo independiente y se encuentra en la parte superior del hypervisor. Toda máquina virtual será parte del alcance de PCI DSS si se almacena, procesa y transmite datos de titulares de tarjetas, si se conecta o proporciona un punto de entrada en el CDE. Si una Máquina Virtual está por debajo del host y del hypervisor también estarán dentro del alcance de PCIDSS, ya que están conectados directamente y tienen un impacto fundamental en la funcionalidad y la seguridad de la máquina virtual.

2.2.3 VIRTUAL SWITCH O ROUTER.

Un virtual switch o router es un componente de software que proporciona enrutamiento de datos a nivel de red y la funcionalidad de conmutación, y es a menudo una parte integral de la plataforma de servidores virtualizados. Además los switch y routers virtuales pueden utilizarse para generar múltiples dispositivos de red lógica desde una sola plataforma física.

Las redes provisionados en un hypervisor basados en virtual switch son parte del alcance de PCI DSS, si proporcionan servicios o conexión a un componente y además a los dispositivos físicos que alojan a los virtual switches o routers.

2.3 VERIFICACIÓN DE CUMPLIMIENTO PCI DSS VERSIÓN 2.0 EN INFRAESTRUCTURA VIRTUAL CON VMWARE VSPHERE 5.5.

Para realizar la verificación de cumplimento de la norma en la infraestructura virtual se utilizará una herramienta gratuita basada en "VMware's vCenter Configuration Manager", llamada "VMware Compliance Checker for PCI". El resultado del informe nos detalla unas reglas las cuales indica si pasaron o no la norma. Para solucionar las que tuvieron inconformidades existe una base de conocimientos para obtener una explicación detallada de la norma violada y asesoramiento sobre la remediación que se debe aplicar.

2.3.1 INSTALACIÓN "VMWARE COMPLIANCE CHECKER FOR PCI".

El Procedimiento de instalación es muy sencillo. Primero debemos dirigirnos al portal de vwmare.com realizar el registro con un usuario, para luego proceder a descargar la herramienta siguiente enlace http://www.vmware.com/products/pci-compliance-checker/download.html.

Fuente: Portal de Vmware [2]

Figura 2.1 Portal de descarga Vmware Compliance Cheker for PCI

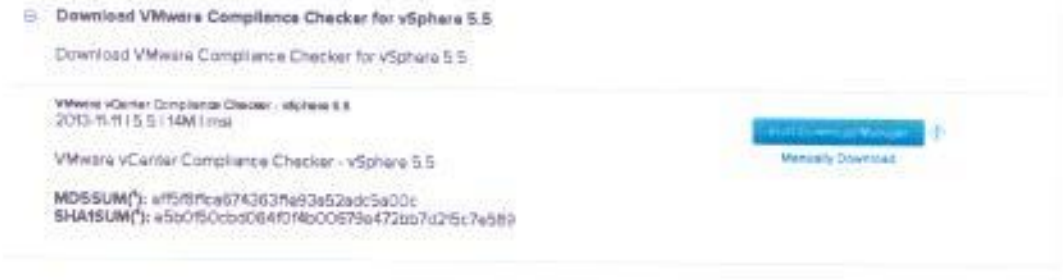


Figura 2.2 Área de descarga Vmware Complieance Checker for vSphere 5.5

Podemos citar algunos beneficios del uso de esta herramienta:

- El informe de producido por el verificador de Cumplimiento de PCI DSS se puede utilizar durante una auditoria para demostrar el cumplimiento de TI contra la norma.
- Ayudará a detectar los problemas afecten su postura de seguridad.
- Obtener una orientación detallada sobre la remediación de violaciones de cumplimiento y de asesoramiento detallado para la remediación de cada requerimiento.

Finalizada la descarga procederemos a realizar la instalación de la herramienta, siguiendo el Wizard del instalador.

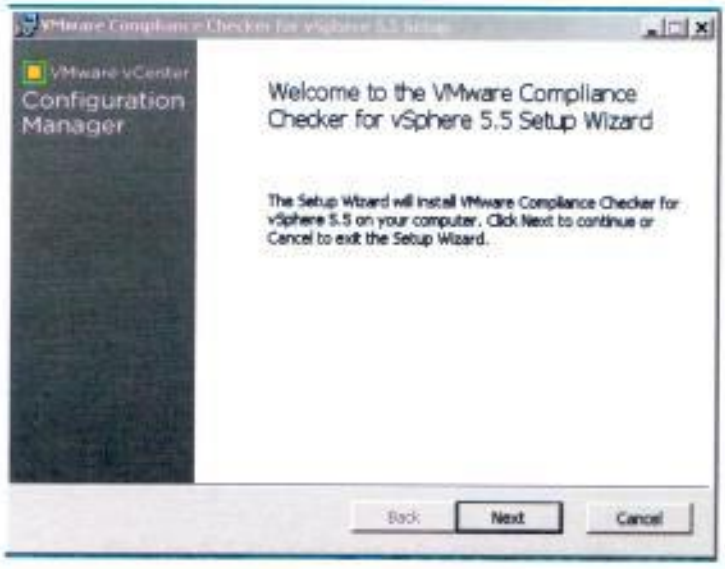


Figura 2.3 Pantalla del Wizard de Instalación

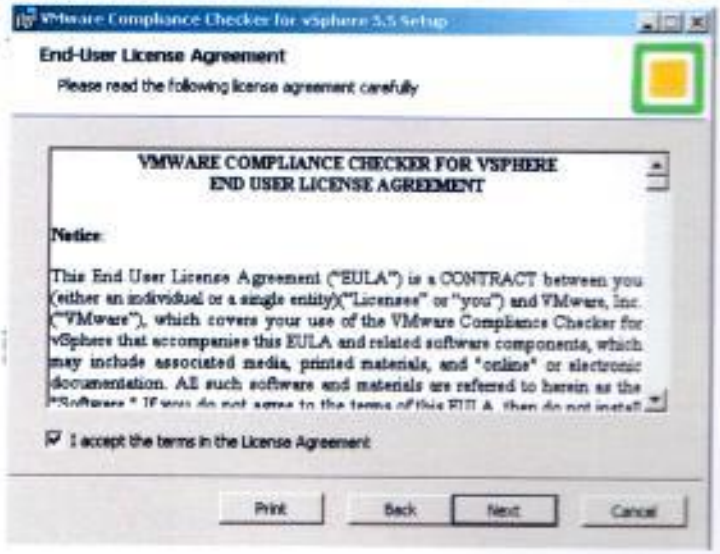


Figura 2.4 Pantalla de aceptación de Licencia

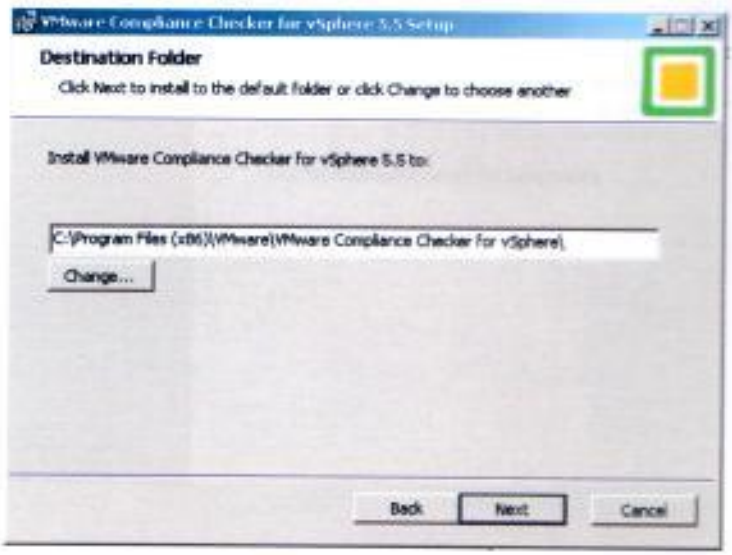


Figura 2.5 Pantalla de ruta de instalación

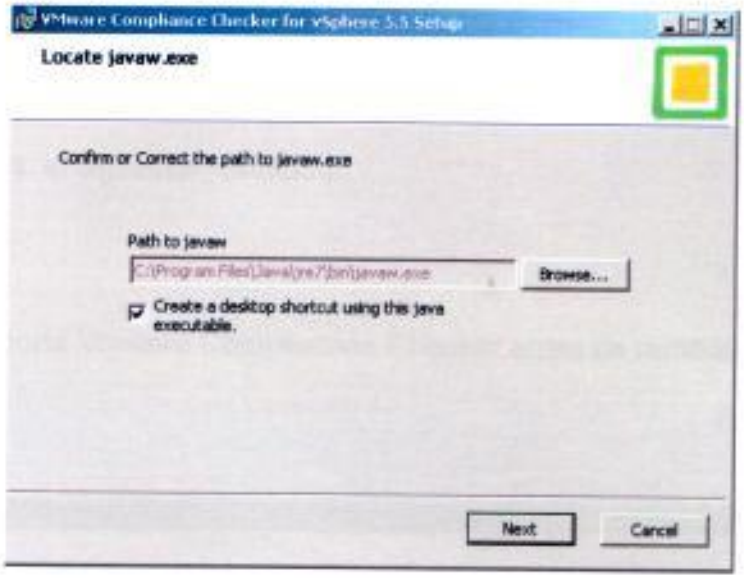


Figura 2.6 Pantalla de ruta del ejecutable de java

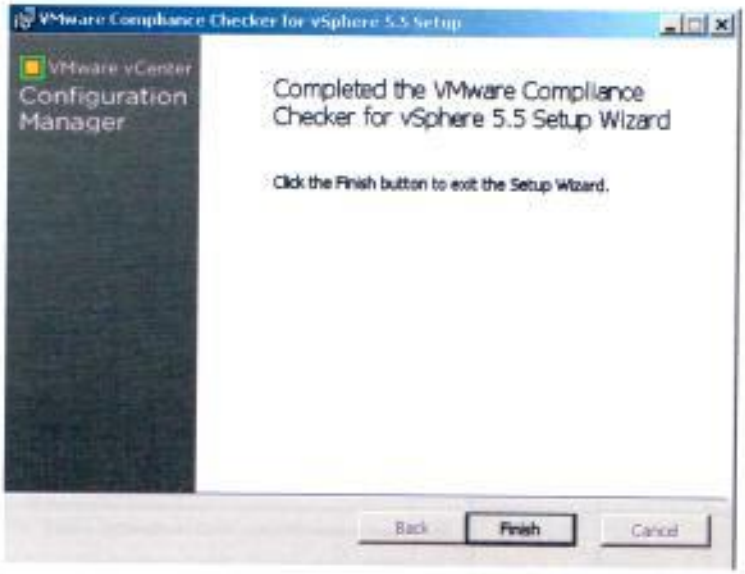


Figura 2.7 Pantalla de finalización de la instalación.

2.3.2 EJECUCIÓN DE VMWARE COMPLIANCE CHECKER FOR PCI.

Para verificar el cumplimento vamos a proceder a ejecutar la herramienta y obtendremos el siguiente resultado:

Tabla 2 Reporte Vmware Complieance Checker antes de remediación

Fuente: [2, 3]

Compliance Check Results

Compliance Rule	host1.ESXi 5.5.0	Host2. ESXi 5.5.0	host3.ESXi 5.5.0	host4.ESXi 5.5.0
DISABLE-ESXI-SHELL - Disable ESXi Shell unless needed for diagnostics or troubleshooting. ESXi Shell is an interactive command line environment available from the DCUI or remotely via SSH. Access to this mode requires the root password of the server. The ESXi Shell can be turned on and off for individual hosts. Activities performed from the ESXi Shell bypass vCenter RBAC and audit controls. The ESXi shell should only be turned on when needed to troubleshoot/resolve problems that cannot be fixed through the vSphere client or vCLI/PowerCLI.	✓	✓	✓	✓
DISABLE-SSH - Disable SSH. The ESXi Shell is an interactive command line environment available on the console of the ESXi server. The shell can be accessed directly from the host console through the DCUI or remotely using SSH. Remote access to the host should be limited to the vSphere Client, remote command-line tools (vCLI/PowerCLI), and through the published APIs. Under normal circumstances remote access to the host using SSH should be disabled.	✓	✓	✓	✓
ENABLE-LOCKDOWN-MODE - Enable lockdown mode to restrict root access. Enabling lockdown mode disables all remote access to ESXi 5.0 machines. Any subsequent local changes to the host must be made-Using the DCUI or in a vSphere Client session or using vCLI commands to vCenter Server.	✗	✗	✗	✗
DISABLE-DCUI - Disable DCUI to prevent all local administrative control. The DCUI allows for simple low-level configuration, such as ipaddress, hostname and root password, as well as diagnostic capabilities such as viewing log files, restarting agents, and resetting configurations. To restrict local administrative activity, it can be disabled.	✗	✗	✗	✗
CONFIG-NTP - Configure NTP time synchronization By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time?UTC), you can make it simpler to track and correlate an intruder's actions when reviewing the relevant log files.	✓	✓	✓	✓
ENABLE-CHAP-AUTH - Ensure bidirectional CHAP authentication is enabled for iSCSI traffic vSphere allows for the use of bidirectional authentication of both the iSCSI target and host. Choosing not to enforce more stringent authentication can make sense if you create a dedicated network or VLAN to service all your iSCSI devices. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation.	✗	✓	✓	✓
LABEL-PORTGROUPS - Ensure that port groups are configured with a clear network label A network label identifies each port group with a name. These names are important because they serve as a functional descriptor for the port group.	✓	✓	✓	✓

Without these descriptions, identifying port groups and their functions becomes difficult as the network becomes more complex.				
▼NO-UNUSED-DVPORTS - No Unused Ports on a Distributed Virtual Switch The number of ports available on a vdSwitch distributed port group can be adjusted to exactly match the number of virtual machine vNICs that need to be assigned to that dvPortgroup. Limiting the number of ports to just what is needed limits the potential for an administrator, either accidentally or maliciously, to move a virtual machine to an unauthorized network. This is especially relevant if the management network is on a dvPortgroup, because it could help prevent someone from putting a rogue virtual machine on this network.	✓	✓	✓	✓
▼REJECT-MAC-CHANGES - Ensure that the "MAC Address Change" policy is set to reject If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network. This will prevent VMs from changing their effective MAC address.	✗	✗	✗	✗
▼REJECT-FORGED-TRANSMIT - Ensure that the "Forged Transmits" policy is set to reject If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network. Forged transmissions should be set to accept by default. This means the virtual switch does not compare the source and effective MAC addresses. To protect against MAC address impersonation, all virtual switches should have forged transmissions set to reject.	✗	✗	✗	✗
▼REJECT-PROMISCUOUS-MODE - Ensure that the "Promiscuous Mode" policy is set to reject When promiscuous mode is enabled for a virtual switch all virtual machines connected to the dvPortgroup have the potential of reading all packets across that network, meaning only the virtual machines connected to that dvPort group. Promiscuous mode is disabled by default on the ESX Server, and this is the recommended setting. However, there might be a legitimate reason to enable it for debugging, monitoring or troubleshooting reasons.	✓	✓	✓	✓
▼NO-VGT-VLAN-4095 - Ensure that port groups are not configured to VLAN 4095 When a port group is set to VLAN 4095, this activates VGT mode. In this mode, the vSwitch passes all network frames to the guest VM without modifying the VLAN tags, leaving it up to the guest to deal with them. VLAN 4095 should be used only if the guest has been specifically configured to manage VLAN tags itself.	✗	✗	✗	✗
▼LABEL-VSWITCHES - Ensure that all vSwitches have a clear network label Virtual switches within the ESXi Server require a field for the name of the switch. This label is important because it serves as a functional descriptor for the switch, just as physical switches require a host name. Labeling virtual switches will indicate the function or the IP subnet of the virtual switch.	✓	✓	✓	✓
▼CONTROL-RESOURCE-USAGE - Prevent virtual machines from taking over resources By default, all virtual machines on an ESXi host share the resources equally. By using the resource management capabilities of ESXi, such as shares and limits, you can control the server resources that a virtual machine consumes. You can use this mechanism to prevent a denial of service that causes one virtual machine to consume so much of the host's resources that other virtual machines on the same host cannot perform their intended functions.	✓ 100%	✗ 87%	✗ 60%	✗ 66%
▼DISABLE-DISK-SHRINKING-SHRINK - Prevent virtual disk shrinking Shrinking a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to invoke this procedure. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature.	✗ 87%	✗ 65%	✗ 10%	✗ 66%
▼DISABLE-DISK-SHRINKING-WIPER - Prevent virtual disk shrinking Shrinking a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to invoke this procedure. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature.	✗ 87%	✗ 65%	✗ 10%	✗ 66%

LIMIT-CONSOLE-CONNECTIONS-ONE - Prevent other users from spying on administrator remote consoles By default, remote console sessions can be connected to by more than one user at a time. When multiple sessions are activated, each terminal window gets a notification about the new session.	✗ 12%	✗ 4%	✗ 0%	✗ 0%
DISCONNECT-DEVICES-FLOPPY - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	✗ 96%	✗ 95%	✗ 90%	✓ 100%
DISCONNECT-DEVICES-USB - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	✓ 100%	✗ 92%	✗ 90%	✓ 100%
DISCONNECT-DEVICES-IDE - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	✗ 3%	✗ 4%	✗ 0%	✗ 33%
DISCONNECT-DEVICES-SERIAL - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
DISCONNECT-DEVICES-PARALLEL - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
PREVENT-DEVICE-INTERACTION-CONNECT - Prevent unauthorized removal, connection and modification of devices Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, as well as the ability to modify device settings. In general, you should use the virtual machine settings editor or configuration editor to remove any unneeded or unused hardware devices. However, you might want to use the device again, so removing it is not always a good solution. In that case, you can prevent a user or running process in the virtual machine from connecting or disconnecting a device from within the guest operating system, as well as modifying devices.	✗ 87%	✗ 85%	✗ 10%	✗ 66%
PREVENT-DEVICE-INTERACTION-EDIT - Prevent unauthorized removal, connection and modification of devices Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, as well as the ability to modify device settings. In general, you should use the virtual machine settings editor or configuration editor to remove any unneeded or unused hardware devices. However, you might want to use the device again, so removing it is not always a good solution. In that case, you can prevent a user or running process in the virtual machine from connecting or disconnecting a device from within the guest operating system, as well as modifying devices.	✗ 87%	✗ 85%	✗ 10%	✗ 66%
DISABLE-INTERVM-VMCI - Disable virtual machine-to-virtual machine communication through VMCI	✓ 100%	✓ 100%	✓ 100%	✓ 100%

If the interface is not restricted, a virtual machine can detect and be detected by all others with the same option enabled within the same host. This might be the intention, but custom-built software can have unexpected vulnerabilities that might potentially lead to an exploit. Additionally, it is possible for a virtual machine to detect how many others are within the same ESX system by simply registering the virtual machine. This information might also be used for a potentially malicious objective.				
▼DISABLE-CONSOLE-COPY - Explicitly disable copy operations Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct.	✖ 0%	✖ 0%	✖ 0%	✖ 0%
▼DISABLE-CONSOLE-PASTE - Explicitly disable paste operations Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct.	✖ 0%	✖ 0%	✖ 0%	✖ 0%
▼LIMIT-SETINFO-SIZE - Limit informational messages from the virtual machine to the VMX file The configuration file containing these name-value pairs is limited to a size of 1MB. This 1MB capacity should be sufficient for most cases, but you can change this value if necessary. You might increase this value if large amounts of custom information are being stored in the configuration file. The default limit is 1MB; this limit is applied even when the sizeLimit parameter is not listed in the .vmx file.	✖ 12%	✖ 4%	✖ 0%	✖ 0%
▼DISABLE-INDEPENDENT-NONPERSISTENT - Avoid using independent nonpersistent disks The security issue with nonpersistent disk mode is that successful attackers, with a simple shutdown or reboot, might undo or remove any traces that they were ever on the machine. To safeguard against this risk, you should set production virtual machines to use either persistent disk mode or nonpersistent disk mode; additionally, make sure that activity within the virtual machine is logged remotely on a separate server, such as a syslog server or equivalent Windows based event collector.	✔ 100%	✔ 100%	✔ 100%	✔ 100%
▼DISABLE-UNEXPOSED-FEATURES-AUTOLOGON - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	✖ 83%	✖ 83%	✖ 10%	✖ 66%
▼DISABLE-UNEXPOSED-FEATURES-BIOSBBS - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	✖ 83%	✖ 83%	✖ 10%	✖ 66%
▼DISABLE-UNEXPOSED-FEATURES-GETCREDS - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	✖ 87%	✖ 85%	✖ 10%	✖ 66%
▼DISABLE-UNEXPOSED-FEATURES-LAUNCHMENU - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	✖ 87%	✖ 85%	✖ 10%	✖ 66%
▼DISABLE-UNEXPOSED-FEATURES-MEMSFSS - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	✖ 87%	✖ 83%	✖ 10%	✖ 66%
▼DISABLE-UNEXPOSED-FEATURES-UNITYPUSH - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	✖ 87%	✖ 85%	✖ 10%	✖ 66%

RESTRICT-HOST-INFO - Do not send host performance information to guests If enabled, a virtual machine can obtain detailed information about the physical host. The default value for the parameter is FALSE. This setting should not be TRUE unless a particular virtual machine requires this information for performance monitoring.	100%	100%	100%	100%
VERIFY-VMSAFE-CPUMEM-AGENTADDRESS - Control access to virtual machines through VMsafe CPU/memory APIs A virtual machine must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to enable the API, one to set the IP address used by the security virtual appliance on the introspection vSwitch, and one to set the port number for that IP address. This should be done only for virtual machines for which you want this to be done.	100%	100%	100%	100%
VERIFY-VMSAFE-CPUMEM-AGENTPORT - Control access to virtual machines through VMsafe CPU/memory APIs A virtual machine must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to enable the API, one to set the IP address used by the security virtual appliance on the introspection vSwitch, and one to set the port number for that IP address. This should be done only for virtual machines for which you want this to be done.	100%	100%	100%	100%
VERIFY-VMSAFE-CPUMEM-ENABLE - Control access to VMs through VMsafe CPU/memory APIs. A virtual machine must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to enable the API, one to set the IP address used by the security virtual appliance on the introspection vSwitch, and one to set the port number for that IP address. This should be done only for virtual machines for which you want this to be done.	100%	100%	100%	100%
VERIFY-NETWORK-FILTER - Control access to VMs through VMsafe CPU/memory APIs. A VM must be configured explicitly to accept access by the dvfilter network API. This should be done only for VMs for which you want this to be done. An attacker might compromise the VM by making use of this introspection channel.	100%	100%	100%	100%

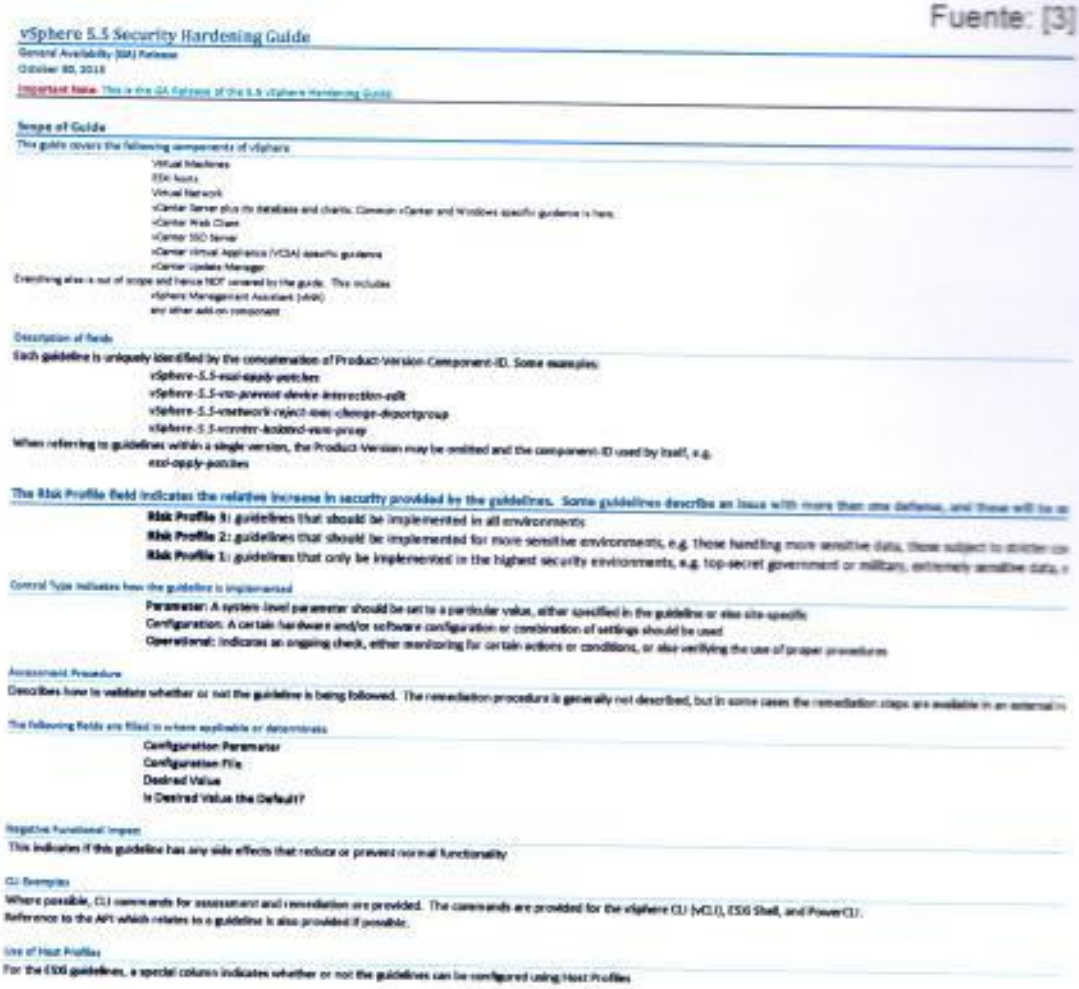
El resultado de la ejecución de la herramienta nos muestra algunos incumplimientos en las configuraciones a nivel de host y máquinas virtuales de la infraestructura

2.4 REMEDIACIÓN DE INCUMPLIMIENTOS.

En base al reporte de Vmware complience Checker podemos observar las reglas que se están incumpliendo dentro de la configuración de los hosts y máquinas virtuales en una infraestructura implementada con Vmware Vsphere 5.5. Para poder remediar utilizaremos un documento guía proporcionado por

Vmware llamado "hardeningguide-vsphere5-5-ga-released.xls[8]". Con este documento se realizaran las respectivas correcciones en las configuraciones de las máquinas virtuales y hosts.

Fuente: [3]



vSphere 5.5 Security Hardening Guide

General Availability (GA) Release

October 30, 2013

Important Note: This is the GA Release of the 5.5 vSphere Hardening Guide

Scope of Guide

This guide covers the following components of vSphere:

- Virtual Machines
- ESXi hosts
- Virtual Network
- vCenter Server plus its database and clients. Common vCenter and Windows specific guidance is here.
- vCenter Web Client
- vCenter SSO Server
- vCenter Virtual Appliance (VCSA) specific guidance
- vCenter Update Manager

Everything else is out of scope and hence NOT covered by the guide. This includes:

- vSphere Management Assistant (vMA)
- any other add-on component

Description of fields

Each guideline is uniquely identified by the concatenation of Product-Version-Component-ID. Some examples:

- vSphere-5.5-esxi-apply-patches
- vSphere-5.5-vm-prevent-device-interaction-split
- vSphere-5.5-vnetwork-reject-non-change-dvportgroup
- vSphere-5.5-vcenter-isolated-vum-proxy

When referring to guidelines within a single version, the Product-Version may be omitted and the component-ID used by itself, e.g.

- esxi-apply-patches

The Risk Profile field indicates the relative increase in security provided by the guidelines. Some guidelines describe an issue with more than one defense, and these will be at

- **Risk Profile 3:** guidelines that should be implemented in all environments
- **Risk Profile 2:** guidelines that should be implemented for more sensitive environments, e.g. those handling more sensitive data, those subject to stricter co
- **Risk Profile 1:** guidelines that only be implemented in the highest security environments, e.g. top-secret government or military, extremely sensitive data, e

Control Type indicates how the guideline is implemented

- **Parameter:** A system-level parameter should be set to a particular value, either specified in the guideline or else site-specific
- **Configuration:** A certain hardware and/or software configuration or combination of settings should be used
- **Operational:** Indicates an ongoing check, either monitoring for certain actions or conditions, or else verifying the use of proper procedures

Assessment Procedure

Describes how to validate whether or not the guideline is being followed. The remediation procedure is generally not described, but in some cases the remediation steps are available in an external re

The following fields are filled in where applicable or determinable:

- **Configuration Parameter**
- **Configuration File**
- **Desired Value**
- **Is Desired Value the Default?**

Negative Functional Impact

This indicates if this guideline has any side effects that reduce or prevent normal functionality

CLI Examples

Where possible, CLI commands for assessment and remediation are provided. The commands are provided for the vSphere CLI (vCLI), ESXi Shell, and PowerCLI.
Reference to the API which relates to a guideline is also provided if possible.

Use of Host Profiles

For the ESXi guidelines, a special column indicates whether or not the guidelines can be configured using Host Profiles

Figura 2.8 vSphere 5.5 Security Hardening Guide

[8] https://www.vmware.com/security/hardening-guides

La remediación se debe realizar con la ayuda de la herramienta "VMware Infrastructure Client" conectada al Virtual Center. Para todos los casos es necesario apagar las máquinas virtuales y se realiza los cambios en la configuración.

CAPÍTULO 3

ANÁLISIS DE RESULTADOS.

3.1 REVISIÓN DE RESULTADOS

Luego de la realizar la remediación en el virtual center y la ejecución de "Vmware Compliance Checker For PCI" se obtuvo como resultado el cumplimiento de cada una de las reglas para tener un entorno con vmware certificado para PCIDSS. En la siguiente tabla se muestra los resultados:

Tabla 3 Reporte Vmware Complieance Checker después de remediación.

Fuente: [2]

Compliance Check Results

Compliance Rule	host1.ESXi 5.5.0	Host2. ESXi 5.5.0	host3.ESXi 6.5.0	host4.ESXi 5.5.0
▼DISABLE-ESXI-SHELL - Disable ESXi Shell unless needed for diagnostics or troubleshooting. ESXi Shell is an interactive command line environment available from the DCUI or remotely via SSH. Access to this mode requires the root password of the server. The ESXi Shell can be turned on and off for individual hosts. Activities performed from the ESXi Shell bypass vCenter RBAC and audit controls. The ESXi shell should only be turned on when needed to troubleshoot/resolve problems that cannot be fixed through the vSphere client or vCLI/PowerCLI.	✓	✓	✓	✓
▼DISABLE-SSH - Disable SSH. The ESXi Shell is an interactive command line environment available on the console of the ESXi server. The shell can be accessed directly from the host console through the DCUI or remotely using SSH. Remote access to the host should be limited to the vSphere Client, remote command-line tools (vCLI/PowerCLI), and through the published APIs. Under normal circumstances remote access to the host using SSH should be disabled.	✓	✓	✓	✓
▼ENABLE-LOCKDOWN-MODE - Enable lockdown mode to restrict root access. Enabling lockdown mode disables all remote access to ESXi 5.0 machines. Any subsequent local changes to the host must be made Using the DCUI or in a vSphere Client session or using vCLI commands to vCenter Server.	✓	✓	✓	✓

Compliance Rule	host1.ESXi 6.5.0	Host2. ESXi 6.5.0	host3.ESXi 6.5.0	host4.ESXi 6.5.0
▼DISABLE-DCUI - Disable DCUI to prevent all local administrative control. The DCUI allows for simple low-level configuration, such as ipaddress, hostname and root password, as well as diagnostic capabilities such as viewing log files, restarting agents, and resetting configurations. To restrict local administrative activity, it can be disabled.	✓	✓	✓	✓
▼CONFIG-NTP - Configure NTP time synchronization By ensuring that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time?UTC), you can make it simpler to track and correlate an intruder's actions when reviewing the relevant log files.	✓	✓	✓	✓
▼ENABLE-CHAP-AUTH - Ensure bidirectional CHAP authentication is enabled for iSCSI traffic vSphere allows for the use of bidirectional authentication of both the iSCSI target and host. Choosing not to enforce more stringent authentication can make sense if you create a dedicated network or VLAN to service all your iSCSI devices. If the iSCSI facility is isolated from general network traffic, it is less vulnerable to exploitation.	✓	✓	✓	✓
▼LABEL-PORTGROUPS - Ensure that port groups are configured with a clear network label A network label identifies each port group with a name. These names are important because they serve as a functional descriptor for the port group. Without these descriptions, identifying port groups and their functions becomes difficult as the network becomes more complex.	✓	✓	✓	✓
▼NO-UNUSED-DVPORTS - No Unused Ports on a Distributed Virtual Switch The number of ports available on a vdSwitch distributed port group can be adjusted to exactly match the number of virtual machine vNICs that need to be assigned to that dvPortgroup. Limiting the number of ports to just what is needed limits the potential for an administrator, either accidentally or maliciously, to move a virtual machine to an unauthorized network. This is especially relevant if the management network is on a dvPortgroup, because it could help prevent someone from putting a rogue virtual machine on this network.	✓	✓	✓	✓
▼REJECT-MAC-CHANGES - Ensure that the "MAC Address Change" policy is set to reject If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network. This will prevent VMs from changing their effective MAC address.	✓	✓	✓	✓
▼REJECT-FORGED-TRANSMIT - Ensure that the "Forged Transmits" policy is set to reject If the virtual machine operating system changes the MAC address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network. Forged transmissions should be set to accept by default. This means the virtual switch does not compare the source and effective MAC addresses. To protect against MAC address impersonation, all virtual switches should have forged transmissions set to reject.	✓	✓	✓	✓
▼REJECT-PROMISCUOUS-MODE - Ensure that the "Promiscuous Mode" policy is set to reject When promiscuous mode is enabled for a virtual switch all virtual machines connected to the dvPortgroup have the potential of reading all packets across that network, meaning only the virtual machines connected to that dvPort group. Promiscuous mode is disabled by default on the ESX Server, and this is the recommended setting. However, there might be a legitimate reason to enable it for debugging, monitoring or troubleshooting reasons.	✓	✓	✓	✓
▼NO-VGT-VLAN-4095 - Ensure that port groups are not configured to VLAN 4095 When a port group is set to VLAN 4095, this activates VGT mode. In this mode, the vSwitch passes all network frames to the guest VM without modifying the VLAN tags, leaving it up to the guest to deal	✓	✓	✓	✓

Compliance Rule	host1.ESXi 5.5.0	Host2. ESXi 5.5.0	host3.ESXi 5.5.0	host4.ESXi 5.5.0
with them. VLAN 4095 should be used only if the guest has been specifically configured to manage VLAN tags itself.				
▼LABEL-VSWITCHES - Ensure that all vSwitches have a clear network label Virtual switches within the ESXi Server require a field for the name of the switch. This label is important because it serves as a functional descriptor for the switch, just as physical switches require a host name. Labeling virtual switches will indicate the function or the IP subnet of the virtual switch.	✓	✓	✓	✓
▼CONTROL-RESOURCE-USAGE - Prevent virtual machines from taking over resources By default, all virtual machines on an ESXi host share the resources equally. By using the resource management capabilities of ESXi, such as shares and limits, you can control the server resources that a virtual machine consumes. You can use this mechanism to prevent a denial of service that causes one virtual machine to consume so much of the host's resources that other virtual machines on the same host cannot perform their intended functions.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
▼DISABLE-DISK-SHRINKING-SHRINK - Prevent virtual disk shrinking Shrinking a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to invoke this procedure. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
▼DISABLE-DISK-SHRINKING-WIPER - Prevent virtual disk shrinking Shrinking a virtual disk reclaims unused space in it. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive. Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to invoke this procedure. However, if this is done repeatedly, the virtual disk can become unavailable while this shrinking is being performed, effectively causing a denial of service. In most datacenter environments, disk shrinking is not done, so you should disable this feature.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
▼LIMIT-CONSOLE-CONNECTIONS-ONE - Prevent other users from spying on administrator remote consoles By default, remote console sessions can be connected to by more than one user at a time. When multiple sessions are activated, each terminal window gets a notification about the new session.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
▼DISCONNECT-DEVICES-FLOPPY - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
▼DISCONNECT-DEVICES-USB - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	✓ 100%	✓ 100%	✓ 100%	✓ 100%
▼DISCONNECT-DEVICES-IDE - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used	✓ 100%	✓ 100%	✓ 100%	✓ 100%

Compliance Rule	host1.ESXI 5.5.0	Host2. ESXI 5.5.0	host3.ESXI 5.5.0	host4.ESXI 5.5.0
devices that are not required, either the parameter should not be present or its value must be FALSE.				
▼DISCONNECT-DEVICES-SERIAL - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	100%	100%	100%	100%
▼DISCONNECT-DEVICES-PARALLEL - Ensure that unauthorized devices are not connected Besides disabling unnecessary virtual devices from within the virtual machine, you should ensure that no device is connected to a virtual machine if it is not required to be there. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. For less commonly used devices that are not required, either the parameter should not be present or its value must be FALSE.	100%	100%	100%	100%
▼PREVENT-DEVICE-INTERACTION-CONNECT - Prevent unauthorized removal, connection and modification of devices Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, as well as the ability to modify device settings. In general, you should use the virtual machine settings editor or configuration editor to remove any unneeded or unused hardware devices. However, you might want to use the device again, so removing it is not always a good solution. In that case, you can prevent a user or running process in the virtual machine from connecting or disconnecting a device from within the guest operating system, as well as modifying devices.	100%	100%	100%	100%
▼PREVENT-DEVICE-INTERACTION-EDIT - Prevent unauthorized removal, connection and modification of devices Normal users and processes that is, users and processes without root or administrator privileges within virtual machines have the capability to connect or disconnect devices, such as network adaptors and CD-ROM drives, as well as the ability to modify device settings. In general, you should use the virtual machine settings editor or configuration editor to remove any unneeded or unused hardware devices. However, you might want to use the device again, so removing it is not always a good solution. In that case, you can prevent a user or running process in the virtual machine from connecting or disconnecting a device from within the guest operating system, as well as modifying devices.	100%	100%	100%	100%
▼DISABLE-INTERVM-VMCI - Disable virtual machine-to-virtual machine communication through VMCI If the interface is not restricted, a virtual machine can detect and be detected by all others with the same option enabled within the same host. This might be the intention, but custom-built software can have unexpected vulnerabilities that might potentially lead to an exploit. Additionally, it is possible for a virtual machine to detect how many others are within the same ESX system by simply registering the virtual machine. This information might also be used for a potentially malicious objective.	100%	100%	100%	100%
▼DISABLE-CONSOLE-COPY - Explicitly disable copy operations Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct.	100%	100%	100%	100%
▼DISABLE-CONSOLE-PASTE - Explicitly disable paste operations Copy and paste operations are disabled by default however by explicitly disabling this feature it will enable audit controls to check that this setting is correct.	100%	100%	100%	100%
▼LIMIT-SETINFO-SIZE - Limit informational messages from the virtual machine to the VMX file The configuration file containing these name-value pairs is limited to a size of 1MB. This 1MB capacity should be sufficient for most cases, but you can change this value if necessary. You might increase this value if large amounts of custom information are being stored in the	100%	100%	100%	100%

Compliance Rule	host1.ESXi 5.5.0	Host2. ESXi 5.5.0	host3.ESXi 5.5.0	host4.ESXi 5.5.0
configuration file. The default limit is 1MB; this limit is applied even when the sizeLimit parameter is not listed in the .vmx file.				
▼DISABLE-INDEPENDENT-NONPERSISTENT - Avoid using independent nonpersistent disks The security issue with nonpersistent disk mode is that successful attackers, with a simple shutdown or reboot, might undo or remove any traces that they were ever on the machine. To safeguard against this risk, you should set production virtual machines to use either persistent disk mode or nonpersistent disk mode; additionally, make sure that activity within the virtual machine is logged remotely on a separate server, such as a syslog server or equivalent Windows based event collector.	100%	100%	100%	100%
▼DISABLE-UNEXPOSED-FEATURES-AUTOLOGON - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	100%	100%	100%	100%
▼DISABLE-UNEXPOSED-FEATURES-BIOSBBS - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	100%	100%	100%	100%
▼DISABLE-UNEXPOSED-FEATURES-GETCREDS - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	100%	100%	100%	100%
▼DISABLE-UNEXPOSED-FEATURES-LAUNCHMENU - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	100%	100%	100%	100%
▼DISABLE-UNEXPOSED-FEATURES-MEMSFSS - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	100%	100%	100%	100%
▼DISABLE-UNEXPOSED-FEATURES-UNITYPUSH - Disable certain unexposed features Because VMware virtual machines are designed to work on both vSphere as well as hosted virtualization platforms such as Workstation and Fusion, there are some VMX parameters that don't apply when running on vSphere. Although the functionality governed by these parameters is not exposed on ESX, explicitly disabling them will reduce the potential for vulnerabilities.	100%	100%	100%	100%
▼RESTRICT-HOST-INFO - Do not send host performance information to guests If enabled, a virtual machine can obtain detailed information about the physical host. The default value for the parameter is FALSE. This setting should not be TRUE unless a particular virtual machine requires this information for performance monitoring.	100%	100%	100%	100%
▼VERIFY-VMSAFE-CPUMEM-AGENTADDRESS - Control access to virtual machines through VMsafe CPU/memory APIs A virtual machine must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to	100%	100%	100%	100%

Compliance Rule	host1.ESXi 5.5.0	Host2. ESXi 5.5.0	host3.ESXi 5.5.0	host4.ESXi 5.5.0
enable the API, one to set the IP address used by the security virtual appliance on the introspection vSwitch, and one to set the port number for that IP address. This should be done only for virtual machines for which you want this to be done.				
▼VERIFY-VMSAFE-CPUMEM-AGENTPORT - Control access to virtual machines through VMsafe CPU/memory APIs A virtual machine must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to enable the API, one to set the IP address used by the security virtual appliance on the introspection vSwitch, and one to set the port number for that IP address. This should be done only for virtual machines for which you want this to be done.	100%	100%	100%	100%
▼VERIFY-VMSAFE-CPUMEM-ENABLE - Control access to VMs through VMsafe CPU/memory APIs. A virtual machine must be configured explicitly to accept access by the VMsafe CPU/memory API. This involves three parameters: one to enable the API, one to set the IP address used by the security virtual appliance on the introspection vSwitch, and one to set the port number for that IP address. This should be done only for virtual machines for which you want this to be done.	100%	100%	100%	100%
▼VERIFY-NETWORK-FILTER - Control access to VMs through VMsafe CPU/memory APIs. A VM must be configured explicitly to accept access by the dvfilter network API. This should be done only for VMs for which you want this to be done. An attacker might compromise the VM by making use of this introspection channel.	100%	100%	100%	100%

3.2 ASEGURAMIENTO DE OTROS COMPONENTES.

Dentro de una infraestructura virtual existen también otros componentes que entran en el alcance los cuales deben estar dentro de la política de seguridad donde se establecerán, los roles y permisos necesarios para tener acceso a la ambiente virtual.

Es importante que los otros componentes se les realicen el aseguramiento basado en las buenas prácticas recomendadas por el fabricante, ya sea a nivel de sistema operativo del Host y Guest, red, almacenamiento y aplicación.

La seguridad de toda la infraestructura recae sobre la seguridad del sistema de gestión de la virtualización, que controla al hypervisor y permite al operador la creación de SO guests, iniciarlas y realizar otras acciones. Las seguridades del ambiente virtual son vulneradas cuando una política de seguridad no es bien gestionada o no tiene las debidas configuraciones que garanticen el ambiente. En la virtualización existen dos áreas que comúnmente son fundamentalmente de ataque al hypervisor y de intercomunicación entre máquinas virtuales.

El tipo de ataque que es al sistema operativo host del hypervisor, se basan principalmente en explotar las vulnerabilidades del sistema operativo del host donde el hypervisor se está ejecutando.

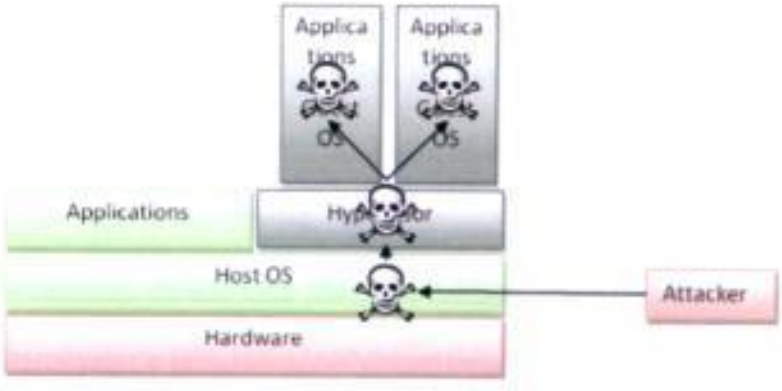


Figura 3.1 Ataques al hypervisor SO Host.

Otro ataque se basa en el uso de un sistema operativo invitado para obtener acceso no autorizado a las máquinas virtuales o el hypervisor.

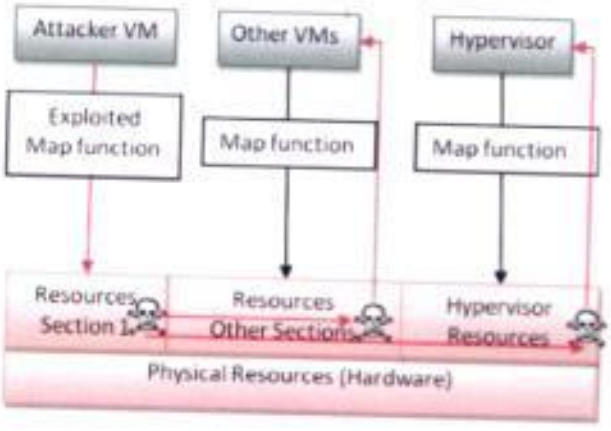


Figura 3.2 Ataques al hypervisor con SO invitado.

También podemos mencionar otros tipos de ataques al hypervisor como:

- Hyperjacking: Toma el control del hypervisor y el atacante podría tomar control sobre cualquier Máquina Virtual de ambiente.
- VM Scape: desde una MV se inicia el ataque hasta llegar al hypervisor y tomar control del mismo.
- VM Hopping: desde una Máquina Virtual inicia el ataque para llegar a comprometer a otra Máquina Virtual desde a dentro del mismo hardware físico.

Otra forma de ataque que se mencionó es la que gira en torno a la intercomunicación que tienen las Máquinas Virtuales en la infraestructura virtual, ya que podría generarse ataques al momento de su creación, asignación de recursos de conexión o incluso al momento de realizase una tarea de migración.

CONCLUSIONES Y RECOMENDACIONES

1. En base a la metodología que se utilizó para verificar el cumplimento de la norma PCIDSS en un ambiente virtualizado con vmware vsphere 5.5, se puede indicar que la implementación de un entorno virtualizado debe cumplir con el objetivo de todos los requisitos, de tal modo que los ambientes virtualizados se puedan trabajar efectivamente como una unidad de hardware independiente, ya que debe existir una clara segmentación de funciones y segregación de redes con diferentes niveles de seguridad. Además la segmentación debe impedir que se comparta los entornos de producción, test y desarrollo.

2. Para las configuraciones en ambientes virtualizados debe existir un procedimiento para asegurar que las vulnerabilidades no puedan afectar a la seguridad de otras funciones, y que otros dispositivos conectados, tales como dispositivos USB, CDROM, no deberían ser accesibles por todas las instancias virtuales.

3. Para finalizar las plataformas de virtualización deben ser capaces de poder realizar la separación de la administración de la red virtual y de la administración del servidor virtual a través de roles y privilegios, donde se implementarán controles de autenticación, para asegurarnos que los usuarios se autentiquen ante los componentes virtuales apropiados del sistema y para distinguir entre las máquinas virtuales, huésped y el hypervisor.

Basados en las requisitos de PCI DSS éstas son las recomendaciones y mejores prácticas que pueden ayudar a los ambientes virtualizados con cumplimiento de la norma.

1. Realizar una evaluación de los riesgos asociados a las tecnologías virtuales, ya que las entidades deben realizar una evaluación cuidadosa de los riesgos asociados con la virtualización de los componentes del sistema antes de seleccionar o implementar una solución de virtualización. Debido a que el flujo y el almacenamiento de datos de los tarjetahabientes deben documentar con precisión como parte de este proceso de evaluación de riesgos para garantizar que todas las áreas de riesgo son identificados y adecuadamente mitigados. Los Entornos

virtualizados y componentes del sistema deben estar incluido en un proceso anual de evaluación de riesgos.

2. Es muy importante comprender el impacto de la virtualización dentro del entorno de los datos de los titulares de crédito el CDE, ya que las entidades que utilizan la virtualización para consolidar su infraestructura en una o más plataformas de hardware físico puede encontrar como resultado, un complejo conjunto de configuraciones de sistemas virtuales que sería difícil identificar los límites o alcance de su CDE.

El entorno virtual debe ser evaluado utilizando la orientación proporcionada por PCI DSS. Si cualquiera de los componentes que se ejecutan en un único hypervisor están en su alcance, se recomienda que todos los componentes del hypervisor sean también considerados, incluyendo pero no limitado a las máquinas virtuales, dispositivos virtuales y hipervisor plug-ins. Dicho esto para el cumplimiento de los requisitos de seguridad de PCI DSS no sólo se proporcionará un punto de referencia seguro para el entorno virtual, sino que también reducirá la complejidad y el riesgo asociado a la gestión de múltiples perfiles de seguridad, y reducir la sobrecarga y el esfuerzo requeridos para mantener y validar el cumplimiento de los componentes.

5. Las funciones de seguridad proporcionadas por las máquinas virtuales deben ser ejecutadas con la misma separación como lo es en el ambiente físico. Se recomienda que esto sea más estricta en los sistemas virtualizados, ya que complica considerablemente los esfuerzos necesarios por un atacante para comprometer varios componentes del sistema dentro del entorno de los datos de los titulares de tarjeta de crédito CDE.

6. Se recomienda que exista una política de asignación de privilegios mínimos y de separación de funciones para el acceso administrativo al hypervisor para ser controlados cuidadosamente, y en función del nivel de riesgo, el uso de controles de acceso hipervisor más restrictivas y de ser necesario que sea justificado el uso. Las entidades deben *considerar métodos adicionales para asegurar el acceso administrativo,* tales como la implementación de la autenticación o del establecimiento de controles a las contraseñas administrativas entre varios administradores. Los controles de acceso se deben evaluar tanto para el acceso local y remoto al sistema hypervisor para su gestión. Para asegurar que los controles sean los adecuados se recomienda utilizar el acceso basado en roles (RBAC).

7. Es fundamental que el hypervisor y todas las máquinas virtuales, individuales están instalados y configurados de forma segura de acuerdo con las mejores prácticas de la industria y apoyado con las directrices de seguridad.

Estas recomendaciones pueden no ser todos aplicables para cada tipo de máquina virtual o componente ya que deben ser evaluados individualmente antes de ser implementadas:

a. Deshabilitar o quitar todas las interfaces innecesarias, puertos, dispositivos y servicios.
b. Asegurar configurar todas las interfaces de red virtuales y áreas de almacenamiento.
c. Establecer límites en el uso de recursos VM.
d. Asegurar que todos los sistemas operativos y las aplicaciones que se ejecutan dentro de la máquina virtual también sean asegurados.
e. Realizar aseguramiento individual a cada Máquina Virtual y contenedores.

8. Se debe usar una apropiada herramienta de administración que permitirá a los administradores realizar las funciones como copia de seguridad, restaurar la conectividad, migración y los cambios de configuración de los sistemas virtuales. Estas herramientas de administración de los componentes son consideradas en alcance de PCI DSS, ya que estas herramientas afectan directamente a la seguridad y el funcionamiento de los componentes. El acceso a las herramientas de administración debe limitarse a aquellos usuarios que tengan una necesidad relacionada con el trabajo. Se recomienda la segregación de funciones y responsabilidades para las funciones de la herramienta de administración y el uso de la misma debe ser monitoreado y registrado.

9. Hay que realizar una evaluación de la seguridad de las redes virtualizadas, ya que cada dispositivo virtualizado debe mantener configuraciones de acceso controlado individuales e independientes. Además, para infraestructuras virtuales deben ser granular y suficientemente detallada para identificar el acceso individual a las actividades realizadas en cada componente virtual específico. Los controles de acceso deben cumplir privilegios mínimos, tanto de forma individual para cada dispositivo y en toda la plataforma.

Fuente de consulta: [3]

BIBLIOGRAFÍA

[1]. PCI Security Standards Council, Requirements and Security Assessment Procedures version 2.0, https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf, fecha de publicación: Octubre 2010

[2]. PCI Security Standards Council, PCI DSS Virtualization Guidelines version 2.0, https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf, fecha de publicación: Junio 2011

[3]. PCI Security Standards Council, Understanding the Intent of the Requirements, https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf, fecha de publicación: Octubre 2010

[4]. VMWARE Inc, VMware Solution Guide for Payment Card Industry (PCI), https://www.vmware.com/files/pdf/VMware-Payment-Card-Industry-Solution-Guide.pdf, fecha de publicación: Septiembre 2012

[5]. VMWARE Inc, Instalador VMware Compliance Checker for PCI, http://www.vmware.com/products/pci-compliance-checker/download.html, fecha de consulta 20 DE JULIO 2015

[6]. VMWARE Inc, VMware Security Hardening Guides. Obtenido de vmware.com: https://www.vmware.com/files/xls/hardeningguide-vsphere5-5-ga-released.xlsx , fecha de consulta 20 de JULIO 2015