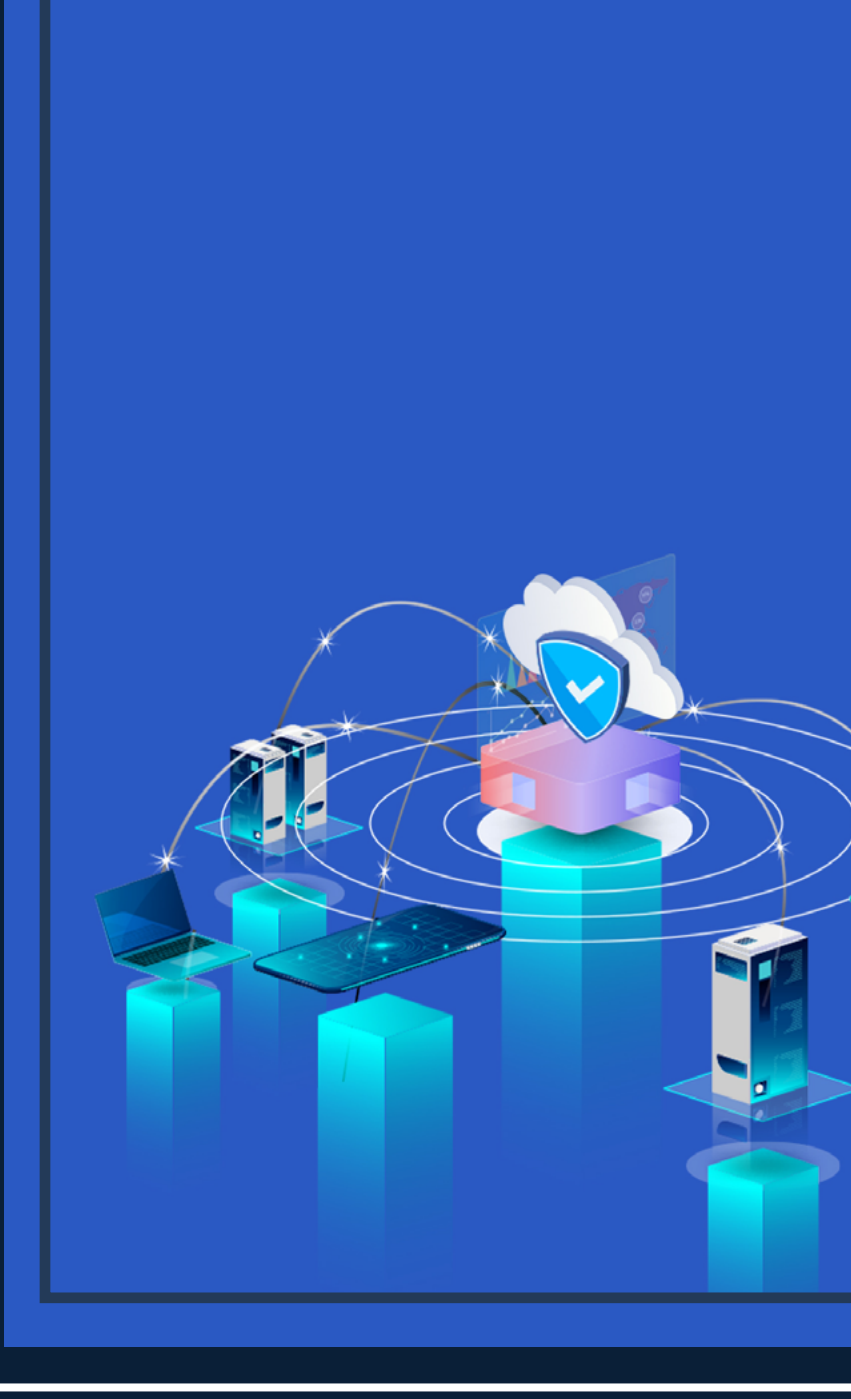
CCN-CERT

BP/15



Buenas Prácticas en Virtualización

INFORME DE BUENAS PRÁCTICAS

AGOSTO **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SBP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.09.13 20:17:06 +02'00'

Centro Criptológico Nacional, 2021

Fecha de edición: Agosto de 2021

Índice

1. Sobre CCN-CERT, CERT Gubernamental Nacional 5

2. Introducción 6

3. Tipos de virtualización 8

4. Retos de seguridad en la virtualización 9

5. Tipos de redes virtualizadas 10

6. Buenas prácticas Hyper-V 11

6.1 Creación de máquina virtual y asignación de recursos 13

6.1.1 Memoria RAM 14

6.1.2 Disco 16

6.2 Protección de los recursos de la máquina virtual 18

6.3 Cifrado 20

6.4 Aislamiento y configuración de redes 23

6.5 Gestión de extensiones de conmutador 28

6.6 Servicios de integración 30

6.7 Seguridad "Virtualization-Based" para máquinas virtuales de generación 2 32

6.8 Puntos de control 33

7. Buenas prácticas VMware Workstation / Player 34

7.1 Cifrado y restricción de máquinas virtuales 35

7.2 Configuración de recursos 37

7.3 Aislamiento y configuración de redes 39

7.4 VMware Tools 40

7.5 Proteccion de máquinas virtuales en los *hosts* 41

7.6 Transferencia de ficheros y texto 42

7.7 Snapshots de las máquinas virtuales 44

Índice

8. Buenas prácticas VirtualBox 45

8.1 Cifrado de máquinas virtuales 47

8.2 Aislamiento y configuración de redes 50

8.3 Compartición portapapeles 53

8.4 Arrastrar y soltar 54

8.5 Carpetas compartidas 55

8.6 Instantáneas en VirtualBox 57

9. Máquina segura de navegación 58

10. Decálogo de recomendaciones 59

11. Glosario 61

1. Sobre CCN-CERT, CERT gubernamental nacional

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo con esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. Introducción

La virtualización es un término que ha sido utilizado para múltiples tecnologías. En el mundo de la informática, se entiende como la recreación de un recurso físico (hardware) o lógico (software), por medio de un hipervisor (hypervisor) que permite la ejecución de más de un entorno al mismo tiempo. En el entorno de máquinas virtuales, el hipervisor permite el uso simultáneo del hardware para más de un sistema operativo, controla la capa física (RAM, CPU, disco, etc.), a la cual sólo él accede, y presenta a los equipos virtuales una interfaz de hardware compatible.

El equipo que presta los medios físicos y sobre el que se instala el hipervisor es conocida como *host* o anfitrión. La máquina virtual que interactúa con el hipervisor y donde se suele instalar un sistema operativo completo, recibe el nombre de *guest* o invitado. El número de máquinas virtuales que puede soportar un *host* depende directamente de los recursos físicos disponibles y de las demandas de cada *guest*.

El hipervisor gestiona el acceso a los diferentes recursos de forma individual y con distintos grados de aislamiento, según el modelo y las necesidades. Sin él, el hardware, tendría problemas de decisión en el momento de atender demandas de uso por parte de sistemas no conectados ni coordinados.

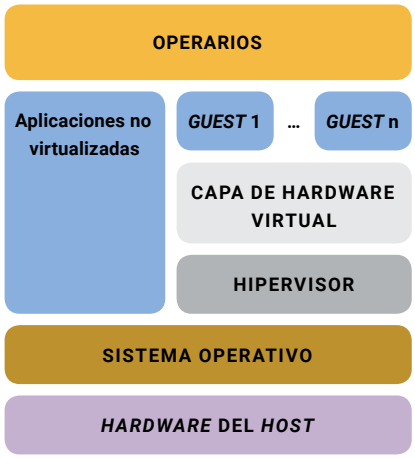
El auge de la virtualización ha llegado con la utilización de la nube (cloud), donde este sistema de reparto de los recursos se hace casi indispensable. Aunque ya existían múltiples sistemas de muchos fabricantes, el desarrollo y avance de los mismos se han incrementado de una forma exponencial. Actualmente se puede optar, entre otros, por XenServer de Citrix, VMware ESXi de Dell, Oracle VM Server, VirtualBox de Oracle e Hyper-V de Microsoft.

El número de máquinas virtuales que puede soportar un *host* depende directamente de los recursos físicos disponibles y de las demandas de cada *guest*

Por lo que respecta a Microsoft, la multinacional ha incorporado herramientas de virtualización desde mediados de la primera década del presente siglo. Con la distribución del sistema operativo Windows Server 2008, se libera la versión inicial de Hyper-V. Desde entonces, con cada nueva versión o release, se incluye un hipervisor con más y mejores capacidades.

VMware comenzó a trabajar la virtualización en 1998. Esta compañía, subsidiaria de Dell, es actualmente una de las principales proveedoras de este tipo de software. Su hipervisor funciona en los principales sistemas operativos del mercado (Windows, Linux y Mac OS). Además, posee una versión específica que permite ejecutar el hipervisor sobre el hardware de servidores físicos, sin necesidad de un sistema operativo adicional. También ofrece la posibilidad de instalarlo desde una memoria USB, de manera que aquellos equipos que disponen de una entrada USB pueden ejecutarlo sin utilizar los discos duros, que quedan liberados para las máquinas virtuales.

Por su parte, VirtualBox comenzó en 1997 a ofrecer un software de virtualización para los principales sistemas operativos, incluido Solaris. La facilidad de uso y su licenciamiento GNU (General Public License versión 2), le han hecho muy popular, especialmente en entornos de escritorio. Actualmente pertenece a Oracle, quien también posee otro hipervisor (Oracle VM Server) de alto rendimiento diseñado para entornos empresariales y de funcionamiento en la nube.



[Ilustración 1]
Ejemplo de esquema de montaje de varias máquinas virtuales.

El auge de la virtualización ha llegado con la utilización de la nube (cloud)

3. Tipos de virtualización

Las principales taxonomías de virtualización atienden a la forma de reparto del hardware y a cuál es el elemento virtualizado. Respecto al primer punto, el reparto de un recurso físico como pueda ser la RAM, la CPU, etc. se conoce como particionado o particionamiento (partitioning). Una manera de hacerlo es mediante la asignación en valores absolutos y estáticos (hard partitioning).

En estos casos, la suma de los recursos parciales será siempre igual o inferior al valor total existente. A modo de ejemplo, si un *host* de ocho núcleos aloja tres máquinas virtuales a las que se les han asignado a cada una dos núcleos, solo se podría incluir una nueva máquina con un núcleo (el otro núcleo debería ser para el sistema operativo y el hipervisor). Esta forma de reparto asegura recursos y un aislamiento mayor, pero no optimiza los elementos hardware.

En ciertos casos, con el fin de optimizar los medios, la mayoría de hipervisores permite un reparto de los recursos con sobreasignación (soft partitioning). Continuando con el ejemplo anterior, en este entorno la suma de los núcleos puede ser mayor que el número real con los que cuenta la máquina. La razón en la que se sustenta para permitir esto, es que todos los equipos virtuales nunca van a alcanzar el máximo de utilización de la capacidad de procesamiento simultáneamente. Si se diera el caso, se efectuaría un reparto proporcional.

Cuando se quiere categorizar por el elemento virtualizado, las principales posibilidades de virtualización son el hardware, las aplicaciones o las sesiones de usuario.

El objetivo de esta guía se centra en estudiar la virtualización del hardware del equipo, tanto con “soft” como con “hard partitioning”.

El objetivo de esta guía se centra en estudiar la virtualización del hardware del equipo, tanto con “soft” como con “hard partitioning”

4. Retos de seguridad en la virtualización

La seguridad en la virtualización tiene la misma premisa que cualquier otro sistema, "minimizar la superficie de exposición". No obstante, cuenta con particularidades que hace que asegurar dicha superficie sea más difícil como por ejemplo la multitud de recursos compartidos o los sistemas operativos que funcionan simultáneamente con sus propias aplicaciones sobre una misma máquina física.

En una situación en la que se tenga un *host* con Windows 10 donde estén virtualizados varios *guest* con la misma versión de sistema operativo, tendrá que multiplicar los esfuerzos para proteger cada una de las máquinas (anfitrión e invitados). Si incluye un sistema operativo diametralmente diferente, como por ejemplo Oracle Linux, aumentan los esfuerzos de manera proporcionada, pero se duplican los conocimientos que debe tener el administrador de sistemas. A eso hay que añadirle que se tienen que aplicar buenas prácticas de seguridad propias de los hipervisores y su gestión.

Para disminuir la complejidad de la gestión de este tipo de entornos los fabricantes están aplicando medidas propias (built in), cada vez de mayor efectividad y seguridad: SMB 3.0 (con cifrado de extremo a extremo), aislamiento de red, extensiones de red, etc.

Asimismo, se deben tener en cuenta consideraciones generales que aplican a los sistemas no virtualizados. Por ejemplo, la navegación por Internet y el correo electrónico son dos de los principales vectores de ataque para un sistema. La "configuración absolutamente segura" no existe, pero siempre se pueden implementar una serie de medidas de seguridad razonablemente adecuadas para conseguir un entorno de trabajo confiable del conjunto hipervisor-anfitrión-invitado.

En definitiva, la principal cuestión de la virtualización, en lo que respecta a la seguridad, es tratar al sistema como si fuese un centro de proceso de datos completo donde se establecen medidas perimetrales (aplicadas al anfitrión) y medidas individuales para cada una de las máquinas alojadas en el mismo (aplicadas al anfitrión y a cada una de las máquinas virtuales).

La navegación por Internet y el correo electrónico son dos de los principales vectores de ataque para un sistema

5. Tipos de redes virtualizadas

Cuando se crean máquinas virtuales en un mismo *host* se pueden asignar todas las interfaces de red físicas a una único *guest*, asociar todas las máquinas virtuales a un único adaptador o hacer un reparto más equilibrado.

En la medida de lo posible, hay que intentar racionalizar la asignación de recursos ya que sobrecargar una tarjeta de red con muchos *guest* penaliza considerablemente el rendimiento. Esto es observable en servidores físicos, pero lo es más aún en equipos portátiles o sobremesas donde es difícil disponer de más de una conexión de red, bien por carencias del propio equipo o bien por la falta de disponibilidad de conexiones en los puestos de trabajo de los usuarios. Además, el uso individualizado de las interfaces de red va en contra del espíritu de la virtualización, donde el aprovechamiento de los recursos por más de una instancia es prácticamente la norma.

Por todo lo indicado anteriormente, los fabricantes han buscado estrategias de virtualización de la red que permiten compartir el ancho de banda de una o más interfaces para todas las máquinas que lo requieran y estén alojadas en el *host*. El fundamento es la creación de tarjetas de red virtuales en la capa de abstracción de la virtualización, gestionadas por el hipervisor, que se adjudican a los *guest*. Posteriormente, las tarjetas de red se podrán dejar aisladas o conectadas a los dispositivos de red físicos.

El conmutador virtual añade características adicionales siendo una de las formas de compartición del hardware de red del *host*, cuyo equivalente en una red de datos física sería la instalación de un *switch* convencional. Está creado y gestionado por el hipervisor, tiene funcionalidades de capa 2 del modelo OSI, lo que permite, por ejemplo, la creación de VLAN.

Además, el hecho de disponer de varios conmutadores virtuales posibilita la gestión de las redes de los *guest* con un mayor nivel de aislamiento.

El fundamento es la creación de tarjetas de red virtuales en la capa de abstracción de la virtualización, gestionadas por el hipervisor, que se adjudican a los *guest*

6. Buenas prácticas Hyper-V

Hyper-V tiene dos (2) opciones de instalación en servidores: el modo *core* y el modo gráfico. La diferencia fundamental estriba en que el modo *core* no tiene un entorno de gestión gráfico desde la máquina local.

En cuanto a las buenas prácticas, estas deben estar orientadas en primer lugar al *host* y después a cada una de las máquinas alojadas.

La administración del hipervisor de Microsoft permite la gestión remota. No obstante, se desaconseja efectuarla solo con las medidas propias del sistema, debiéndose añadir algunas adicionales como el cifrado de datos en la conexión. Se puede ver el apartado "Setting Namespace Security to Require Data Encryption for Remote Connections" en el artículo Securing a Remote WMI Connection disponible a través del siguiente enlace.

https://docs.microsoft.com/es-es/windows/desktop/WmiSdk/securing-a-remote-wmi-connection#setting-namespace-security-to-require-data-encryption-for-remote-connections

Respecto a los sistemas invitados, se deben tener en cuenta las siguientes buenas prácticas:

a. **Establecer una correcta gestión de los permisos, impidiendo el acceso a los ficheros a todo usuario que no lo requiera, sea en remoto o en local.**

b. **Sincronizar la hora para permitir auditorías y registros fiables.**

c. **Gestionar los ficheros de manera segura. Para ello, se cifrarán con *BitLocker* y eliminarán aquellos que no se utilicen con herramientas seguras como Eraser para Windows o KillDisk para GNU/Linux, aparte de otras como HDDEraser (autoarrancable para el borrado total de discos).**

d. **Mantener actualizado el *host*, los *guest* y los servicios de integración al día. Como mínimo, sería necesario instalar los parches de seguridad considerados como importantes y críticos.**

e. **Utilizar un producto para evitar el código dañino y soluciones de cortafuegos en los equipos invitados o usar extensiones de conmutador que los integren. No es incompatible la aplicación simultánea de ambas opciones.**

f. **Evitar tener activos CD o DVD en los clientes, ya que las propias imágenes ISO montadas desde el disco duro del anfitrión podrían ser un elemento que incremente la superficie de exposición.**

g. **Mantener el máximo aislamiento de la red, creando únicamente las conexiones imprescindibles.**

h. **En la medida de lo posible, evitar la compartición de recursos entre máquinas virtuales o con el anfitrión. Cuando sea absolutamente imprescindible, se mantendrá una política de permisos lo más restrictiva posible.**

En el apartado de continuidad del servicio es altamente recomendable, realizar copias de seguridad. Los archivos de respaldo podrán almacenarse localmente, en recursos de red o en medios extraíbles (por ejemplo, un disco duro externo USB). En estos casos, es inexcusable el cifrado de datos, medida que se ha de imponer a todos los medios utilizados, ya sean internos o externos.

Los archivos de respaldo podrán almacenarse localmente, en recursos de red o en medios extraíbles

6.1 Creación de máquina virtual y asignación de recursos

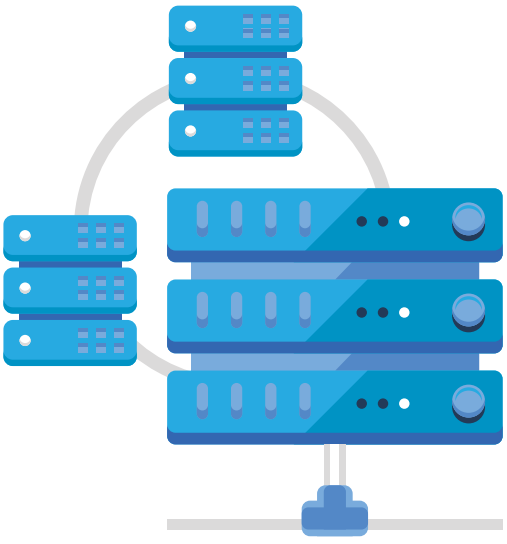
Para generar un *guest* en Hyper-V se utiliza un asistente que es muy similar en Windows 10 Professional o Enterprise y en las versiones de servidor. Dicho asistente permite tanto la creación rápida de máquinas virtuales como su importación desde otros entornos de virtualización. La tecnología de Microsoft soporta una gran variedad de sistemas operativos de escritorio y de servidor, bien sean de Windows o de Linux.

La asignación de recursos de hardware virtualizado se puede efectuar de dos maneras. Por un lado, desde Hyper-V Manager y nada más ejecutar el asistente, escribir el nombre de la máquina y después pulsar en "Finalizar". En este caso el Hypervisor asigna la memoria RAM, el espacio en disco y la red de forma automática. Por otra parte, si se opta por continuar con el asistente se pueden ir definiendo de forma manual los recursos y tener en consideración previa el artículo de Microsoft acerca de la Optimización del rendimiento para servidores Hyper-V, disponible a través del siguiente enlace:

https://docs.microsoft.com/es-es/windows-server/administration/performance-tuning/role/hyper-v-server/

Para usar correctamente la asignación de recursos, es necesario conocer algunos conceptos para una mejor administración de los mismos.

Para usar correctamente la asignación de recursos, es necesario conocer algunos conceptos para una mejor administración de los mismos



6.1.1 Memoria RAM

En Hyper-V hay dos (2) tipos de asignación sobre el recurso de memoria, asignación dinámica y asignación estática.

La memoria dinámica es una característica de Hyper-V que permite que el hipervisor maneje el consumo de la memoria RAM de los invitados de un *host* de manera flexible. Por ejemplo, el hipervisor puede agregar, de manera dinámica, más RAM a un *guest* cuando el sistema operativo lo necesite o reclamar la recuperación del sobrante cuando el *guest* se encuentre inactivo. Esta tecnología es especialmente útil cuando se poseen muchas máquinas virtuales inactivas o con poca carga de trabajo.

Cuando se decida utilizar la memoria dinámica, deben establecerse algunos valores de configuración sobre ésta. Si se decanta por la asignación estática, es necesario que se tenga especial cuidado con las máquinas que están en funcionamiento, ya que la memoria RAM que se escoja quedará reservada para el *guest* una vez que se inicie, aunque no la esté usando.

Por ello, es necesario tener especial cuidado con las máquinas que se inician, debiendo elegir únicamente las imprescindibles.

- **RAM de arranque:** es la cantidad de memoria RAM asignada a un *guest* durante su arranque. Este valor puede ser el mismo que el "mínimo de RAM" o más, hasta el "máximo de RAM". El valor de la memoria RAM de arranque solo se puede modificar con la máquina virtual apagada. Una vez que se complete el arranque de la misma y el hipervisor se haya iniciado, intentará utilizar la cantidad de RAM configurada como el mínimo de memoria RAM.
- **Mínimo de RAM:** es la cantidad mínima de memoria RAM que el *host* debe intentar asignar a una máquina virtual cuando se inicia. Cuando múltiples memorias demandan memoria, el *host* de Hyper-V puede reasignar RAM de la máquina virtual hasta que se cumpla su valor mínimo de RAM.
- **Máximo de RAM:** es la cantidad máxima de memoria RAM que el *host* proporcionará a la máquina virtual. Esta opción solo se puede aumentar mientras que la máquina virtual está en funcionamiento no se pudiéndose reducir salvo que dicha máquina esté apagada.
- **Búfer de memoria:** es el porcentaje de la memoria que Hyper-V debe asignar a la máquina virtual como un búfer. El valor se puede configurar en un rango de 5% a 200% con un 20% configurado de manera predeterminada.
- **Peso de la memoria:** es la prioridad que se configura para una máquina virtual en comparación con otras que funcionan en el mismo *host* de Hyper-V.

La asignación estática de memoria supone la reserva sobre el total de la memoria disponible en el *host*, lo que se traduce en la necesidad de realizar un dimensionamiento adecuado de dicha asignación, de manera que no supere dicho total de memoria disponible, teniendo en consideración los *guest* que pueden estar activos al mismo tiempo.

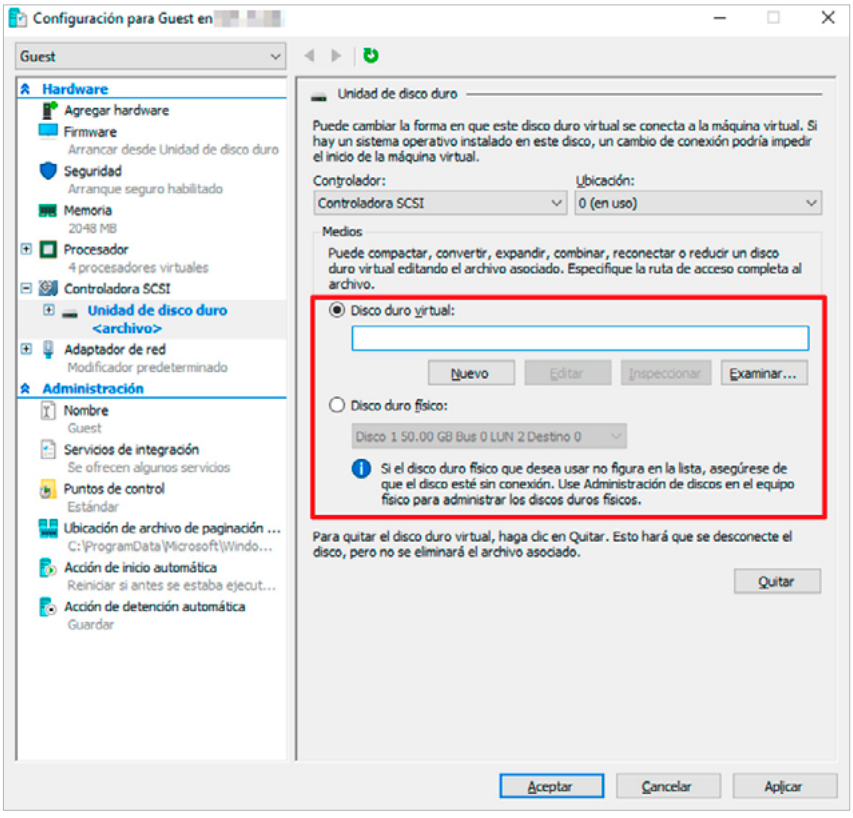
La asignación estática de memoria supone la reserva sobre el total de la memoria disponible en el *host*, lo que se traduce en la necesidad de realizar un dimensionamiento adecuado de dicha asignación

6.1.2 Disco

En cuanto a la asignación de espacio de almacenamiento, existen varias configuraciones respecto al disco y los tipos de éste a seleccionar en Hyper-V.

Se puede crear o asignar según las necesidades dos (2) modelos de discos:

- **Disco duro virtual:** se trata de un disco que es creado en el *host* para ser asociado a la máquina virtual donde poder albergar toda la información generada. Estos discos son los más utilizados ya que generan un fichero propio que puede sufrir diversas modificaciones manteniéndose la capacidad de almacenamiento, pudiendo realizar por ejemplo exportaciones, puntos de control, etc.
- **Disco duro físico:** esta configuración permite asociar un disco perteneciente al *host* (hardware real) para la máquina virtual. Esta opción puede ser útil en ciertas circunstancias, sin embargo, el disco queda asociado a la máquina virtual no pudiendo el *host* hacer uso del disco para otro propósito. Además, se debe tener en consideración que el rendimiento que proporciona el disco en el *guest* depende directamente de éste. Para poder seleccionar esta opción el disco debe estar en modo "sin conexión" en el *host*.



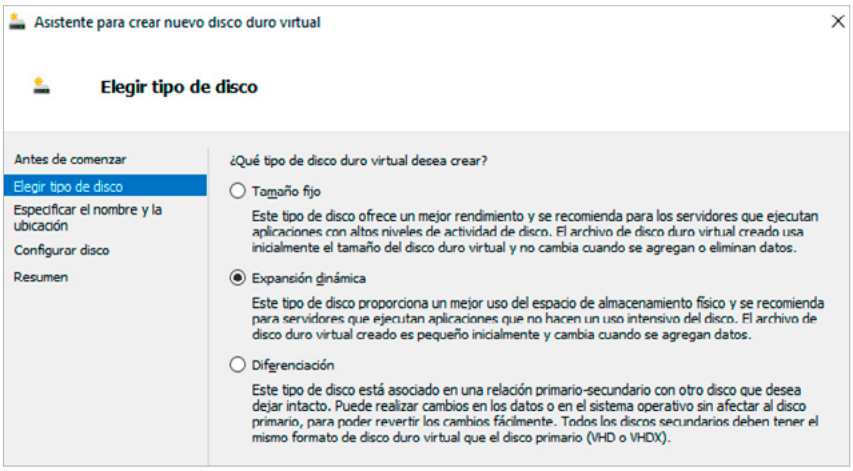
[Ilustración 2] Selección del disco duro en el asistente.

En cuanto al tipo de disco virtual, se pueden seleccionar las siguientes opciones:.

a. **De tamaño Fijo:** los discos duros virtuales fijos proporcionan capacidad de almacenamiento mediante el uso de un archivo con el tamaño especificado para el disco duro virtual en el momento de la creación del disco. El tamaño del archivo permanece "fijo" independientemente de la cantidad de datos almacenados. No obstante, puede utilizarse el Asistente para edición de disco duro virtual con objeto de aumentar el tamaño del disco duro virtual, lo que incrementa el tamaño del archivo. Esta configuración es la recomendada cuando el *guest* implementado requiere de mucha lectura/escritura del propio disco.

b. **Expansión dinámica: l**os discos duros virtuales de este tipo proporcionan la capacidad de almacenamiento necesaria para almacenar los datos. El tamaño del archivo es pequeño cuando se crea el disco y crece hasta el máximo asignado, a medida que se agregan datos al mismo. El tamaño del archivo no disminuye automáticamente cuando se eliminan datos del disco duro virtual. Sin embargo, es posible compactar el disco para reducir el tamaño de archivo después de eliminar datos mediante el Asistente para edición de disco duro virtual. Esta opción es recomendable en máquinas virtuales de prueba o laboratorios, así como en entornos en los que se prevé poco crecimiento y poco uso del mismo.

c. **Diferenciación:** son los discos duros que parten de un disco duro virtual primario y permiten al usuario realizar cambios a partir de él sin alterarlo. Su definición es exactamente igual a la del disco virtual primario en cuanto a su tipo y tamaño. El tamaño del archivo de un disco de diferenciación crece a medida que se almacenan cambios en el disco.



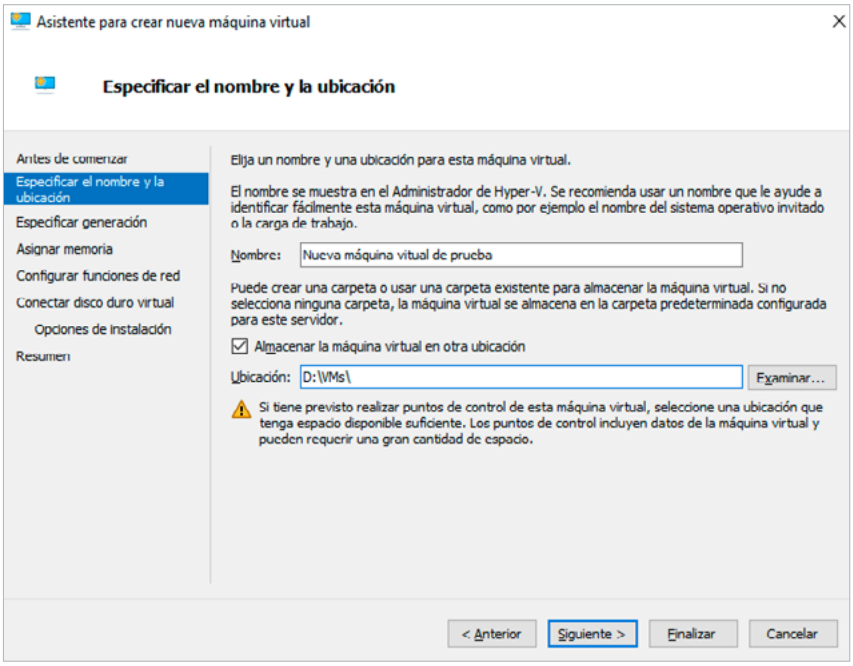
[Ilustración 3] Selección del "Tipo" de disco duro en la máquina virtual.

6.2 Protección de los recursos de la máquina virtual

Cada una de las máquinas virtuales que se cree debe ser protegida de forma individual, tanto en las características asignadas desde el asistente de creación como dentro de la propia máquina.

Después de la primera pantalla informativa del primer paso (donde no es recomendable optar por la creación de una máquina con los valores por defecto), en el segundo paso se debe seleccionar la ubicación de la máquina virtual. Es conveniente la utilización de una carpeta dedicada para facilitar la protección de la misma por medio de permisos NTFS, cifrado, etc. Si se encuentra en un equipo de un único disco duro se debe considerar que la utilización de particiones puede disminuir la superficie de exposición, pero ello va en perjuicio del rendimiento.

La elección de la ubicación puede ayudar a la posterior protección de la máquina virtual



[Ilustración 4]
Selección de la ubicación de la máquina virtual.

La elección de la ubicación puede ayudar a la posterior protección de la máquina virtual. Para ello, la carpeta donde se guarde la definición de las máquinas virtuales y los discos duros deben disponer de, al menos, los siguientes permisos:

[Tabla 1] Permisos directorio de máquinas virtuales y discos duros.

CUENTA	PERMISOS	APLICAR A
Administradores	Control total	Esta carpeta, subcarpetas y archivos
System (Sistema)	Control total	Esta carpeta, subcarpetas y archivos
Creator owner (Propietario creador)	Control total	Solo subcarpetas y archivos

Cuando se haya decidido cuál va ser la carpeta de destino definitiva para los *guest* que se vayan creando se podrá poner esta ruta en las propiedades generales del hipervisor. Para ello hay que pulsar en "Configuración de Hyper-V..." y **en la ventana emergente se deberá cambiar la configuración de los apartados, "Discos duros virtuales" y "Máquinas virtuales".** De esta manera se evita tener que realizar las modificaciones con cada creación de máquina virtual.

En los casos en que se requiera añadir algún usuario o grupo adicionales, se recomienda utilizar el mínimo de permisos indispensable y retirarlos cuando ya no sean necesarios. Microsoft, durante la instalación del hipervisor, crea la cuenta de grupo "Administradores de Hyper-V" vacía. Si se utiliza, también deberá recibir permisos de control total sobre las carpetas.

Esta gestión sobre la Lista de Control de Accesos (ACL) impedirá que los ficheros relacionados con las máquinas virtuales puedan ser alterados, copiados o accedidos por la red de forma no autorizada por cualquiera que no tenga un alto escalado de privilegios. Como medida adicional, **se puede habilitar la auditoría de acceso a las carpetas de alojamiento de los ficheros de virtualización para poder hacer un seguimiento de los accesos por parte de cuentas autorizadas** e incluso para intentos fallidos de acceso a otras cuentas.

En el siguiente paso se selecciona, lo que Microsoft denomina la "Generación". Siempre que el sistema operativo invitado pueda trabajar en entornos con UEFI se tiene que optar por la Generación 2. UEFI proporciona seguridad adicional frente a BIOS clásicas.

NOTA:

Para conocer más sobre Extensible Firmware Interface, UEFI, y obtener sus especificaciones puede consultar el siguiente enlace: https://www.intel.es/content/www/es/es/architecture-and-technology/unified-extensible-firmware-interface/efi-homepage-general-technology.html

El documento *CCN-CERT IA-08/15 Amenazas BIOS* disponible a través del siguiente enlace https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/789-ccn-cert-ia-08-15-amenaza-en-bios/file.html ayuda a incrementar la seguridad en este tipo de elementos

6.3 Cifrado

Cuando las máquinas virtuales alojadas en el *host* lo requieran se deben proteger los ficheros por medio de cifrado *BitLocker*, siempre que el equipo disponga de dicha posibilidad. Para conocer más acerca de *BitLocker*, revise el documento Información general en la web TechNet de Microsoft, disponible a través del siguiente enlace.

https://docs.microsoft.com/es-es/previous-versions/windows/server/hh831713(v=ws.11)

No es una opción válida el cifrado de los ficheros por medio de Encrypting File System (EFS) ya que esto no permitiría la utilización de los discos o ficheros de definición por cuentas ajenas a la que proporciona el certificado utilizado para el cifrado. En ciertos entornos de dominio puede haber cuentas maestras de descifrado, pero no se debe contar con ello sin tener la certeza de su existencia. Puede obtener más información sobre Encrypting File System (EFS) en el enlace:

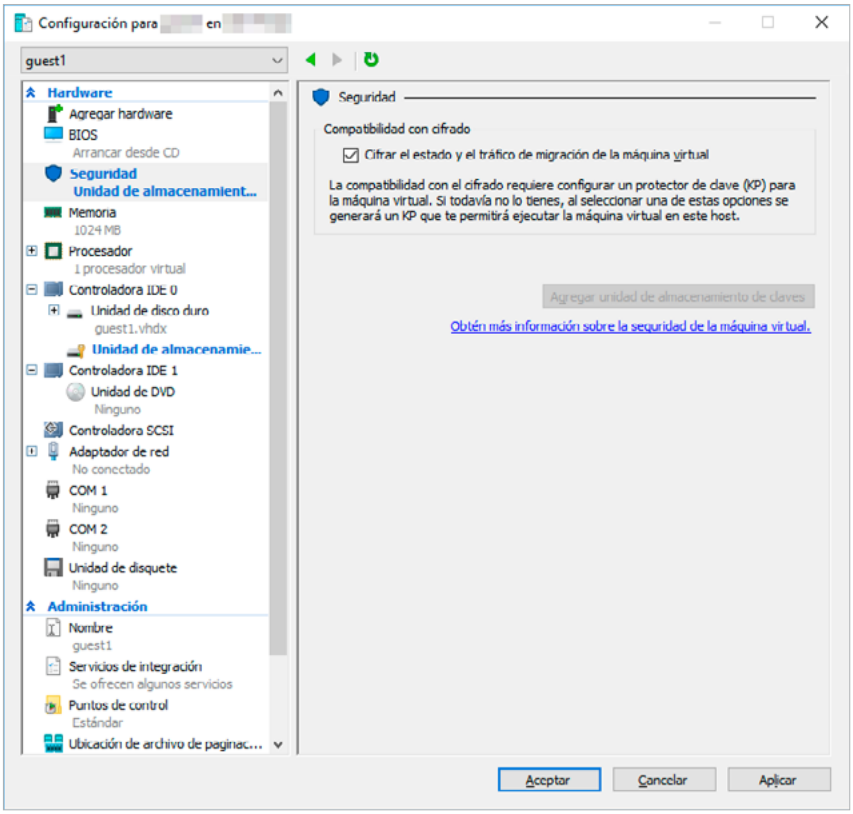
https://docs.microsoft.com/en-us/windows/desktop/fileio/file-encryption

El uso de *BitLocker* dentro de una máquina virtual no está disponible de forma general. Sin embargo, se puede utilizar el sistema EFS, de forma habitual, para el cifrado de ficheros que contengan información reservada. Eso sí, siempre con la salvedad indicada más arriba, sobre el usuario único que puede acceder.

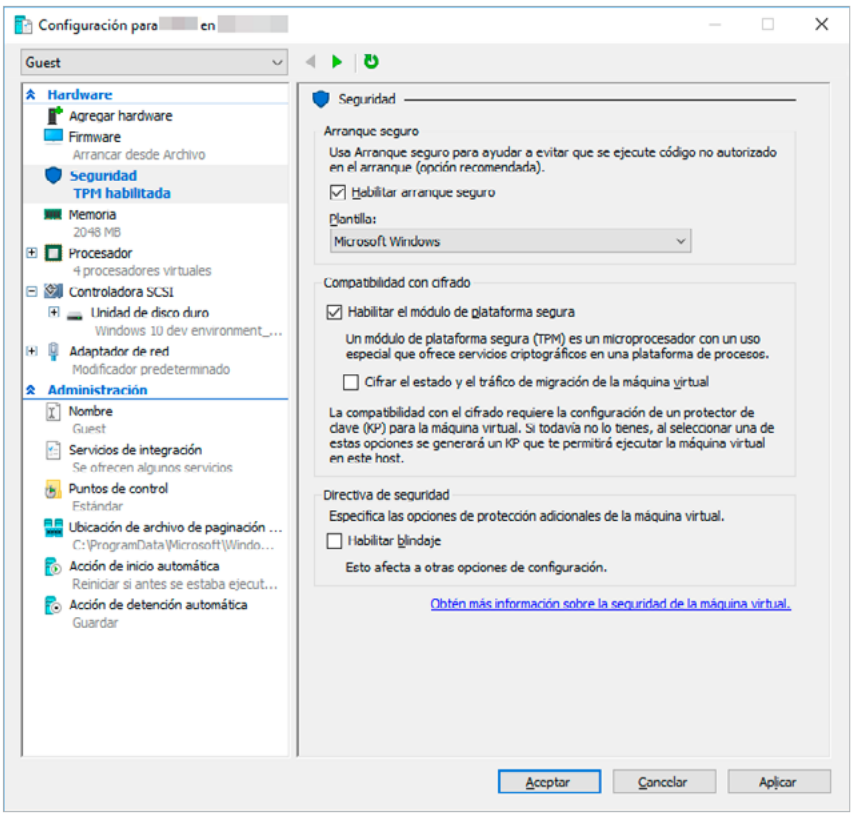
Hasta ahora solo las máquinas virtuales de generación 2 poseían la capacidad de cifrado para proteger los recursos que éstas contenían. **La nueva versión de Hyper-V permite proteger el disco del sistema operativo mediante el cifrado de unidad *BitLocker* en máquinas virtuales de generación 1.** Esta nueva funcionalidad hace uso de una unidad pequeña y dedicada para almacenar la clave de *BitLocker* de la unidad del sistema.

Cuando las máquinas virtuales alojadas en el *host* lo requieran se deben proteger los ficheros por medio de cifrado *BitLocker*

[Ilustración 5] Configuración de cifrado en máquina de Generación 1.



Tal y como se ha indicado anteriormente, las máquinas virtuales de Generación 2 pueden seguir haciendo uso de la funcionalidad de un TPM virtual que permita cifrar el disco de la máquina virtual mediante *BitLocker* como si se tratase de una máquina física.



[Ilustración 6] Configuración de cifrado en máquina de Generación 2.

Otra de las novedades en Hyper-V 2016 son las denominadas **"Máquinas virtuales blindadas", que permiten cifrar las máquinas virtuales y su estado de modo que se asegura que éstas solo se ejecutan en *host* autorizados por el Servicio de protección de *host*.** Se puede ampliar la información consultando en los siguientes enlaces:

https://docs.microsoft.com/es-es/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms

https://docs.microsoft.com/es-es/windows-server/security/guarded-fabric-shielded-vm/guarded-fabric-and-shielded-vms-top-node

Las máquinas virtuales blindadas protegen los datos y el estado de la máquina virtual contra el robo y la manipulación de privilegios de administrador. Las máquinas virtuales blindadas funcionan con las máquinas virtuales de generación 2, que proporcionan el arranque seguro necesario, el firmware UEFI y el soporte virtual TPM (vTPM) 2.0. El *host* de Hyper-V debe ejecutar Windows Server 2016 o Windows 10, y el sistema operativo invitado alojado en la máquina virtual debe ser Windows Server 2012 o superior.

Las máquinas virtuales blindadas protegen los datos y el estado de la máquina virtual contra el robo y la manipulación de privilegios de administrador

Las máquinas virtuales blindadas ofrecen los siguientes beneficios:

- **Los discos están cifrados.**
- **El proceso de trabajo de las máquinas virtuales se encuentra fortalecido ayudando a prevenir una posible manipulación. (VMWP).**
- **Bloqueo de PowerShell direct y acceso mediante consola.**

6.4 Aislamiento y configuración de redes

La creación de la máquina virtual debería contar, en la mayoría de los casos, con un adaptador virtual de red no conectado. Más adelante, una vez implementadas todas las medidas de seguridad necesarias, se unirá al conmutador adecuado. Microsoft implementa, por defecto, una serie de medidas de seguridad que permiten un grado de aislamiento alto, pero esto se debe completar con buenas prácticas, ya que este medio de comunicación constituirá la mayor parte de la superficie expuesta por las máquinas virtuales.

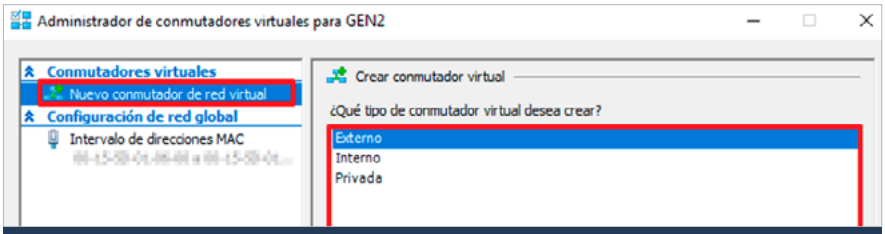
En lo que se refiere a Hyper-V, esta tecnología trabaja con una capa de abstracción de la red física del *host* que crea conmutadores y tarjetas de red virtuales. Es una elección conectar dichas tarjetas a los mencionados *switches* de forma permanente, temporal o no hacerlo. Se debe, siempre, optar por la configuración mínima requerida y, de esta forma, si no se requiere conectividad alguna, la máquina virtual debería permanecer con los valores de creación predeterminados. Los conmutadores de red virtuales pueden ser externos, internos o privados.

[Tabla 2] Descripción y ejemplos de uso de conmutadores virtuales.

TIPO	DESCRIPCIÓN	EJEMPLOS DE USO
Externo	Crea un conmutador virtual que se enlaza al adaptador de red físico para que las máquinas virtuales puedan obtener acceso a la red física donde esté conectado.	Las máquinas virtuales necesitan conectividad con Internet. Las máquinas virtuales deben ser accedidas por usuarios de la red.
Interno	No conecta con la red física del *host*, pero crea un punto de unión que puede ser utilizado por cualquiera de las máquinas virtuales que se ejecuten en él, además del propio anfitrión.	Red de equipos virtuales que deben interaccionar entre ellos y donde el equipo *host* se utiliza como cliente de pruebas.
Privado	Es igual que el interno, pero no se incluye al *host* como equipo de esta red.	Red de equipos virtuales que deben interaccionar entre ellos, pero no con cualquier otro equipo.

Cuando un conmutador se conecta al dispositivo de red físico, conmutador externo, existen otros parámetros y variables que deben tenerse en cuenta.

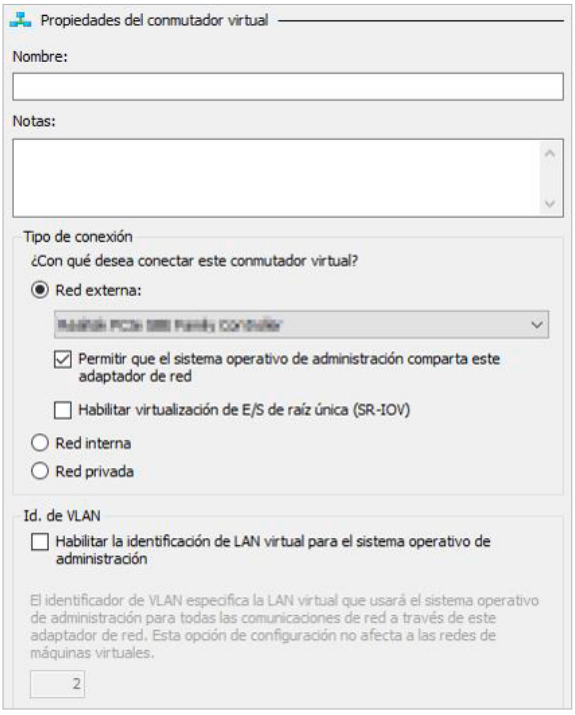
[Ilustración 7] Pantalla de creación de un conmutador externo.



NOTA: En este ejemplo dispondrá de conectividad a la red a la que se encuentre alojado el adaptador físico.

La casilla, marcada por defecto, "Permitir que el sistema operativo de administración comparta este adaptador de red", confiere valores de "soft partitioning" a este elemento del *host*. Si se desmarca se obtiene un alto valor de aislamiento de red. Pero **el adaptador físico no podrá ser utilizado en otros conmutadores ni por el anfitrión.**

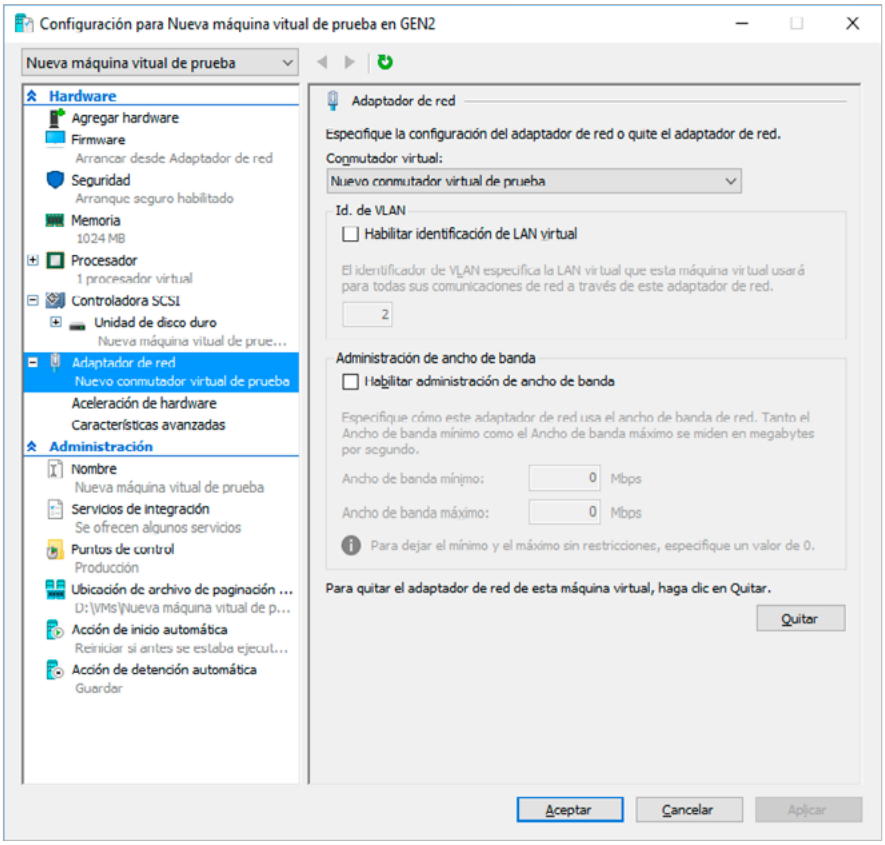
[Ilustración 8] Propiedades de un conmutador virtual.



El "Id. de VLAN", de activarse, permitirá que todas las comunicaciones del sistema operativo anfitrión vayan marcadas por el identificador de VLAN que se seleccione en la casilla inferior (el valor por defecto es (2). Esta opción requerirá que el puerto del conmutador físico al que se conecta la red física del *host* permita el tráfico de la VLAN elegida, sea porque el puerto pertenece a dicho segmento de red o porque el puerto es una conexión troncal (trunk) y la VLAN esté incluida en la lista de redes permitidas. También se debe asegurar que los equipos virtuales utilicen este conmutador y dispongan de una dirección IP válida en la VLAN elegida.

Una vez creada la máquina virtual desconectada y creados los conmutadores de red virtuales deseados, es el momento de configurar los dispositivos de red virtuales según las necesidades. Para ello se debe abrir la configuración del *guest* y seleccionar "Adaptador de red".

[Ilustración 9] Configuración de un adaptador de red de una VM alojada en el anfitrión.



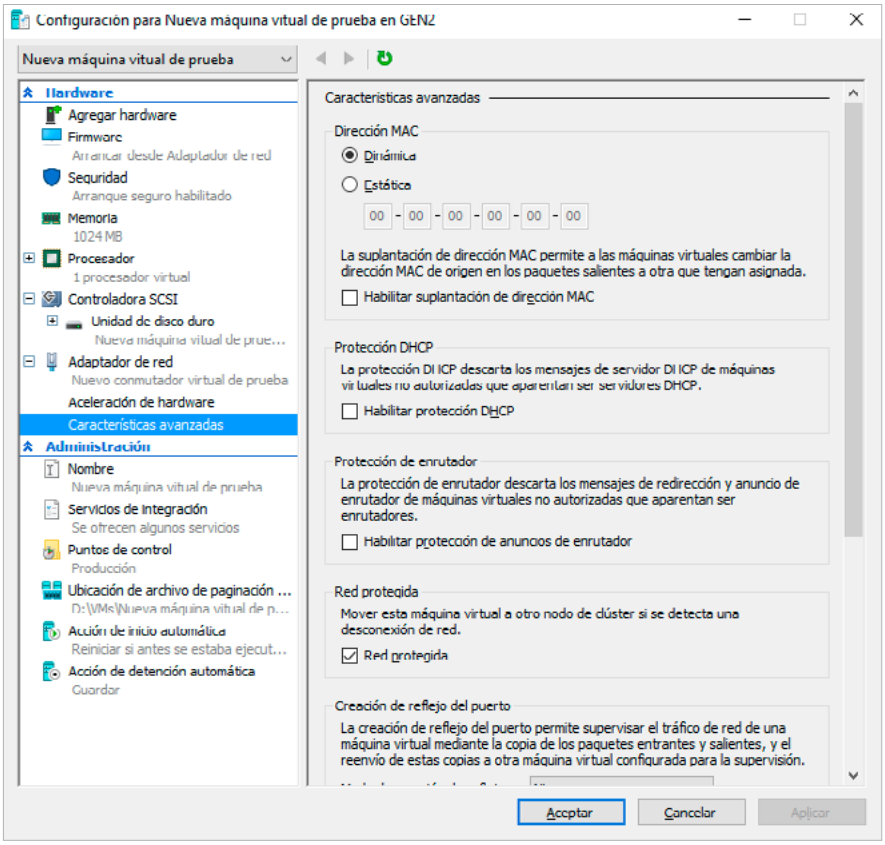
A nivel del adaptador de red del *guest*, el "Id. de VLAN" permite seleccionar un identificador de una Red de Área Local Virtual pero solo para ese único dispositivo, no para todo el conmutador. No se debe seleccionar si ya se configuró en el *switch* virtual en modo VLAN.

Por su parte, **la "Administración del ancho de banda" permite el ya mencionado "soft partitioning" de la red física,** además de la reserva de ancho de banda para un determinado adaptador de red. En el caso del mínimo, la suma de los parciales debe ser menor que el valor del dispositivo físico al que se conecta el conmutador virtual. **Se debe descontar una cantidad reservada para el propio *host*.** Por ejemplo, para una red GigaEthernet se bloquearían 100 Mbps para el anfitrión.

La opción de "Características avanzadas" conduce a una ventana donde se pueden activar o desactivar variables de la red que gestionarán protecciones de este elemento.

La opción de "Características avanzadas" conduce a una ventana donde se pueden activar o desactivar variables de la red que gestionarán protecciones de este elemento

[Ilustración 10] Características avanzadas de una tarjeta de red virtual.



Todas las características de esta ventana son necesarias en algún momento en la gestión, especialmente de servidores, ya que no existen, en general, unos valores ideales. A continuación, se describen una serie de consejos rápidos que se pueden extrapolar a otros casos particulares.

[Tabla 3] Características avanzadas de tarjeta de red de Hyper-V y ejemplos de uso.

CARACTERÍSTICA	DESCRIPCIÓN	EJEMPLOS DE USO
Dirección de MAC	Permite la asignación de una MAC concreta o activa la suplantación de la MAC (MAC Address Spoofing) del equipo virtual.	Asigne una MAC estática en pruebas de máquinas virtuales que se encuentran en lista de control de acceso de dispositivos de red.
Protección DHCP	Protege contra servidores DHCP fraudulentos en equipos virtualizados. Es conveniente la activación de esta variable.	Se desactiva esta opción para un servidor virtualizado destinado a pruebas con Active Directory y servidor DHCP, que, además, esté conectado a una red interna con otros equipos, algunos de ellos clientes DHCP.
Protección de enrutador	Protege contra anuncios fraudulentos. Es conveniente la activación de esta variable.	En un entorno de análisis forense de una máquina virtual se puede activar para observar si emite mensajes de esta índole.
Red protegida	Es una medida de alta disponibilidad.	Pruebas de máquinas virtuales en clúster de alta disponibilidad.
Creación de reflejo del puerto	La activación crea un puerto “mirror” donde se duplica el tráfico. Su habilitación puede aumentar la superficie de exposición.	Análisis de tráfico para auditoría de seguridad, sin alterar la red en estudio.
Formación de equipo de NIC	La creación de “Network Teams” es una medida de alta disponibilidad e incremento de recursos.	Pruebas de alta disponibilidad de red en una máquina virtual que va a ser puesta en producción, posteriormente, con esta característica.
Nomenclatura de dispositivos	**La activación de la propagación de nombres podría provocar una filtración de información**, habitualmente no grave, pero innecesaria. No active esta casilla sin una necesidad específica.	En un entorno de pruebas de máquinas Windows, sin datos de seguridad, se quiere facilitar la tarea de conexión entre las máquinas virtuales en una red interna (en conmutadores externos no debería activarse en ningún caso).

NOTA: Puede consultar más información, y uso de PowerShell, para estas características en el artículo “Novedades del conmutador virtual de Hyper-V en Windows Server 2012” a través del siguiente enlace:

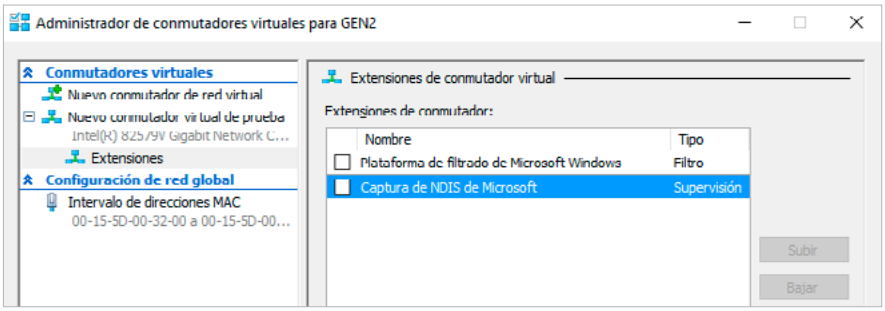
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj679878(v=ws.11)

6.5 Gestión de extensiones de conmutador

Las extensiones de conmutador virtual permiten la inclusión de software de terceros para el filtro, la captura y el reenvío de tráfico de red. La configuración segura de cada extensión de conmutador depende de los parámetros de cada uno de los fabricantes, en general, y de la propia extensión en particular.

Por lo que respecta a Hyper-V, este se proporciona con dos extensiones instaladas, pero no habilitadas. Se trata de la Plataforma de filtrado de Microsoft Windows (WFP) y la Captura de NDIS de Microsoft.

[Ilustración 11] Extensiones por defecto de un conmutador virtual en Hyper-V.



La primera de ellas, WFP, se debe activar cuando así lo requiera la extensión de un tercero, con el condicionamiento que podría afectar a ciertas máquinas virtuales. Puede consultar el artículo de TechNet "Hyper-V: The WFP virtual *switch* extension should be enabled if it is required by third party extensions" disponible a través del siguiente vínculo para más información.

https://social.technet.microsoft.com/wiki/contents/articles/13071.hyper-v-the-wfp-virtual-switch-extension-should-be-enabled-if-it-is-required-by-third-party-extensions.aspx

Esta arquitectura habilita el filtrado y modificación de paquetes de red, la monitorización, la conexión promiscua y otras funciones. La extensión de captura de NDIS es una API que permite la instalación de extensiones en el driver del conmutador virtual de Hyper-V.

Fabricantes de software, como por ejemplo "5NINE SOFTWARE", disponen de extensiones que permiten la inclusión de firewall virtual, antivirus, sistema de detección de intrusiones (IDS), inspección de anomalías de red, escaneado de tráfico de red, listado de conexiones y estadísticas de las máquinas virtuales implementadas en un servidor de Hyper-V.

La extensión de captura de NDIS es una API que permite la instalación de extensiones en el driver del conmutador virtual de Hyper-V

6.6 Servicios de integración

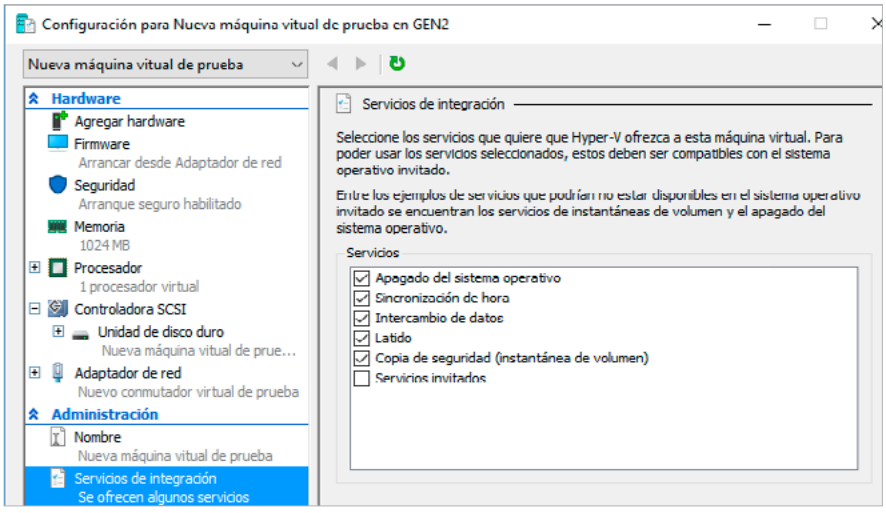
Los servicios de integración, "integration services" de Hyper-V, habilitan la comunicación de las máquinas virtuales con el *host*. Su instalación proporciona muchas ventajas para la mejora del rendimiento y el correcto funcionamiento de *guest* (por ejemplo, la sincronización de la hora), pero aumenta la superficie expuesta a los ataques. Se puede ampliar la información en el artículo "Administrar servicios de integración de Hyper-V".

https://docs.microsoft.com/es-es/windows-server/virtualization/hyper-v/manage/Manage-Hyper-V-integration-services

En los sistemas Windows, cada uno de los servicios de integración se instala como un servicio y se puede gestionar desde la MMC como tal

Funcionan en dos partes, por lo que para que un servicio esté activo debe ser habilitado en ambos extremos, anfitrión e invitado. Los invitados con sistemas Windows Server 2008 R2 y Windows Vista SP2 y posteriores incorporan los servicios de integración de forma predeterminada.

Dentro de la configuración de cada máquina virtual de Hyper-V se accede a los servicios de integración. Por defecto todos están activados, excepto "Servicios invitados".



[Ilustración 12] Servicios de integración.

En los sistemas Windows, cada uno de los servicios de integración se instala como un servicio y se puede gestionar desde la MMC como tal. Puede consultar los servicios a través del siguiente enlace:

https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/reference/integration-services

NOMBRE DEL SERVICIO	CONFIGURACIÓN DE SERVIDOR		SISTEMA OPERATIVO INVITADO	
	CONFIGURACIÓN DE MÁQUINA VIRTUAL PREDE-TERMINADA	VERSIONES QUE ADMITEN LA EJECUCIÓN EN WINDOWS HYPER-V	NOMBRE DE SERVICIO DE WINDOWS	CONTROLADOR DE LINUX / NOMBRE DE DEMONIO
Apagado del sistema operativo	Habilitada	Windows Server 2012 y posteriores	Servicio de apagado de invitado de Hyper-V	hv_utils
Sincronización de hora	Habilitada	Windows Server 2012 y posteriores	Servicio de sincronización de hora de Hyper-V	hv_utils
Intercambio de datos	Habilitada	Windows Server 2012 y posteriores	Servicio de intercambio de datos de Hyper-V	hv_utils y hv_kvp_daemon
Latido	Habilitada	Windows Server 2012 y posteriores	Servicio de latido de Hyper-V	hv_utils
Copia de seguridad (instantánea de volumen)	Habilitada	Windows Server 2012 y posteriores	Solicitante de copia de instantáneas de volumen de Hyper-V	hv_utils y hv_vss_daemon
Servicios invitados	No habilitado	Windows Server 2012 R2 y posteriores	Interfaz de servicios de sistemas invitados de Hyper-V	hv_utils y hv_fcopy_daemon

[Tabla 4]
Lista de servicios de integración.

El caso particular del servicio de integración de intercambio de datos puede requerir de la instalación de un fichero ".cab", disponible en el centro de descargas de Microsoft. Este servicio permite el intercambio de información de relevancia y utiliza una clave de registro para estas funciones. Para la descarga del servicio de integración de intercambio de datos visite el siguiente enlace de Microsoft:

https://support.microsoft.com/es-es/help/3071740/hyper-v-integration-components-update-for-windows-virtual-machines-that-are-running-on-a-windows-10-based-host.

Habilitar el servicio de integración llamado "Servicios invitados" conduce a la comunicación entre *host* y *guest*, aunque no haya una red establecida entre ambos, por lo que se desaconseja su activación en entornos sensibles.

6.7 Seguridad “Virtualization-Based” para máquinas virtuales de generación 2

En Hyper-V 2016 está disponible una funcionalidad de seguridad basada en virtualización que ofrece características como *Device Guard* y *Credential Guard*, que brindan una mayor protección del sistema operativo contra ataques de código dañino. La seguridad basada en virtualización está disponible para los *guest* de generación 2 a partir de la versión 8.

***Device Guard* es un grupo de características clave, diseñadas para fortalecer un sistema informático contra código dañino.** Su enfoque es evitar que se ejecute el código dañino al garantizar que solo se pueda ejecutar un código bueno conocido.

***Credential Guard* es una característica específica, que no forma parte de Device Guard, y que tiene como objetivo aislar y fortalecer los sistemas de clave y de los usuarios contra el compromiso,** lo que ayuda a minimizar el impacto y la amplitud de un ataque de tipo "Pass the Hash" en caso de que ya se esté ejecutando un código dañino a través de un vector local o basado en la red.

La primera tecnología que se necesita entender antes de poder profundizar en estas dos características es el modo seguro virtual (VSM). VSM es una característica que aprovecha las extensiones de virtualización de la CPU para proporcionar una mayor seguridad de los datos en la memoria.

Puede ampliar la información de estas características en el siguiente enlace de Technet:

https://blogs.technet.microsoft.com/ash/2016/03/02/windows-10-device-guard-and-credential-guard-demystified/

VSM es una característica que aprovecha las extensiones de virtualización de la CPU para proporcionar una mayor seguridad de los datos en la memoria

6.8 Puntos de control

Un punto crítico de cualquier entorno de virtualización es la creación y gestión de puntos de control (*checkpoints*) o estado de los *guest*. Estos no pueden ser considerados como una copia de seguridad de la máquina, es mejor pensar en el *checkpoint* como un estado consistente de una máquina virtual en un momento específico en el tiempo.

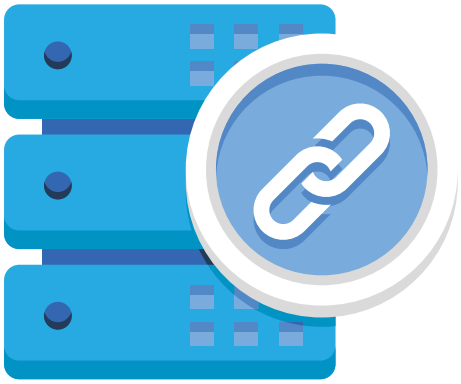
Un *checkpoint* es un disco duro virtual diferencial, que tiene un nombre especial y una extensión ".avhd [x]" y un archivo de configuración xml con nombre GUID. Además, puede haber dos archivos adicionales con memoria de máquina virtual (VM) (.bin) y estado de dispositivos (.vsv) si la máquina virtual se encendió durante la creación del punto de control. Una vez que se toma el punto de control, el disco de diferenciación (.avhd [x]) se convierte en un lugar donde se almacenan los cambios temporales en el disco original de la máquina virtual, mientras que el disco original permanece en modo de solo lectura. No es posible realizar un *checkpoint* de una máquina virtual que utilice discos virtuales de tipo Pass-through (es decir, que no utilice ficheros VHD-VHDX como discos virtuales).

Por este motivo es necesario controlar la generación de *checkpoints* de las máquinas invitadas en un *host* por la degradación que estos producen en los sistemas tanto por la creación de nuevos archivos que no solo debe gestionar el hipervisor, sino al consumo extra de espacio de almacenamiento que estos generan.

Se puede ampliar más información al respecto en el siguiente enlace de Microsoft:

https://docs.microsoft.com/es-es/virtualization/hyper-v-on-windows/user-guide/checkpoints

No es posible realizar un *checkpoint* de una máquina virtual que utilice discos virtuales de tipo Pass-through



7. Buenas prácticas VMware Workstation / Player

En el presente epígrafe se presentan algunos de los apartados más relevantes a la hora de establecer buenas prácticas en el proceso de creación y gestión de máquinas virtuales con VMware Workstation.

El entorno expuesto en el presente documento consta de la creación de estaciones de trabajo virtuales, es decir, el de la virtualización en equipos cliente a través de aplicaciones de escritorio como son las versiones Workstation Pro (que se adquiere mediante una licencia de pago y permite crear y gestionar máquinas virtuales) y Workstation Player (software gratuito que solo permite utilizar máquinas virtuales previamente creadas).

Dentro de los productos ofrecido por VMware existen otras versiones de servidores de máquinas virtuales más profesionales como son ESX y ESXi.

NOTA:

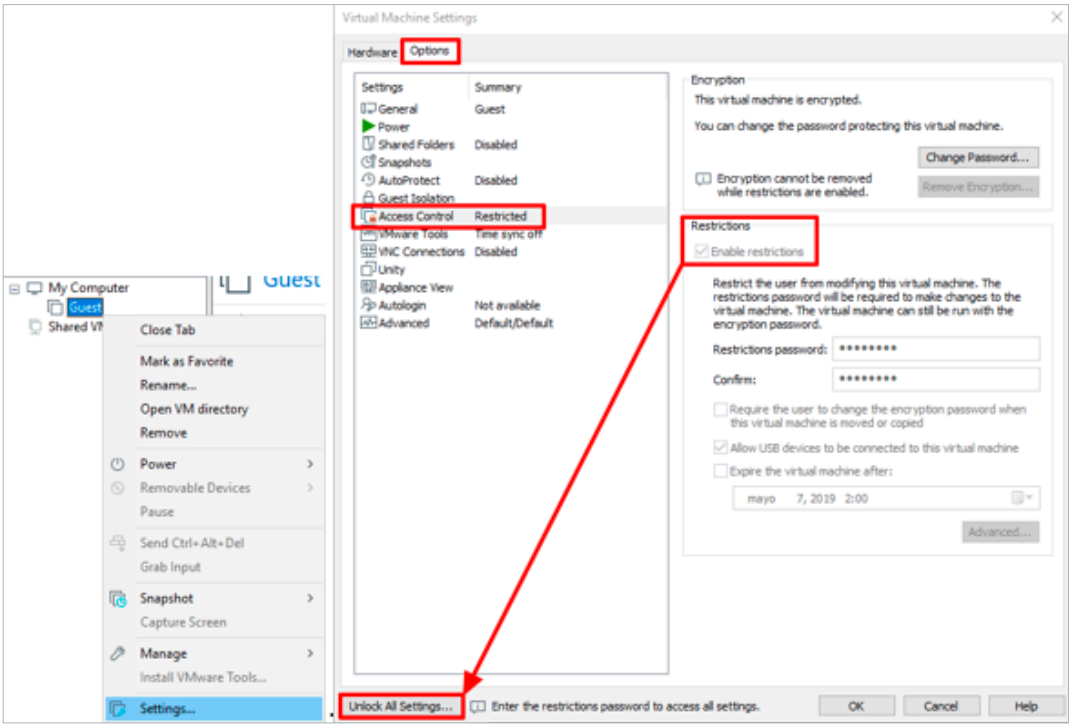
Los ejemplos mostrados a continuación se han obtenido sobre la versión de VMware WorkStation Pro v.15, con licenciamiento gratuito de 30 días

7.1 Cifrado y restricción de máquinas virtuales

En un espacio de trabajo con máquinas físicas, ya sea en fases de prueba o en entornos de producción, se contempla la necesidad de proteger los equipos cliente para evitar que usuarios no autorizados los enciendan, se los lleven a otras ubicaciones o extraigan componentes como memoria RAM, tarjetas de vídeo o red, discos duros, etc. Todas estas acciones pueden ocasionar un funcionamiento erróneo de los sistemas y lo que es más comprometido, una sustracción ilegítima de la información corporativa.

En los entornos virtuales, después de crear una máquina virtual, la primera tarea recomendada es la de proteger el acceso a la misma, así como a sus parámetros básicos de configuración para prevenir daños ocasionados por un uso inadecuado. Esto se puede realizar mediante las opciones de cifrado y restricción, las cuales sólo se pueden configurar con la máquina virtual apagada.

[Ilustración 13] Opciones de Cifrado y Restricción.



El cifrado permite asegurar el acceso a la máquina virtual, incluyendo los componentes que se le han asignado (memoria RAM, unidades externas, discos duros, etc.). Para ello se debe introducir una contraseña que será solicitada posteriormente cada vez que se arranque en la consola de gestión, cuando se exporte a otra consola o si se quiere revertir el proceso de cifrado. La duración del proceso de cifrado dependerá del tamaño de la máquina virtual. Una vez concluido, al reiniciar la consola de gestión, la máquina virtual tendrá el icono de un candado cerrado y aparecerá un cuadro de diálogo en el que se le pedirá al usuario que introduzca la correspondiente contraseña.

La restricción evita que los usuarios accedan a los parámetros de configuración de la máquina virtual, a menos que introduzcan una contraseña específica. Si no se protege este apartado, los usuarios podrían efectuar acciones como permitir conexiones por VNC (un protocolo de conexión remota no seguro porque no se cifra), compartir carpetas (con el correspondiente riesgo de pérdida de información) o modificar el directorio de trabajo donde se almacenan las máquinas virtuales.

Las opciones de cifrado y restricción están estrechamente relacionadas ya que si la primera no está activada no se puede poner en marcha la segunda, y si la segunda está activada no se puede desactivar la primera.

Es muy importante almacenar las contraseñas, tanto de cifrado como de restricción, de manera conveniente en un registro seguro, ya que VMware no contempla sistemas de recuperación de claves perdidas.

Esto significa que si se extravían las contraseñas no se podrán iniciar las máquinas virtuales, cambiar su configuración o anular el cifrado. Asimismo, se debe definir claramente qué usuarios tendrán accesos a estas claves, ya que con ellas se les da acceso para manejar sistemas operativos corporativos que en algunos casos pueden ser críticos.

Es muy importante almacenar las contraseñas, tanto de cifrado como de restricción, de manera conveniente en un registro seguro

7.2 Configuración de recursos

Dentro del proceso de creación de una máquina virtual, se recomienda hacer una correcta planificación previa de los recursos de hardware que se van a asignar en función de las características físicas de las que se dispone.

Es importante tener una visión global de toda la infraestructura, es decir, se debe tener en cuenta todas las máquinas virtuales que se van a utilizar en un mismo *host*, así como los recursos que este último necesita para continuar funcionando correctamente.

Por norma general, se recomienda minimizar el número de máquinas virtuales con las que se trabaja en un mismo *host* para evitar el uso innecesario de recursos. Asimismo, una vez se tenga bien definido el entorno de trabajo, se deberán iniciar únicamente las máquinas virtuales que sean completamente imprescindibles. Mantener iniciadas aquellas máquinas virtuales con las que realmente no se está trabajando supone un desperdicio de recursos que va en detrimento del resto de las máquinas virtuales y del propio *host* que podría provocar una ralentización en la ejecución de procesos e incluso el colapso del sistema completo.

Respecto al espacio en disco, es recomendable una asignación dinámica, sobre todo si se trabaja con múltiples máquinas virtuales, para minimizar la parte ocupada y que esta vaya aumentando solamente cuando se necesite.

Para aplicaciones que sean muy sensibles al rendimiento y a la escritura en disco sí se recomienda una asignación permanente del espacio, ajustado a las necesidades del software en ejecución. Existe también una opción de dividir el archivo del disco en varios ficheros de 2 GB, esto sólo es recomendable si se tiene que almacenar el contenido de la máquina virtual en medios de poca capacidad o si hay que transmitirla por red en una localización donde el ancho de banda sea limitado.

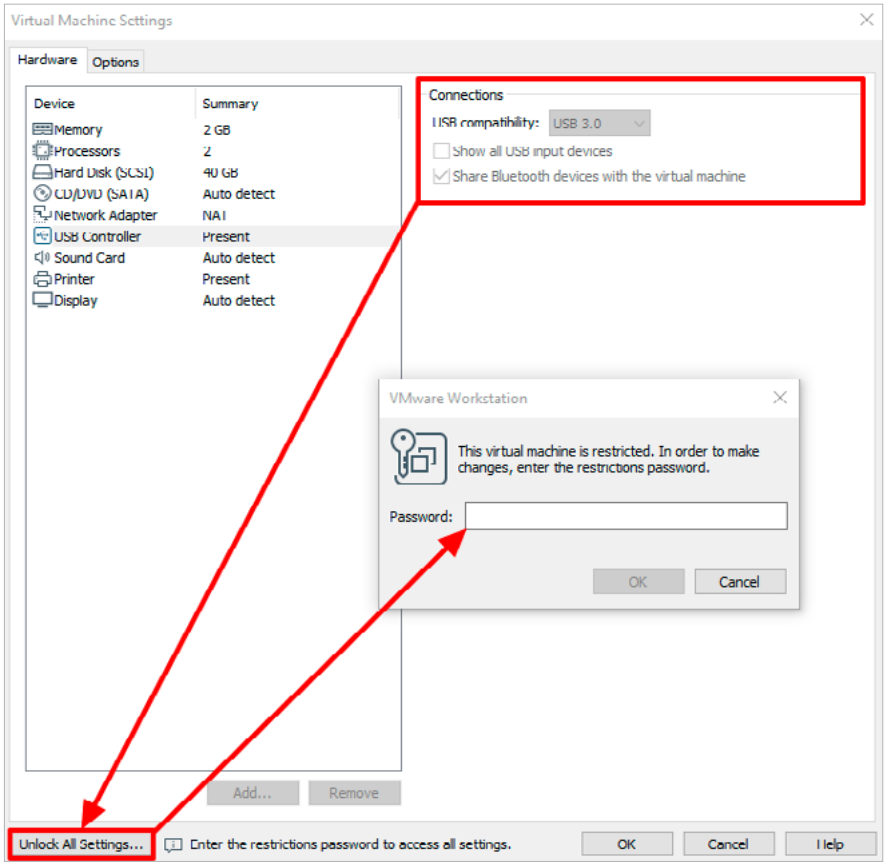
Se recomienda minimizar el número de máquinas virtuales con las que se trabaja en un mismo *host* para evitar el uso innecesario de recursos

Siempre que sea posible, se debería utilizar una herramienta de suma de verificación (CheckSum) para comprobar la integridad de los ficheros, y por supuesto, cifrar el disco virtual.

Por otra parte, **se desaconseja dejar abierta la posibilidad de conectar medios externos como DVD o USB**. Para ello, se cuenta con la posibilidad de restringir las opciones de configuración, como se ha visto en el punto anterior. Si se permite que un usuario pueda utilizar un archivo "iso" como DVD de arranque en un sistema operativo Linux, se da la posibilidad de hacer un chroot que le podría dar acceso y control de la máquina virtual.

De igual modo, permitir el uso de USB puede suponer la sustracción no autorizada de información o la instalación, voluntaria o accidental, de código dañino. La mejor opción, por lo tanto, es inhabilitar el uso de medios externos mediante restricciones y activarlos solo en caso de ser necesarios, volviéndose a inhabilitar después de su uso.

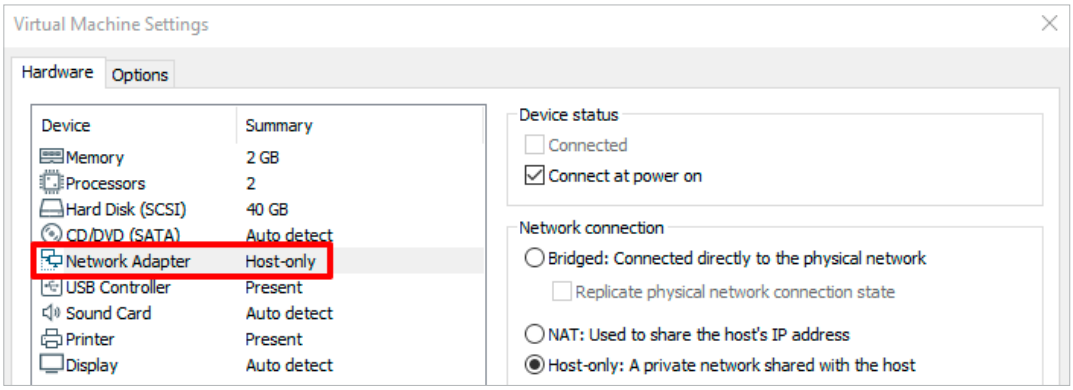
Permitir el uso de USB puede suponer la sustracción no autorizada de información o la instalación, voluntaria o accidental, de código dañino



[Ilustración 14] Recursos hardware protegidos con contraseña.

7.3 Aislamiento y configuración de redes

Las máquinas virtuales cargadas en las versiones Workstation Pro y Player deberían estar aisladas del resto de la red y trabajar, en la medida de lo posible, solo en modo "Host-Only" para no afectar ni verse afectadas por la infraestructura en producción.



[Ilustración 15] Red en modo "Host-only".

No obstante, hay situaciones en las que las máquinas virtuales deben tener presencia en la red, bien sea para interactuar con otros equipos o para descargarse paquetes de instalación desde Internet. Si esta interactuación no es absolutamente necesaria ni constante, es recomendable configurar el dispositivo de red principal para que actúe en modo "Host-Only" y añadir un segundo dispositivo de red con presencia en la red externa el cual será activado únicamente cuando sea necesario, por lo que se recomienda mantener desactivado cuando no esté en uso.

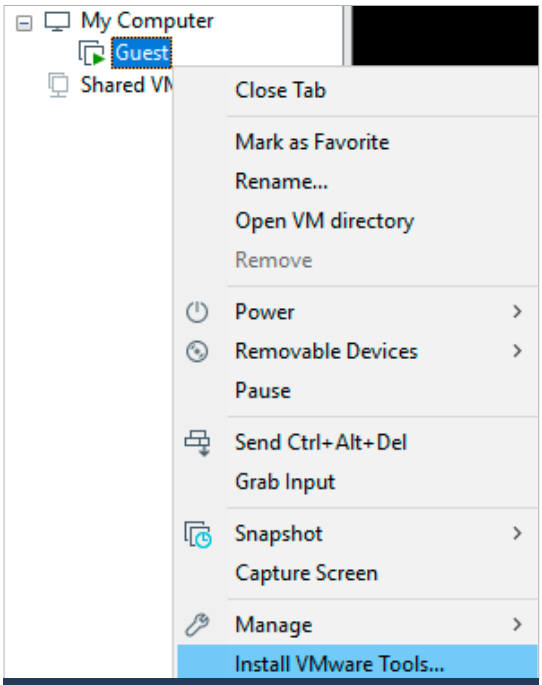
Por lo que respecta a la conexión externa, **es preferible utilizar el modo "NAT" ya que permite un mayor control del tráfico de red,** al funcionar las máquinas virtuales en una red interna creada por el *host*. La configuración en modo "Bridge" es más sencilla de poner en funcionamiento, pero, a parte de un menor control, puede sobrecargar el controlador de red si hay un número elevado de máquinas virtuales usando simultáneamente la misma interfaz física.

7.4 VMware tools

La instalación de las herramientas de VMware no es fundamental para el funcionamiento de las máquinas virtuales. Sin embargo, sí que es muy necesaria si se quieren optar a ciertas características de interactuación entre el *host* y la máquina, como la transferencia de ficheros y texto.

Antes de efectuar la instalación de las mencionadas herramientas, se debe tener en cuenta el sistema operativo de la máquina virtual sobre la que se va a actuar. La práctica totalidad de sistemas Windows no ofrece ningún problema a la hora de ejecutar esta acción, pero por lo que respecta a las distribuciones Linux, no todas lo soportan. Con las últimas versiones de Debian y Ubuntu no suele haber dificultades.

Al instalar las VMware Tools habrá que tener en cuenta que, periódicamente, será necesaria su actualización para optimizar su funcionamiento.



[Ilustración 16] Instalación de VMware Tools.

NOTA:

En este documento se ha utilizado la versión actual de VMware WorkStation Pro v.15, con licenciamiento gratuito 30 días y puede consultar su Guía de compatibilidad de VMware en el siguiente enlace: https://kb.vmware.com/s/article/2129859

7.5 Proteccion de máquinas virtuales en los *hosts*

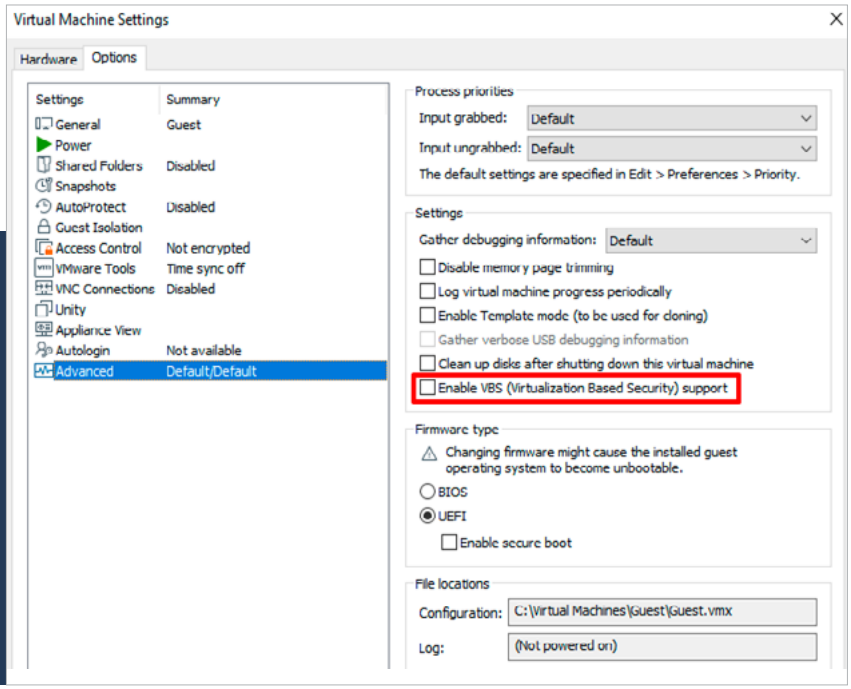
Para aumentar la seguridad en entornos virtuales, se puede habilitar la seguridad basada en la virtualización (VBS) para las máquinas virtuales que ejecutan los últimos sistemas operativos Microsoft Windows 10 y Microsoft Windows Server 2016.

La seguridad basada en la virtualización (VBS) utiliza la tecnología de virtualización de Microsoft Hyper-V para aislar los servicios centrales del sistema operativo Windows en un entorno segregado y virtualizado. Dicho aislamiento proporciona un nivel adicional de protección, ya que hace imposible que los servicios clave en su entorno sean manipulados.

Al habilitar VBS en una máquina virtual, se habilita automáticamente el hardware virtual que Windows requiere para la función VBS. Al habilitar VBS, una variante de Hyper-V comienza en la máquina virtual y Windows comienza a ejecutarse dentro de la partición raíz de Hyper-V.

[Ilustración 17] Opción para habilitar VBS.

En VMware Workstation, puede habilitarse VBS durante la creación de una máquina virtual. Alternativamente, se puede habilitar o deshabilitar VBS para una máquina virtual existente.



NOTA:

Puede obtener más información en el siguiente enlace:
https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.hostclient.doc/GUID-E2A6D2F4-BA66-48EC-98D5-35D8E2C3B192.html

7.6 Transferencia de ficheros y texto

Una vez instalas las herramientas de VMware, se pueden utilizar de forma conjunta el portapapeles entre el *host* y las máquinas virtuales, así como transferir determinados tipos de ficheros de manera sencilla.

Para esto último existen varios métodos, por lo que se deberá escoger uno o varios en función de las necesidades de cada sistema.

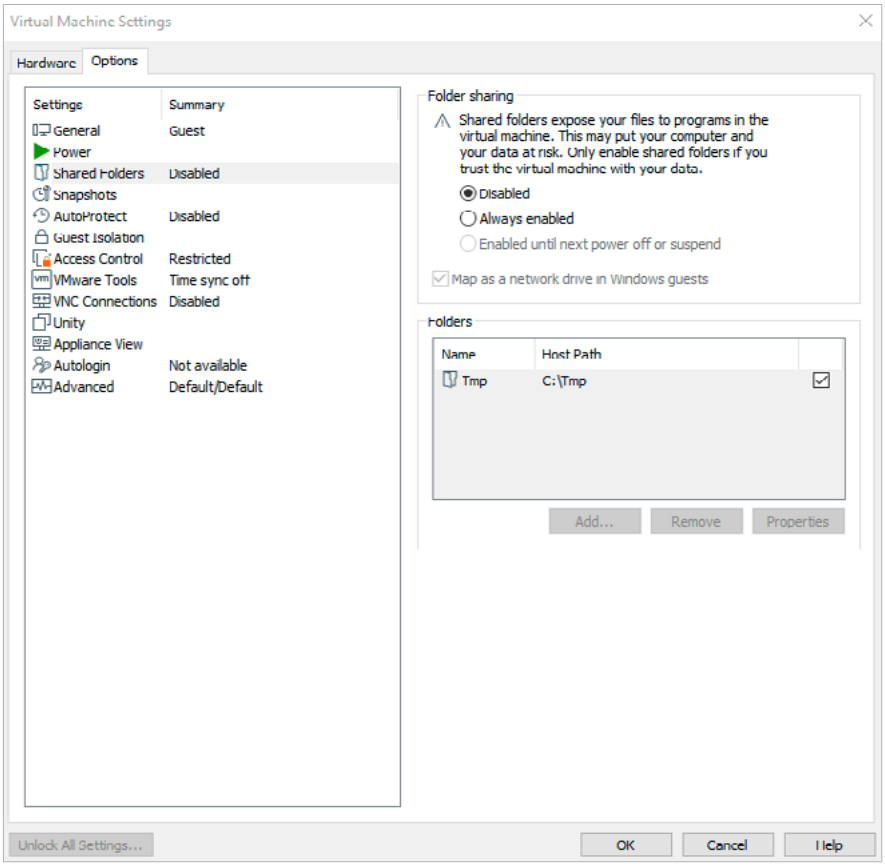
El primero que se puede mencionar es "drag and drop", es decir, arrastrar los ficheros desde el equipo anfitrión hasta la máquina virtual o viceversa. Es sencillo de usar, pero puede ser problemático por las limitaciones de tamaño y formato para algunos ficheros.

También se puede optar por la utilización de la característica de "copiar y pegar". Aparte de una limitación en el formato y tamaño de ficheros, como sucedía en el caso anterior, presenta el inconveniente de que no funciona entre máquinas virtuales.

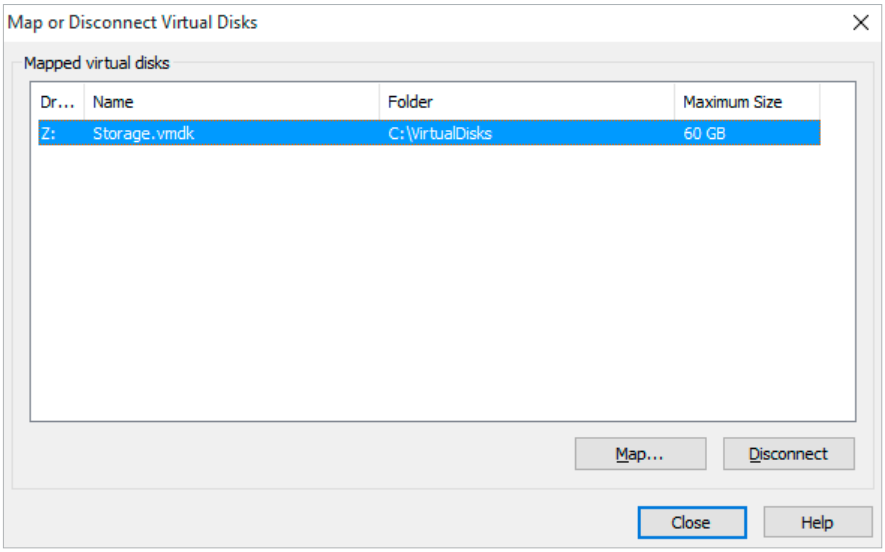
En tercer lugar, existe la opción de compartir carpetas. Esta solución es más compleja de configurar que las anteriores, pero permite una desactivación sencilla cuando no esté en uso. Tiene como gran inconveniente la posibilidad de que se corrompan los ficheros si son utilizados por diferentes máquinas de manera simultánea.

Por último, existe la opción de que el *host* mapee un disco duro virtual en el que almacenar los ficheros. Cuenta con la ventaja de que permite usar un punto de encuentro entre varias máquinas virtuales y el *host* sin salir de la infraestructura de virtualización. Si se opta por este método, se recomienda cifrar el disco duro virtual.

[Ilustración 18] Compartir una carpeta del *host* con uno de los *guest*.



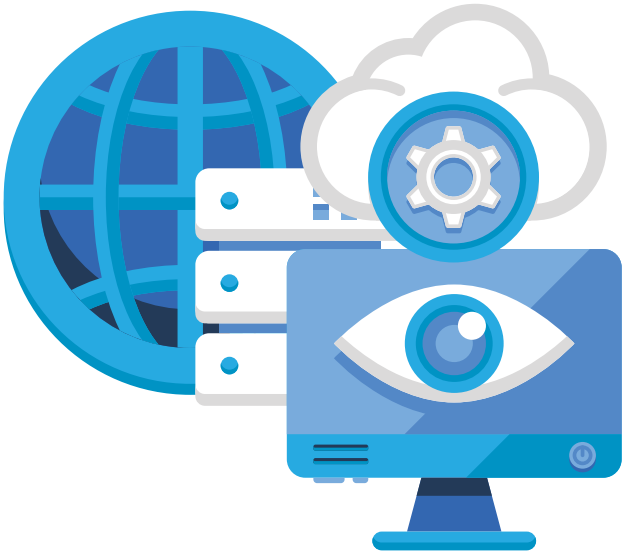
[Ilustración 19] Fichero de disco duro virtual mapeado en el *host*.



Siempre que sea posible se debe trabajar en local. Pero si fuera necesario compartir ficheros con usuarios o equipos externos, es altamente recomendable utilizar un sistema que provea de un método de validación sólido, como los basados en Servicios de Directorio (por ejemplo, Active Directory de Windows).

7.7 Snapshots de las máquinas virtuales

Como en el resto de sistemas de virtualización, se pueden realizar puntos de control o estado de las máquinas virtuales. Dicha opción no debe utilizarse como un sistema de copias de seguridad de las máquinas virtuales, ya que VMware los trata como un registro donde almacena los cambios del disco duro virtual primario, creando un nuevo disco de marcador de posición a partir del momento de su creación.



NOTA:

Puede ampliar más información al respecto en el siguiente enlace del fabricante:
Best practices for using snapshots in the vSphere environment

8. Buenas prácticas VirtualBox

Como en los demás hipervisores, las actuaciones de protección y, en general, las buenas prácticas deben estar orientadas primero al anfitrión y después a cada una de las máquinas virtuales alojadas.

A continuación, se listan algunas de las consideraciones generales que deben atenderse:

a. **Mantener el software de virtualización actualizado.** Para ello se puede habilitar la opción en las preferencias de VirtualBox o hacer una comprobación manual en "Archivo" y luego en "Comprobar actualizaciones…".

b. **Mantener actualizadas las "Guest Additions" en todas las máquinas virtuales.** Del mismo modo, se deben actualizar los "Extension Packs".

c. **No se debe ejecutar VirtualBox con privilegios de administrador,** salvo en acciones requeridas que no pueden realizarse sin privilegios y, en general se deben mantener los permisos más restrictivos posibles.

d. **Restringir las conexiones de red de tal forma que el *host* y los *guest* tengan la conectividad mínima requerida.** De igual forma, dicha conexión se debe asegurar con un sistema de cortafuegos en cada uno de los equipos instalados.

e. **Auditar los registros de seguridad de forma periódica para detectar comportamientos anómalos y crear una línea base que permita la comparación en caso de necesidad.**

Las actuaciones de protección y, en general, las buenas prácticas deben estar orientadas primero al anfitrión y después a cada una de las máquinas virtuales alojadas

f. **Utilizar únicamente la web oficial de Oracle como fuente de los instalables.**

g. **En entornos tipo sandbox-antimalware, evitar la instalación de las "Guest Additions",** ya que permiten la comunicación con el *host* y se convierten en un posible vector de infección.

h. **No crear instantáneas (*snapshots*) que no sean necesarias y eliminarlas de forma segura llegado el caso.**

i. **Utilizar con extremo cuidado la utilización de dispositivos de almacenamiento USB, CD o DVD ya que permiten la entrada directa de software en las máquinas virtuales.** Especialmente, los primeros son un vector de entrada habitual para código dañino.

j. **Evitar el gestor del hipervisor en modo HTML porque no utiliza una conexión segura.** Es preferible usar la aplicación cliente-servidor "Oracle VM VirtualBox Administrator" (aplicación de escritorio), que es más segura.

NOTA:

Web oficiales de VirtualBox para la descarga de sus productos:

- https://www.oracle.com/virtualization/virtualbox/

- https://www.virtualbox.org/

8.1 Cifrado de máquinas virtuales

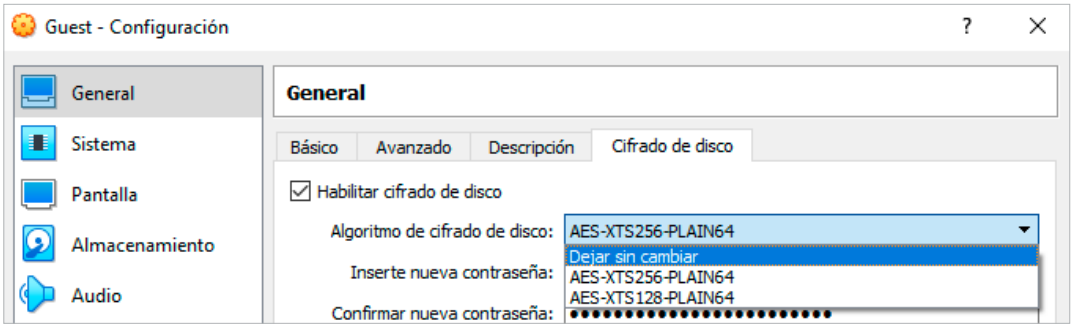
Por lo que respecta al cifrado de las máquinas virtuales, este es transparente al *guest* y puede ser aplicado al disco duro y a cualquiera de sus formatos disponibles (VDI, VHD, VMDK).

VirtualBox, a partir de la versión 5, ya incluía como característica de seguridad el cifrado de los discos duros de las máquinas virtuales, sin embargo, es necesario instalar un paquete de extensión para poder utilizar la característica en la configuración general de las máquinas virtuales.

Durante la creación de la máquina con el asistente gráfico, no se puede configurar el cifrado, por lo que si el equipo es crítico es conveniente no añadir el disco hasta que no se haya activado el cifrado con la contraseña. Además, debe considerarse que el cifrado agrega carga de trabajo al *host* y que las máquinas creadas con este método en VirtualBox no se pueden transportar a otros sistemas de virtualización si antes no se procede a su descifrado.En VMware Workstation, puede habilitarse VBS durante la creación de una máquina virtual. Alternativamente, se puede habilitar o deshabilitar VBS para una máquina virtual existente.

NOTA:

Puede elegir el algoritmo más seguro en función de la importancia y/o criticidad del sistema



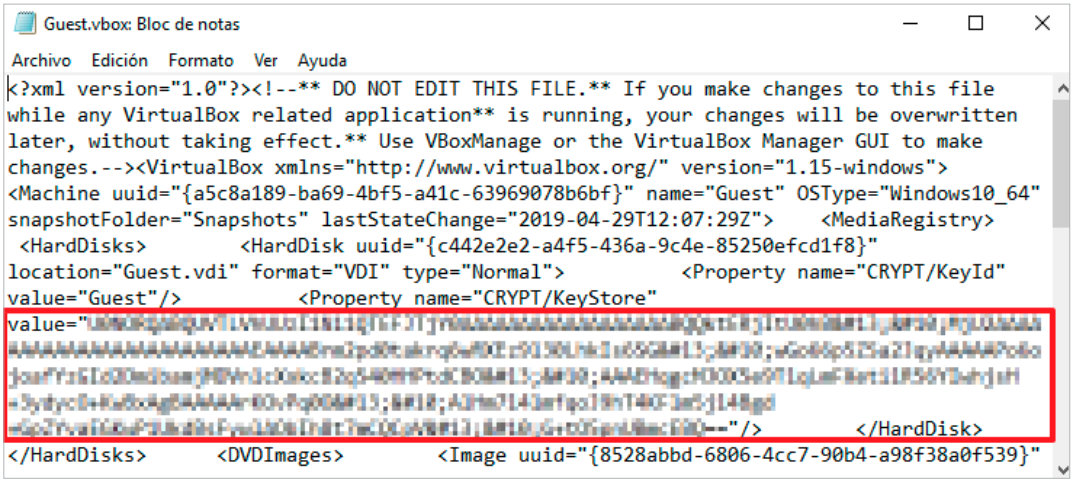
[Ilustración 20] Activación del cifrado en máquina virtual.

Es imprescindible resaltar que la pérdida de la contraseña implica la pérdida de los discos duros de forma irremediable. La clave se guarda en el fichero de configuración de la máquina virtual, por lo que es conveniente disponer de una copia de seguridad del mismo.

El fichero de definición de la máquina, en el que se incluye la codificación de la contraseña de cifrado en texto plano, tiene que ser protegido por medio de permisos NTFS, y debe hacerse antes de crear la contraseña para evitar filtraciones en el intervalo de tiempo de exposición.

La protección por cifrado de Windows EFS no es una alternativa, ya que se revierte el cifrado en el primer arranque del *guest* en VirtualBox.

Es imprescindible resaltar que la pérdida de la contraseña implica la pérdida de los discos duros de forma irremediable



[Ilustración 21] Fichero de configuración de máquina virtual.

Por otra parte, **se deben planificar correctamente la asignación de permisos a la carpeta donde se guarde la definición de las máquinas virtuales y los discos duros para evitar accesos no autorizados** (por accidente o como resultado de un ataque). Deben, al menos, configurarse los siguientes permisos:.

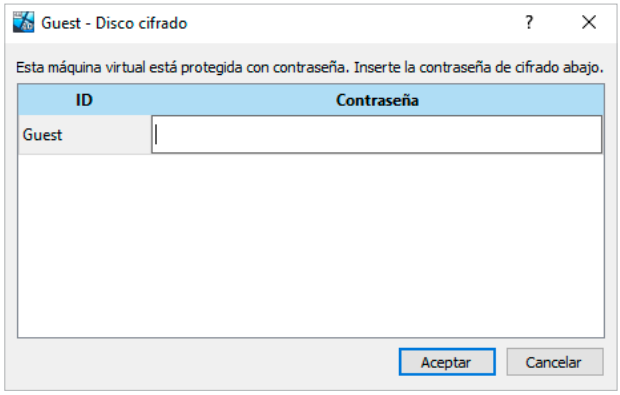
[Tabla 5] Permisos mínimos para directorios de máquinas virtuales y discos duros.

CUENTA	PERMISOS	APLICAR A
Administradores	Control total	Esta carpeta, subcarpetas y archivos
System (Sistema)	Control total	Esta carpeta, subcarpetas y archivos
Creator owner (Propietario creador)	Control total	Solo subcarpetas y archivos

NOTA:
La inclusión de otros usuarios o grupos deberá ser valorada en cada caso

Con los permisos de la tabla superior cada usuario puede generar sus propias máquinas virtuales, pero no podrá acceder a los *guest* creados por otros. Cualquier administrador del *host* puede acceder a todas las máquinas.

Cuando se inicia una máquina virtual que tiene el disco protegido con contraseña, esta será requerida en cada inicio de la máquina virtual. **Al utilizar el cifrado de disco aparecen algunas limitaciones, por lo que se considera conveniente consultar el manual antes de utilizar esta funcionalidad.** Valga como ejemplo mencionar que es incompatible con *snapshots* o que la contraseña se carga en memoria y se transfiere en plano durante la utilización de la máquina virtual.



[Ilustración 22] Ventana de petición de clave de cifrado.

El cifrado de VirtualBox es compatible con el cifrado del disco físico por medio de *BitLocker*, por lo que para entornos críticos deberían utilizarse ambos, además de establecer medidas adicionales para la protección de la contraseña.

8.2 Aislamiento y configuración de redes

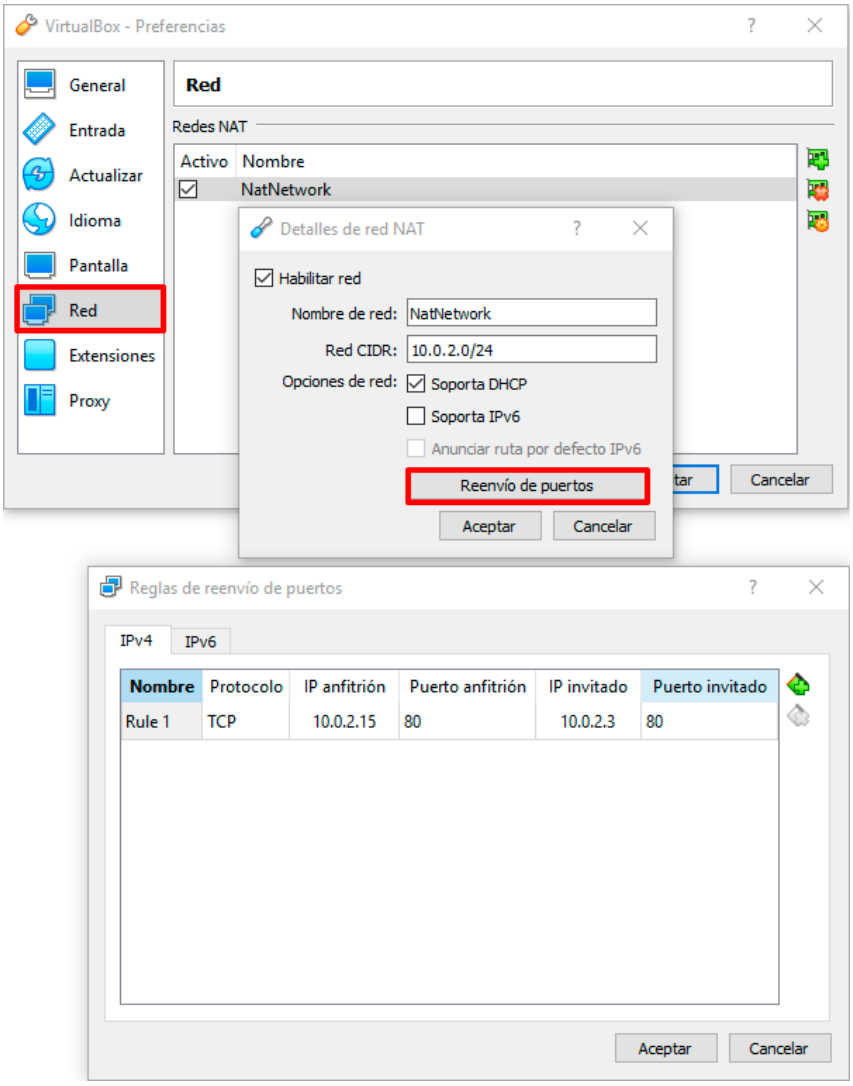
Por lo que se refiere a la conectividad en VirtualBox, los dispositivos de red virtuales de los invitados pueden estar configurados en uno de los siguientes estados:

- **No conectado.**
- **NAT.**
- **Red NAT.**
- **Adaptador puente.**
- **Red interna.**
- **Adaptador sólo-anfitrión.**
- **Controlador genérico.**
- **Avanzadas.**

El valor por defecto que se asigna a una nueva creación es "NAT", por lo que el hipervisor se comporta como un router (dispositivo de capa 3 del modelo OSI). Esto le confiere al invitado capacidades de conexión a la red física del anfitrión, pero oculta las direcciones IP y MAC a los equipos externos.

El cortafuegos del *host* puede proporcionar protección a las máquinas virtuales alojadas. Esto impide la publicación de servicios de los servidores alojados como *guest*, excepto de aquel para el que se ha seleccionado esta opción. Se puede considerar como una ventaja de seguridad, pero también como un impedimento si lo que se requiere es la conectividad de varios invitados desde la red.

Cuando se requiera la publicación de servidores, se puede hacer que VirtualBox trabaje como un enrutador con todas las funcionalidades posibles del mismo. Para ello se debe crear una "Red NAT" a la que luego se podrán conectar adaptadores virtuales de los invitados.



[Ilustración 23] Creación de una "Red NAT" con la publicación del puerto 80.

La opción "Adaptador puente" permite la conexión directa de los invitados a través de la conexión física, que se comporta como un conmutador (capa 2 del modelo OSI). Es una configuración cómoda para conseguir conectividad externa, pero que aumenta de forma considerable la superficie expuesta, por lo que debe ser protegida cada máquina virtual por sus propios medios (producto para evitar código dañino, cortafuegos, IDS, etc.).

"Red interna" permite conectar las máquinas virtuales entre ellas a los equipos alojados que tengan seleccionada esta opción y que además coincidan con el mismo identificador de la red. Se pueden, por tanto, crear redes internas distintas. Si se requiere probar equipos como si estuviesen en red, esta es una opción válida, pero se debe crear una red interna propia y solo conectar los equipos indispensables.

Si la visibilidad de red que se necesita es con el *host*, se debe seleccionar la opción **"Adaptador sólo anfitrión"**, que unirá ambos equipos, anfitrión e invitado.

"Controlador genérico" no se utiliza habitualmente. Permite presentar un driver de red incluido en VirtualBox o en un "Extensión Pack".

Cuando se activa **"Avanzadas"**, en cada una de las opciones se habilita la gestión de la dirección MAC, la activación del modo promiscuo, el tipo de adaptador y el reenvío de puertos (cada uno según aplique).

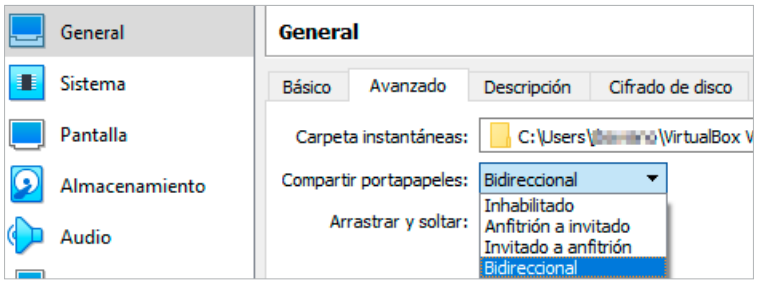
Como en cualquier otro hipervisor, **se recomienda la configuración "No conectado" siempre que sea posible e ir escalando desde la más baja conectividad a una mayor.** Por ejemplo, pasar del "Adaptador sólo-anfitrión", a la red interna, luego a la NAT, después a la red NAT, etc.

En VirtualBox se pueden crear hasta cuatro tarjetas de red virtuales por *guest* y en todas se deben tomar las mismas precauciones siendo importante considerar que no se deben definir tarjetas que no vayan a ser utilizadas.

8.3 Compartición portapapeles

La herramienta de portapapeles compartido presenta una funcionalidad habitualmente interesante para el trabajo rápido y cómodo, pero podría ser un punto de intercambio de código dañino. Funciona independiente del tipo de red que se utilice y puede funcionar en ambos sentidos o en uno de ellos, entre el *guest* y el *host* o viceversa. Esta herramienta requiere que el invitado tenga instaladas las "Guest Additions" de VirtualBox.

La herramienta de portapapeles compartido presenta una funcionalidad habitualmente interesante pero podría ser un punto de intercambio de código dañino



[Ilustración 24] Configuración del portapapeles.

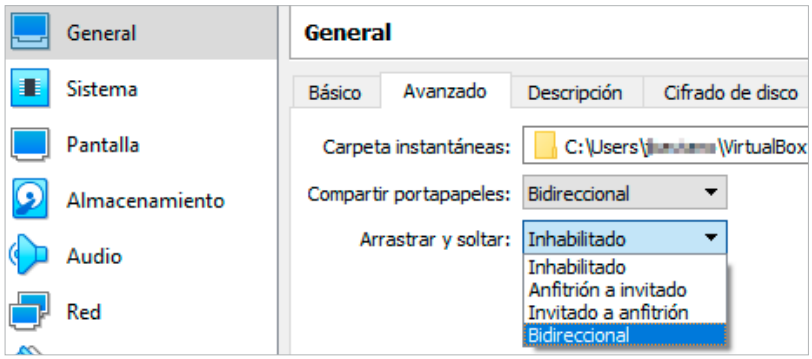
Como norma, esta funcionalidad debe permanecer inhabilitada, ya que un potencial atacante podría obtener, por ejemplo, acceso a información sensible que se alojase en el portapapeles del *host* al haber conseguido previamente la entrada a un *guest* no protegido de forma adecuada. Si se requiere por motivos de fuerza mayor, debería ser activado temporalmente sólo por el período indispensable.

NOTA:
En la configuración de la máquina virtual en VirtualBox, puede seleccionar el modo de funcionamiento del portapapeles (por defecto está inhabilitado)

8.4 Arrastrar y soltar

Esta funcionalidad, conocida en inglés como "drag & drop", permite arrastrar y dejar un objeto (fichero, carpeta o texto plano) en ambos sentidos, entre el *guest* y el *host* o viceversa. Esta herramienta requiere que el invitado tenga instaladas las "Guest Additions" de VirtualBox.

Las posibilidades de elección de configuración son iguales a las del portapapeles compartido, así como la opción por defecto, "Inhabilitado", y la recomendación de mantenerlo en ese estado. Si se requiere su uso, debería ser activado el tiempo estrictamente necesario.



[Ilustración 25] Configuración de "Arrastrar y soltar".

NOTA:

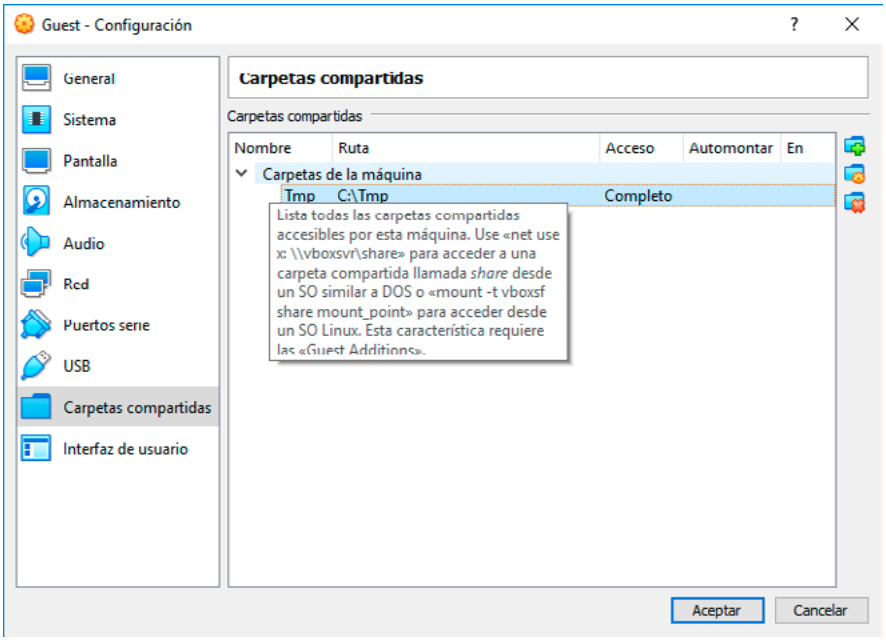
En la configuración de la máquina virtual en VirtualBox, puede seleccionar el modo de funcionamiento del portapapeles (por defecto está inhabilitado).

8.5 Carpetas compartidas

En este caso el término "carpeta compartida" no hace referencia al recurso de red creado por el sistema operativo, sino a la característica de VirtualBox que se hace disponible con la instalación de las "Guest Additions" en el invitado. Esto permite poner a disposición del invitado un directorio alojado en el anfitrión, al que podrá acceder por medio de las rutas de acceso de convención de nomenclatura universal (UNC), que se usan para acceder a los recursos de red.

Para la descripción de UNC se puede ver el siguiente enlace:

https://docs.microsoft.com/eses/dotnet/standard/io/file-path-formats#unc-paths



[Ilustración 26] Configuración de carpetas compartidas.

Por defecto, VirtualBox no incluye ninguna carpeta compartida. La decisión de crearlas debe ser meditada, adoptando las máximas medidas de seguridad para proteger la información manejada.

Una vez definida una carpeta compartida, esta se comporta como un recurso de red. Se publica con el nombre dado durante la creación y con la nomenclatura "vboxsvr" para el servidor. Si se opta por ejecutar la instrucción "Automontar" en Windows, se montará la carpeta de forma inmediata y en Linux se montará del mismo modo en "/media" con el prefijo "sf_".

Se desaconseja su utilización ya que se incrementa la superficie de exposición (por ejemplo, la mayor parte del ransomware cifraría la unidad con letra de Windows). Para conocer más sobre la protección contra el ransomware se puede consultar el Informe de amenazas CCN-CERT IA-11/18: Medidas de seguridad contra ransomware y la Guía de Buenas Prácticas asociada CCN-CERT BP/04 Ransomware en el sitio web del CCN-CERT.

En las últimas versiones de VirtualBox es posible definir el punto de montaje asegurando de este modo que dicho punto es diferente al estándar y pudiendo aplicar medidas de seguridad adicionales sobre el punto de montaje.

Como se ha señalado en anteriores epígrafes de esta guía, **compartir información,** por el medio que sea, **siempre se considera un incremento de la superficie expuesta a posibles ataques,** pero que en ocasiones es necesario.

Por ello, se deben tomar las medidas adecuadas, ya que **un atacante que acceda al *guest* tendría acceso a los recursos compartidos.** Entre otras acciones, se puede establecer una limitación del tiempo de compartición (cuando se apaga la máquina virtual el recurso compartido desaparece), minimizar la información publicada, combinar los permisos disponibles en VirtualBox con los de NTFS del *host*, haciéndolos lo más restrictivos posibles, y, en entornos críticos, activar la auditoría de ficheros. Asimismo, aunque no evita la fuga de información, se puede poner el permiso solo lectura (el valor por defecto es el de lectura-escritura).

En las últimas versiones de VirtualBox es posible definir el punto de montaje asegurando de este modo que dicho punto es diferente al estándar

8.6 Instantáneas en VirtualBox

Las máquinas virtuales en VirtualBox están compuestas por una serie de archivos en los que se almacena la información sobre discos duros, características y estado actual de la máquina.

Cada disco duro virtual se corresponde con un archivo con la extensión ".vdi", ".vhd" o ".vdmk" (dependiendo del tipo de disco seleccionado en la creación de la máquina virtual). Los parámetros de configuración se almacenan en un archivo XML con el nombre de la máquina en cuestión. En versiones de VirtualBox posteriores a la 4.0 este archivo tiene la extensión ".vbox", lo que permite arrancar la máquina con hacer doble clic en él o mediante un acceso directo. Si en lugar de apagar se decidió guardar el estado de una máquina existirá también un archivo ".sav", que será eliminado en el momento en que esta vuelva a estar activa.

Las instantáneas (*snapshots*) son una forma de guardar el estado de la máquina virtual en un momento determinado, a partir del cual todo cambio que se haga en ella será almacenado en un nuevo archivo ".vdi" por cada disco duro existente, manteniendo los originales intactos. Sucesivas instantáneas repetirán este proceso, pudiendo aumentar considerablemente el espacio que ocupa la máquina en el disco del *host* por lo que es necesario controlar su creación y gestionar tanto el número de ellas, así como su mantenimiento en el tiempo.

Las instantáneas (*snapshots*) son una forma de guardar el estado de la máquina virtual en un momento determinado

9. Máquina segura de navegación

Con el objetivo de complementar el propósito de esta guía, se ha implementado una máquina virtual, configurada de manera segura, que se encuentra orientada para la navegación web. De esta manera, se garantiza la independencia y aislamiento entre máquina virtual y equipo anfitrión.

El sistema operativo utilizado para la máquina virtual es CentOS 7, que cuenta con licenciamiento gratuito y la guía de configuración segura aplicada es la "CCN-STIC 619 Configuración segura de CentOS 7 (Cliente independiente)".

A continuación se indican los datos necesarios para poder descargar la máquina virtual segura de navegación:

Enlace:
https://loreto.ccn-cert.cni.es/index.php/s/FpniMgp5Hx8Ml66

Clave para la descarga: virtual

SHA256
49C16F00E00C91EEE30D634A1BFB4035E69C2ED4017D0DF8B5BFD7B635E61892

SHA1
209766E9771E375322F6A4EE3742A46C2DED5D0C

La máquina virtual segura de navegación, ha sido concebida para poder ser utilizada con productos software de virtualización (hipervisores) que cuentan con licenciamiento gratuito como por ejemplo:

Oracle VirtualBox: www.virtualbox.org/wiki/Downloads

VMware Workstation Player:
www.vmware.com/products/workstation-player.html

10. Decálogo de recomendaciones

A continuación, se presenta un decálogo de buenas prácticas genéricas para todo tipo de hipervisores.

Decálogo de seguridad en máquinas virtuales

1. **Mantener el sistema actualizado:** tener instaladas en el sistema operativo las últimas actualizaciones de seguridad y contar con la última versión disponible del programa de virtualización reduce drásticamente la exposición ante vectores de ataque tratados por los fabricantes en los parches de actualización.

2. **Segregación física de la red:** si es posible, tener al menos un adaptador de red exclusivo para la infraestructura de virtualización para mantener separado el flujo de red de las máquinas virtuales y el equipo físico que las contiene. En el caso de ataque a la red de la máquina física, el atacante no verá el flujo de red de las máquinas virtuales manteniéndolas seguras por esta separación de adaptadores.

3. **Segregación de roles y permisos:** es aconsejable crear un grupo de seguridad específico para el uso de las máquinas virtuales, donde a los usuarios miembros se les restringirá el empleo del programa de virtualización sin posibilidad de realizar acciones que requieran elevación de privilegios no relacionadas con el uso de las máquinas virtuales. Del mismo modo se recomienda crear un directorio para alojar los archivos de las máquinas virtuales, donde se apliquen permisos posteriormente, mediante ACLs.

4. **Planificar el sistema virtualizado:** hacer un esquema previo de lo que será la infraestructura de virtualización ayuda a la implementación del mismo. En dicha planificación se debe tener en cuenta dimensionar la creación de máquinas virtuales a las necesidades reales y a los recursos de hardware disponibles en el *host*, poniendo especial interés en el tipo de discos a seleccionar según los servicios prestados por cada máquina virtual.

5. **Gestión de los recursos:** los recursos de los hipervisores no son ilimitados. Para liberar dichos recursos es recomendable mantener activas solamente las máquinas virtuales imprescindibles. Además, implementar una política de creación de "snapshots/checkpoints" de las máquinas virtuales también refuerza dicha gestión, ya que implican una degradación de los *host*. Esta creación se debe controlar, tanto en el número total que se crean, como en el tiempo a conservarlos en los hipervisores.

6. **Protección de la información:** para mantener seguros los datos críticos alojados en los medios virtualizados es conveniente cifrar los ficheros de máquinas virtuales, instantáneas y discos duros virtuales destinados al almacenamiento de la plataforma de virtualización. Al igual que cifrar los medios de almacenamiento externos que contengan ficheros de virtualización de respaldo y custodiarlos convenientemente. Del mismo modo, cifrar y mantener convenientemente custodiados los libros de contraseñas para prevenir una posible exfiltración.

7. **Implementación de cortafuegos:** asegurar con una solución de cortafuegos, ya sea físico o lógico, para evitar el código dañino y los intentos de ataque hacia todos los sistemas operativos invitados.

8. **Implementar una política de copias de seguridad:** para evitar pérdidas de datos o la funcionalidad de las máquinas virtuales en caso de emergencia, se recomienda establecer una política de copias de seguridad que contengan una copia completa de dichas máquinas virtuales. Estas copias de seguridad se deberán realizar cada cierto tiempo o en momentos críticos con la finalidad de poder recuperar información o incluso la funcionalidad de dicha máquina. Se deberá tener en cuenta que las copias de seguridad tienen un tamaño elevado y debido a esto, sería recomendable mantener pocas copias de seguridad completas y hacer uso de copias incrementales.

9. **Documentar la plataforma de virtualización:** mantener el sistema documentado ayuda a identificar rápidamente las máquinas en desuso y posibilita la liberación de recursos y obtener una mejor gestión del sistema. Es aconsejable actualizar dicha documentación con cada cambio relevante realizado en el sistema.

10. **Instalar los agentes de hipervisor:** valorar la instalación de dichos añadidos de software tipo "Guest Additions" o "Tools", ya que la implementación de los mismos mejora el rendimiento de las máquinas virtuales y agrega funcionalidades como el portapapeles compartido. En caso de hacerlo, se recomienda mantenerlos actualizados al igual que el software de virtualización.

11. Glosario

A continuación, se presenta un decálogo de buenas prácticas genéricas para todo tipo de hipervisores.

TÉRMINO	DESCRIPCIÓN
Virtualización	Es la abstracción de los recursos de un servidor físico, de forma que se crea una capa entre el hardware de la máquina física (*host* o hipervisor) y el sistema operativo de la máquina virtual (invitado o *guest*).
Invitado o *Guest*	Es el software que simula a un equipo y puede ejecutar programas como si fuese un equipo físico y real.
Máquina Virtual o Virtual Machine (VM)	También denominado así al "Invitado" o "*Guest*".
Hipervisor, Anfitrión o *Host*	Es la plataforma física que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en una misma computadora.
Instantánea, *Snapshot* o *Checkpoint*	Representa el estado de una máquina virtual en el momento en que fue tomado. Básicamente, es una foto de la máquina virtual en un momento dado. Este no debe tomarse como un backup o copia de seguridad de la máquina virtual.
Conmutador o Switch	Es un dispositivo de interconexión de redes entre otros dispositivos o equipos.
Red de Área Local Virtual (VLAN)	Es un método que permite crear redes que lógicamente son independientes, aunque estas se encuentren dentro de una misma red física.

CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es


cn-cert
centro criptológico nacional
CCN
centro criptológico nacional