centro criptológico nacional

Norma de Seguridad de las TIC
CCN-STIC-220

ARQUITECTURAS VIRTUALES

Julio 2020

MINISTERIO DE DEFENSA

Edita:

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.07.24 15:35:44 +02'00'

NIPO: 083-20-179-3

Fecha de Edición: julio de 2020
Sidertia Solutions ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

julio de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

ANEXOS

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.

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

El actual uso de tecnologías emergentes que permiten la virtualización de los sistemas de las Tecnologías de la Información y la Comunicación (TIC), en adelante Sistemas, se ha hecho crítica con la extensión del empleo de dichas tecnologías a todos los ámbitos.

Las amenazas asociadas a un sistema, que pueden afectar a la confidencialidad, integridad y disponibilidad de la información manejada, o a la propia integridad y disponibilidad del sistema, son tenidas en cuenta a la hora de establecer los requisitos de seguridad mínimos, de tal manera, que las medidas de protección que se implementan tienen por objeto hacer frente a dichas amenazas reduciendo la superficie de exposición y minimizando el impacto de estas.

La seguridad se tratará desde la fase de diseño del sistema, donde se definirán las salvaguardas a implementar, permitiendo de esta manera que el análisis y gestión de riesgos de seguridad estén presentes en el proceso de desarrollo del sistema.

3. OBJETO

El objeto de esta norma es establecer las directrices para tener en cuenta cuando se requiere la implementación de sistemas y cuya instalación se basa en una arquitectura virtual.

El presente documento proporciona los aspectos generales de aplicación, recomendaciones de seguridad y buenas prácticas, necesarias para la prevención de los riesgos, amenazas, y vulnerabilidades de seguridad a las que están expuestas las arquitecturas virtuales sobre las que se implementa un Sistema.

4. ALCANCE

El propósito del presente documento es establecer un conjunto de directrices generales de seguridad que se deberán tener en cuenta cuando se implemente una arquitectura de virtualización. Además, se incluyen en esta norma una serie de recomendaciones generales para la protección de los datos y las comunicaciones que almacenan los sistemas basados en una arquitectura virtual.

5. DESCRIPCIÓN DEL USO DE ESTA GUÍA

Para entender bien esta norma de directrices de seguridad es conveniente explicar el proceso de refuerzo de seguridad al que debe estar sometido un sistema que haya sido virtualizado. Dicho proceso estará basado en las recomendaciones de seguridad establecidas por los diferentes fabricantes que ofrecen la posibilidad de virtualizar un sistema con el uso de su tecnología.

En función del fabricante, la metodología de aplicación de las recomendaciones de seguridad establecidas en el presente documento podrá variar, es por ello, que las recomendaciones de seguridad están dirigidas a la tecnología de virtualización en sí y no a un fabricante determinado, aunque para ellos se cuenten como base los principales proveedores de tecnologías de virtualización.

5.1 AVISOS IMPORTANTES A LOS USUARIOS DE ESTA GUÍA

La norma ha sido desarrollada con el objetivo de dotar a las infraestructuras virtuales con la seguridad adecuada dependiendo del entorno sobre el que se aplique, teniendo en consideración el ámbito y nivel de seguridad de la información a tratar. Es posible que algunas de las funcionalidades esperadas hayan sido desactivadas y, por lo tanto, pueda ser necesario aplicar acciones adicionales para habilitar servicios, roles o características deseadas.

El espíritu de esta norma no está dirigido a remplazar políticas de seguridad consolidadas y probadas de las organizaciones, sino a servir como línea base de seguridad. Esta línea deberá ser adaptada a las necesidades propias de cada organización.

6. APLICACIÓN DEL DESARROLLO NORMATIVO

El desarrollo normativo de la Política STIC, se desglosa en procedimientos, normas, instrucciones técnicas y guías. Desde este punto de vista, la implementación de una arquitectura virtual para la ejecución de múltiples sistemas deberá tener en cuenta el cumplimiento de los siguientes documentos dependiendo de si se maneja información clasificada o no:

a) Esta norma de seguridad CCN-STIC 220.

b) En caso de manejo de información clasificada, la instrucción técnica de seguridad de las TIC “CCN-STIC 301 Medidas de Seguridad de las TIC a Implementar en Sistemas Clasificados”.

c) En caso de manejo de información clasificada, la instrucción técnica de seguridad de las TIC “CCN-STIC 302 Interconexión de CIS”.

d) Por su parte, a los sistemas del Sector Público que no traten información clasificada les será de aplicación el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS), de conformidad con lo dispuesto en la Ley 40/2015 de Régimen Jurídico del Sector Público y atendiendo a lo señalado en la Ley 39/2019, de Procedimiento Administrativo Común de las Administraciones Públicas.

e) Las guías de seguridad generales y específicas del sistema, fabricante y versión a instalar correspondientes al tipo de información que maneja la infraestructura.

7. NUBES PRIVADAS Y CENTROS DE DATOS VIRTUALES

Antes de entrar en los detalles sobre tecnologías de virtualización, hiperconvergencia y medidas de seguridad de las arquitecturas virtuales, es importante y recomendable recordar algunos conceptos básicos que mejoren el entendimiento claro de lo que son los centros de datos virtuales y cómo el desarrollo de nubes privadas ha permitido la adopción de tecnologías escalables y elásticas en las infraestructuras propias de cada organización.

Los centros de datos virtuales son una realidad hoy en día, tanto si se habla de virtualización tradicional como de hiperconvergencia. No solo se trata de un conjunto de máquinas virtuales ejecutándose y compartiendo recursos en un único servidor físico, sino que en la mayoría de los casos se hace referencia a grandes centros de datos completamente virtualizados y con ciclos de vida de los servicios completamente automatizados y monitorizados: desde el despliegue de nuevos servicios, su mantenimiento en producción y su retirada final.

Por otro lado, el término de computación en la nube se define como un modelo para permitir un acceso sencillo, universal y bajo demanda a través de una red a un conjunto de recursos de computación compartidos, configurables que pueden ser rápidamente aprovisionados y puestos en producción con un esfuerzo de mantenimiento mínimo o sin interacción del proveedor del servicio. Esta es la definición oficial que aporta el Instituto Nacional de Estándares y Tecnología (NIST). Puede profundizar en esta definición en el siguiente enlace: https://csrc.nist.gov/publications/detail/sp/800-145/final

Es importante destacar la última parte de la definición: "**rápidamente aprovisionados y puestos en producción con un esfuerzo de mantenimiento mínimo o sin interacción del proveedor** ", ya que de eso se trata, precisamente, la tecnología hiperconvergente.

Las principales características de un modelo de computación en la nube (ya sea privada o pública), son las siguientes:

a) **Autoservicio bajo demanda.** Los usuarios pueden aprovisionar capacidad de computación como tiempo de procesamiento, almacenamiento en red y transferencia de datos, automáticamente sin requerir intervención humana.

b) **Acceso desde múltiples plataformas.** Las capacidades del sistema están accesibles a través de la red desde una variedad de plataformas y dispositivos.

c) **Agrupamiento de recursos.** Los recursos de cómputo están agrupados para servir a múltiples usuarios con diferentes asignaciones físicas y virtuales, y se reasignan de acuerdo a la demanda de los usuarios.

d) **Rápida elasticidad.** Las capacidades del sistema se pueden aprovisionar rápidamente y, en algunos casos de forma automática, para escalar recursos y adaptarlos a la demanda.

e) **Servicios medidos y controlados.** El uso de recursos se puede monitorizar, controlar y

reportar, de tal forma que tanto el proveedor del servicio como el usuario conozcan y entiendan cuanto se ha utilizado en un periodo de tiempo determinado.

Desde este punto de vista, se pueden identificar tres variaciones de la computación en la nube: nubes públicas, nubes híbridas y nubes privadas.

Una nube pública ofrece sus recursos y capacidades de forma compartida a través de Internet o redes públicas, normalmente en un modelo de pago por uso.

Una nube hibrida es una mezcla de nubes públicas y privadas que las organizaciones utilizan para aprovechar las ventajas de los servicios de pago por uso, pero manteniendo el control sobre sus servicios "Core" en sus instalaciones.

Una nube privada es una variación de la nube pública en donde todos los recursos e infraestructuras están alojados y controlados por la organización. Su acceso es limitado y restringido a los usuarios o autorizados de la organización.

Esta norma de seguridad **se centra precisamente en el modelo de nube privada**, la cual está apoyada en tecnologías de virtualización y de hiperconvergencia.

El objetivo que se busca cuando se plantea el despliegue de una nube privada es que la organización logre alcanzar los beneficios tecnológicos de un modelo de computación de nube (autoservicio, escalabilidad, automatización, monitorización, etc.) pero **sin renunciar a las medidas de seguridad y el control de la infraestructura adaptado a los requerimientos y normativas aplicables** a la organización.

Independientemente de las tecnologías que se vayan a utilizar en el centro de datos, será necesario definir e identificar las acciones adecuadas que permitan: **planificar una estrategia de TI** acorde con normativas y requerimientos de seguridad en este nuevo contexto, **aprovisionar y entregar** de forma eficiente los distintos servicios a los usuarios, **operar las infraestructuras** de nube privada en el día a día y **mantener en el medio y largo plazo** las medidas de seguridad, mejores prácticas y niveles de riesgo a lo largo del ciclo de vida del sistema.

El diseño, la implementación y las operaciones de la nube privada deberán cumplir con las medidas y principios de seguridad generales establecidos en las diferentes guías CCN-STIC para el tratamiento de la documentación y la información.

El hecho de implementar una nube privada, con sus ventajas asociadas, no implica tener que relajar o renunciar a las medidas de seguridad que habitualmente se adoptan en entornos tradicionales.

a) **Análisis y gestión del riesgo.**

b) **Mínima funcionalidad.**

c) **Mínimo privilegio.**

d) **Nodo autoprotegido.**

e) **Defensa en profundidad.**

f) **Control de configuración.**

g) **Verificación de la seguridad.**

h) **Monitorización, vigilancia y respuesta a incidentes.**

i) **Resiliencia.**

7.1 TECNOLOGÍAS DE VIRTUALIZACIÓN

7.1.1 CONCEPTOS GENERALES

La hiperconvergencia se nutre de tecnologías de virtualización ya consolidadas, por lo que se ha considerado adecuado, realizar en esta norma un breve repaso a dichas tecnologías, con el objetivo de consolidar las directrices de seguridad de este nuevo modelo de infraestructuras.

Como ya es sabido, las tecnologías de virtualización permiten, en mayor o menor medida, la abstracción del sistema operativo y de las aplicaciones, del propio hardware, incluyendo las comunicaciones y el almacenamiento. Con ello, se logra encapsular un equipo físico completo y convertirlo en una máquina virtual, permitiendo de esta forma, el despliegue de sistemas completos basados exclusivamente en máquinas virtuales corriendo sobre el mismo hardware, o sobre un conjunto de servidores físicos en alta disponibilidad.

Entre otros aspectos, **las tecnologías de virtualización permiten**:

a) **Ejecutar simultáneamente** diferentes servidores y/o equipos cliente virtuales en un único hardware físico.

b) **Optimizar el uso de los recursos** físicos, fundamentalmente la capacidad de procesamiento de datos, el uso de la memoria, el almacenamiento y las comunicaciones.

c) **Administrar de forma centralizada** todos los componentes del sistema, facilitando incluso la gestión de varios sistemas alojados en la misma infraestructura física.

d) **Mejorar la disponibilidad** de los servicios en entornos críticos.

e) **Simplificar** y mejorar los planes de contingencia y recuperación ante desastres.

f) **Incrementar la seguridad** mediante el aislamiento físico y lógico de los sistemas, pudiendo incluso aislar servidores y servicios pertenecientes a diferentes ámbitos de información.

Un centro de datos virtual es aquel que hace un **uso intensivo de la virtualización, con una alta densidad de máquinas virtuales**, aprovechando al máximo las capacidades del hardware de hoy en día y pudiendo llegar a convertirse en una **nube privada propiedad de la organización**.

Cabe señalar que, no solo por incorporar tecnologías de virtualización a un centro de datos, éste se convierte en una nube privada. Para que se considere una nube privada, se deberán cumplir con las principales características de un modelo de nube indicadas anteriormente.

Tanto la capacidad de proceso y de memoria del hardware, como las soluciones de virtualización desarrolladas por los distintos fabricantes han evolucionado enormemente en los últimos años, ofreciendo una serie de importantes ventajas frente al modelo tradicional, aunque también algunos inconvenientes que deberán ser tomados en cuenta a la hora de identificar posibles riesgos de seguridad.

Entre las **ventajas** que ofrece la virtualización, destacan las siguientes:

a) **Reducción de costes administrativos**. Los modelos tradicionales de entrega de servicios requieren una serie de labores administrativas, de aprovisionamiento, preparación y de configuración que se ven notablemente simplificadas al emplear entornos virtualizados.

b) **Reducción de costes económicos**. En comparación con los sistemas tradicionales, las arquitecturas virtualizadas permiten un importante ahorro económico, en términos de

costes de adquisición y mantenimiento del hardware, así como en el licenciamiento de las propias máquinas virtuales. Además, los principales fabricantes permiten adquirir licencias de tipo Datacenter o similar con derechos de uso ilimitado de máquinas virtuales dentro del mismo hardware, facilitando así la implementación de centro de datos virtuales con una alta densidad de máquinas virtuales.

c) **Integración y escalabilidad flexibles**. Con la virtualización, es relativamente sencillo añadir capacidad a la infraestructura, así como redundancia y mejoras de rendimiento, ya sea bajo demanda, de forma temporal o permanente.

d) **Disponibilidad.** Las tecnologías de virtualización permiten garantizar excelentes niveles alta disponibilidad en sistemas de misión crítica, los cuales requieren prácticamente que no exista indisponibilidad de los servicios que ofrecen, por pequeña que ésta sea.

e) **Independencia.** La virtualización permite abstraerse del hardware, aislar componentes clave como comunicaciones o almacenamiento, aunque se comparta la infraestructura común de procesamiento en el host de virtualización. Esto abre la posibilidad a que dos o más sistemas puedan coexistir en la misma plataforma de virtualización, siempre y cuando se garanticen los niveles de aislamiento e independencia requeridos.

Sin embargo, también **existen una serie de inconvenientes** que deberán ser tenidos en cuenta, durante las fases de diseño e implementación.

a) Pueden aparecer riesgos de seguridad relacionados precisamente con el **aislamiento de los sistemas**. Dichos riesgos pueden ser debidos a **vulnerabilidades del propio fabricante o a configuraciones** de seguridad deficientes o incorrectas, no ajustadas a normas.

b) En este sentido, **el objetivo de esta guía es proporcionar las directrices y mecanismos de seguridad adecuados** para reducir o mitigar estos riesgos.

La seguridad de cada sistema CIS se deberá diseñar y mantener de la misma forma que hasta ahora, independientemente de si está desplegado en infraestructuras físicas o virtuales.

En el caso de arquitecturas virtuales en donde se implementen más de un sistema, **se deberá garantizar el aislamiento lógico de cada sistema**, proporcionando únicamente los mecanismos definidos en el documento de interconexión correspondiente para la transmisión de datos fuera del propio sistema.

Es fundamental, por lo tanto, en este tipo de diseños de arquitecturas virtuales, implementar una correcta separación del tráfico de red entre los distintos sistemas que van a convivir en la infraestructura y los propios hosts de virtualización.

Además de esto, será necesario definir y mantener una adecuada gestión de roles de acceso, principalmente en el ámbito de la administración de los sistemas y también en la administración de la arquitectura de virtualización que soporta dichos sistemas.

Afortunadamente, gracias a los últimos avances en las tecnologías de virtualización, hoy en día es posible incrementar los niveles de aislamiento y de acceso a las máquinas virtuales, implementando configuraciones de seguridad como pueden ser las máquinas virtuales aisladas del host, el tejido protegido o el cifrado en reposo, entre otras.

Otro de los aspectos para tener en cuenta de cara a mitigar posibles riesgos, es la forma en que se comparte el almacenamiento dentro de la arquitectura de virtualización. **Se deberá diseñar un almacenamiento que garantice los niveles de aislamiento y de seguridad requeridos** por cada uno de los Sistemas, así como un acceso controlado, auditado y puesto a disposición únicamente al personal autorizado para dicho sistema. Esta última medida se encuentra totalmente ligada al concepto "necesidad de conocer".

7.1.2 TIPOS DE VIRTUALIZACIÓN

Desde el punto de vista funcional, no todos los tipos de virtualización están basados en máquinas virtuales. Hoy en día, se pueden encontrar múltiples tipos de virtualización conviviendo en un mismo entorno o infraestructura, dependiendo del objetivo del servicio y los destinatarios a los que va dirigido.

Fundamentalmente, se pueden identificar cinco tipos de virtualización:

- Virtualización del escritorio.
- Virtualización de las aplicaciones.
- Virtualización de servidores.
- Virtualización del almacenamiento.
- Virtualización de la red.

En el siguiente diagrama se puede observar los diferentes tipos de virtualización, así como su ubicación dentro de una arquitectura de hiperconvergencia.

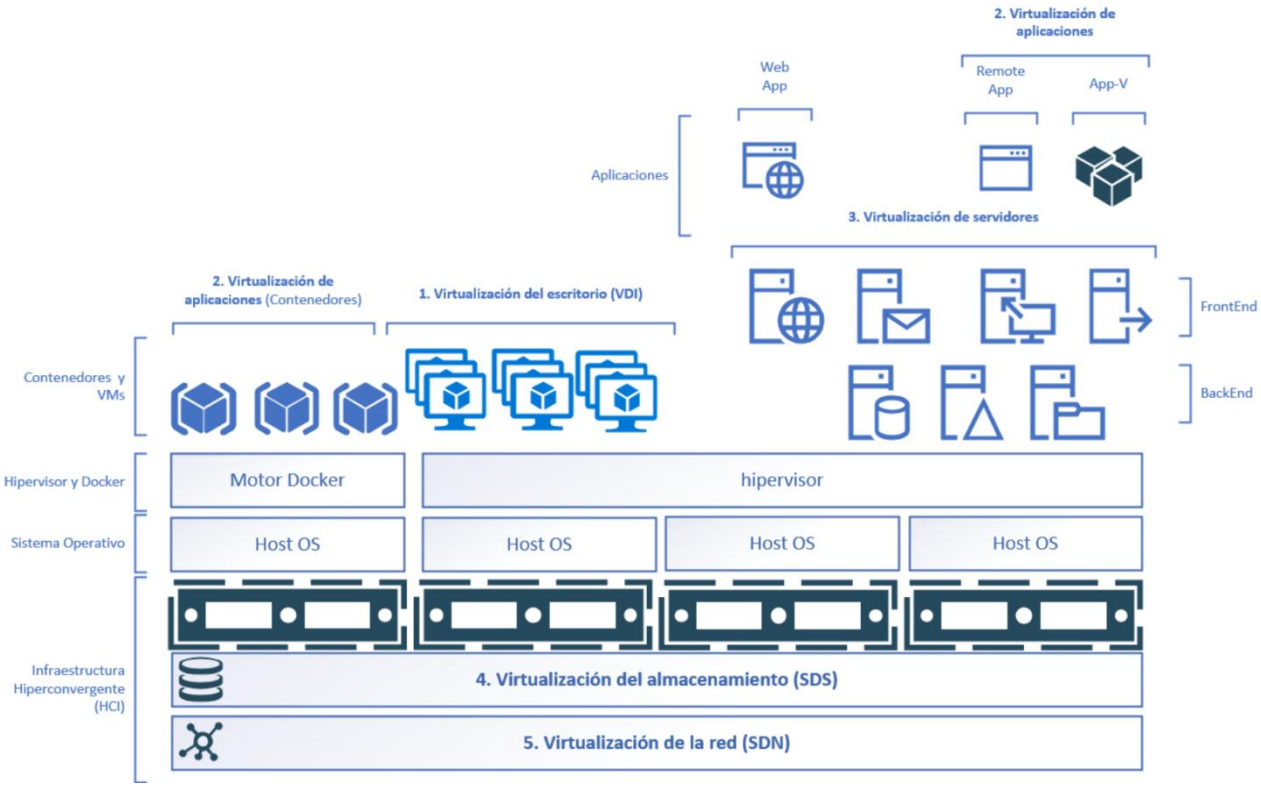

Ilustración 1. Diferentes tipos de virtualización en infraestructura hiperconvergente

7.1.2.1 VIRTUALIZACIÓN DEL ESCRITORIO

Se trata de un modelo de virtualización basado en máquinas virtuales de sistemas operativos cliente. Este modelo de virtualización ofrece a los usuarios acceso remoto a escritorios completos de Windows (fundamentalmente) sin necesidad de disponer de hardware potente en el origen, ya que los escritorios se ejecutan en el centro de datos, en un conjunto o clúster de servidores.

Existen distintos tipos de fabricantes que ofrecen soluciones VDI con más o menos características, pero todos orientados a ofrecer una experiencia de trabajo completa a los usuarios, aunque el sistema operativo no se ejecute en sus equipos. El acceso a los escritorios virtuales se puede hacer desde múltiples plataformas y dispositivos, como estaciones de trabajo, clientes ligeros (thin clients), tablets e incluso teléfonos móviles.

Esta capacidad de acceso desde cualquier dispositivo aporta flexibilidad e independencia del hardware, mientras que añade riesgos de seguridad que deben ser minimizados y controlados.

Además, la virtualización del escritorio optimiza aspectos como la aceleración de los gráficos, mejorando la experiencia del usuario para que sea similar a la que puede ofrecer un equipo físico.

7.1.2.2 VIRTUALIZACIÓN DE APLICACIONES Y CONTENEDORES

La virtualización de aplicaciones ha tenido a lo largo de los años distintas vertientes, muchas veces con algún grado de confusión entre los términos utilizados.

Se considera virtualización de aplicaciones a las tecnologías que permiten encapsular en un entorno aislado o *sandbox*, los ejecutables de las aplicaciones, junto con los ficheros necesarios, servicios y árbol de registro, todo listo para su despliegue y ejecución a través de la red en distintos sistemas operativos, incluso aquellos que pueden no ser compatibles con la propia aplicación. De esta forma se eliminan incompatibilidades y dificultades con las dependencias de ficheros comunes.

Las aplicaciones virtuales se publican en servidores administrados de forma centralizada y se envían a través de la red como si fuera un servicio de *streaming* en tiempo real y bajo demanda.

Los usuarios pueden iniciar sus aplicaciones virtuales desde su escritorio y éstas se ejecutan como si estuvieran realmente instaladas de forma local.

Una variante de la virtualización de aplicaciones son las aplicaciones remotas. En realidad, las aplicaciones remotas no están virtualizadas, sino que se instalan de la manera tradicional en un servidor de aplicaciones, el cual entrega la aplicación a los usuarios en un modelo similar al escritorio virtual, pero sin que se visualice todo el escritorio, solo la ventana correspondiente a la aplicación. Técnicamente no se podría considerar una aplicación virtualizada, aunque muchas veces se incluye esta tecnología como parte de la virtualización de aplicaciones.

La diferencia entre una tecnología y otra es que las aplicaciones virtuales se encapsulan y se ejecutan utilizando los recursos de procesamiento y almacenamiento del equipo cliente, mientras que las aplicaciones remotas se instalan y se ejecutan en el servidor, por lo que únicamente se utilizan recursos del lado del servidor, nunca del cliente.

Por otro lado, en los últimos años se han desarrollado rápidamente las tecnologías basadas en contenedores, las cuales constituyen una nueva forma de virtualizar aplicaciones y servicios,

manteniendo un alto grado de aislamiento con otras aplicaciones y servicios.

Actualmente las tecnologías de contenedores están presentes tanto en sistemas Linux como en sistemas Windows. En ambos casos, se trata de bloques de implementación portables y uniformes en donde se encapsulan todos los componentes necesarios para la ejecución de la aplicación o servicio.

La principal ventaja de los contenedores es su gran capacidad para despliegues rápidos, así como su flexibilidad para ejecutarse en cualquier sistema compatible. Una derivada de esta arquitectura es la seguridad, pudiendo aislar unos contenedores de otros, aunque se ejecuten en el mismo sistema.

Los contenedores, por si mismos no son más seguros que una máquina virtual, por lo tanto, será necesario prestar especial atención a diferentes aspectos de seguridad, como son las fuentes utilizadas para generar la imagen base y protegerla de posibles vulnerabilidades, el aislamiento de procesos, los accesos al contenedor, la automatización en el despliegue y las comunicaciones internas entre contenedores una vez puesto en producción, así como el uso de componentes comunes.

Aunque un contenedor comparte el kernel del sistema operativo host, no obtiene acceso sin restricciones a dicho kernel. En su lugar, el contenedor obtiene una vista aislada (y, en ocasiones, virtualizada) del sistema. Un contenedor puede tener acceso a una versión virtualizada del sistema de archivos y el registro, pero los cambios solo afectan al contenedor y se descartan cuando se detiene.

Dado que un contenedor está aislado del entorno de modo de usuario del host, el contenedor necesita su propia copia de estos archivos del sistema de modo de usuario, que se empaquetan en algo conocido como imagen base. La imagen base cumple el papel de la capa fundamental en la que se basa el contenedor y le proporciona los servicios de sistema operativo que no ofrece el kernel.

A diferencia de un contenedor, una máquina virtual (VM) ejecuta un sistema operativo completo, incluido su propio kernel, tal y como se observa en el siguiente diagrama.

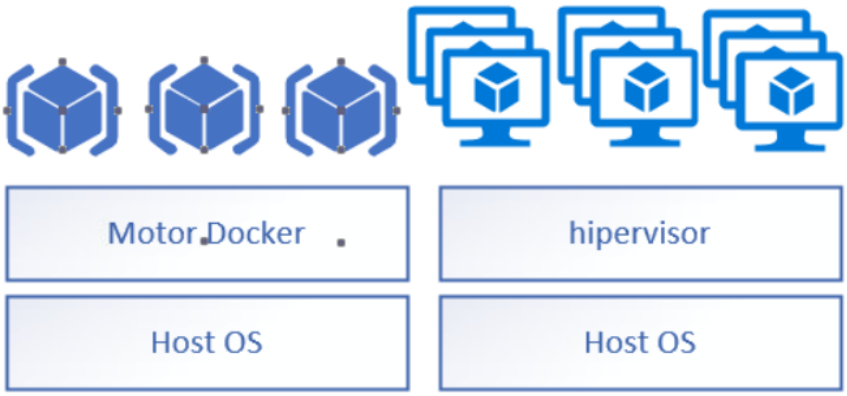

Ilustración 2. Contenedores y máquinas virtuales

7.1.2.3 VIRTUALIZACIÓN DE SERVIDORES

En términos de virtualización, la virtualización de servidores es similar a la virtualización de escritorios, con la diferencia que se trata de sistemas operativos de servidor para ofrecer servicios a los usuarios que se conecten.

La principal diferencia está en que, en una virtualización de servidores, los usuarios que no

son administradores no se conectarán nunca al escritorio de la máquina virtual, por lo tanto, no será necesario implementar mecanismos de aceleración de video o presentación de escritorio. Por el contrario, los servidores virtuales ofrecen servicios de diferentes tipos, a los cuales los usuarios se conectan, ya sea de forma directa desde sus estaciones de trabajo o de forma indirecta a través de un escritorio virtual VDI.

La virtualización de servidores deberá atender aspectos de rendimiento de las aplicaciones en segundo plano, optimización en el uso de recursos de memoria y procesamiento, fundamentalmente. Los fabricantes de soluciones de virtualización permiten la asignación de forma dinámica de los recursos de hardware existentes para consolidad y optimizar un mayor número de servidores en un mismo hardware.

7.1.2.4 VIRTUALIZACIÓN DEL ALMACENAMIENTO

A diferencia de los sistemas tradicionales como NAS (almacenamiento conectado a la red) o SAN (red de área de almacenamiento), el almacenamiento definido por software (SDS) permite unificar en un solo espacio o conjunto lógico, múltiples discos físicos instalados localmente en cada servidor del clúster de hiperconvergencia. Esta capacidad hace que, a efectos del hipervisor, el almacenamiento se muestre como un solo conjunto, independientemente de su ubicación física. Por ejemplo, varios discos físicos pueden ser presentados por la capa de abstracción como un único disco, en lugar de como una colección de discos más pequeños.

La capa de software que gestiona el almacenamiento proporciona los servicios de acceso al almacenamiento, las conexiones de red y la conectividad.

El **almacenamiento definido por software** (más conocido por **SDS**, "*Software-defined storage*"), supone el abandono del uso tradicional del almacenamiento conectado a la red (NAS) y las redes de área de almacenamiento (SAN). A diferencia del almacenamiento tradicional, el almacenamiento definido por software emplea la virtualización del almacenamiento para controlar el acceso a los datos mediante una capa de software abstraída de los dispositivos de almacenamiento.

El uso de almacenamiento definido por software permite una escalabilidad mucho más rápida y, casi siempre, más económica que la que ofrecen las cabinas de almacenamiento tradicionales basadas en hardware en propiedad. El almacenamiento definido por software permite tanto el uso de hardware de almacenamiento basado en discos tradicionales estándar como el almacenamiento basado en discos sólidos SSD, o un hibrido de ambos.

A pesar de que diferentes proveedores/fabricantes proporcionan soluciones diferentes de almacenamiento basado en software, todos tienen en común un conjunto de características esenciales:

a) **Abstracción**: En la arquitectura SDS, el software que administra el almacenamiento es independiente del hardware de almacenamiento, por tanto, se dice que el software se "abstrae", o que está "desacoplado" del hardware.

b) **Virtualización**: La arquitectura SDS agrupa los recursos de almacenamiento y los administra como una unidad cohesionada. Esto es muy similar a la virtualización, pero aplicado al almacenamiento en lugar de a los recursos informáticos.

c) **Automatización:** Se utilizan funciones de automatización para reducir la cantidad de tareas que los administradores del almacenamiento deben realizar manualmente.

d) **Estandarización**: Basado en hardware estándar en la industria. Las soluciones SDS se

basan en hardware estándar de la industria, así como en las API estándar para la administración del almacenamiento.

e) **Flexibilidad:** Es muy fácil añadir o eliminar capacidad de almacenamiento y continuar administrando el almacenamiento como un todo.

Por lo tanto, a modo de resumen, se puede decir que los beneficios del uso de almacenamiento gestionado por software son:

a) **Ahorro de costes:** posibilita el uso de hardware más básico, estándar y no propietario.

b) **Sistema escalable:** facilita la expansión del almacenamiento.

c) **Sistema flexible:** flexibilidad en la gestión TI.

d) **Libertad de elección de proveedor:** se evita estar "atado" a un fabricante o proveedor gracias a que SDS se puede ejecutar en cualquier hardware.

7.1.2.5 VIRTUALIZACIÓN DE LA RED

La virtualización de red (NV – Network Virtualization) hace referencia a la desvinculación de los recursos de red que tradicionalmente se proporcionan en forma de hardware. La virtualización de red hace uso de dos tecnologías (NFV y SDN) para transformar redes estándar en redes virtuales.

Virtualización de las funciones de red (NFV – Network Function Virtualization) flexibiliza la red, permitiendo a cada nodo convertirse en un microcentro de datos, capaz de hospedar varias aplicaciones.

La virtualización de las funciones de red (SDN - Software defined Network) consiste en la gestión mediante un software del enrutamiento o la optimización WAN y Firewall.

El uso combinado de estas tecnologías facilita la gestión de redes frente al modelo tradicional de redes, de manera que

a) Todos los elementos de la red pasan a controlarse de forma centralizada.

b) Los elementos de la red pueden entenderse unos con otros independientemente del fabricante.

c) Se crea una sola red a nivel lógico que se divide en las redes necesarias.

d) La misma red virtual puede estar definida en varios hipervisores y controlarse de forma centralizada.

Las funciones de red como cortafuegos, balanceadores, QoS, etc. se pueden definir por software, ubicar en cualquier punto de la red y controlar de forma centraliza.

7.1.3 TECNOLOGÍAS DE HYPERVISOR

Las tecnologías de virtualización basadas en hipervisor han evolucionado mucho en los últimos años, reduciendo cada vez más las diferencias de rendimiento entre sistemas virtualizados y sistemas físicos, hasta hacerlas prácticamente despreciables.

Pero también han evolucionado en materia de seguridad, trasladando tecnologías del ámbito físico al virtual. Esto está permitiendo implementar entornos seguros, aunque la arquitectura de virtualización esté compartida.

Una máquina virtual es un entorno de ejecución aislado que ha sido creado por el software

encargado de gestionar todos los recursos del hardware. Este componente de software se le conoce como hipervisor y por norma general, el término máquina virtual se relaciona a las tecnologías de virtualización de hardware, aunque también se utiliza en los conceptos de virtualización de procesos tales como máquina virtual de Java (JVM: Java Virtual Machine).

A continuación, se detallan algunas de las mejoras en materia de seguridad que han incorporado los principales fabricantes de tecnologías de virtualización:

a) **Chips virtuales TPM 2.0**

b) **Arranque seguro basado en TPM 2.0**

c) **Módulos criptográficos compatibles con FIPS 140-2**

d) **Máquinas virtuales blindadas.**

Esta característica protege a las máquinas virtuales para que sea más difícil para los administradores y el malware en el host inspeccionar, manipular o robar datos del estado de una máquina virtual blindada.

Si una máquina virtual sale de una organización (de forma intencionada o accidental), cabe la posibilidad de que se ejecute en cualquier otro sistema, invalidando cualquier tipo de protección que se hubiera aplicado a nivel de sistema operativo.

Una máquina virtual blindada es una máquina virtual que tiene un TPM virtual, se cifra mediante BitLocker y solo puede ejecutarse en hosts correctos y aprobados en el tejido. Las máquinas virtuales blindadas y el tejido protegido permiten a los administradores de empresa de nube privada y a los proveedores de servicio en la nube proporcionar un entorno más seguro para las máquinas virtuales inquilinas.

e) **Cifrado de discos de máquinas virtuales**

Hoy en día se pueden proteger los discos del sistema operativo mediante el cifrado de unidad de disco en máquinas virtuales de generación 1. La característica de almacenamiento de claves crea una pequeña unidad dedicada para almacenar la clave de BitLocker de la unidad del sistema, en lugar de usar un Módulo de plataforma segura virtual (TPM), que solo está disponible en las máquinas virtuales de generación 2.

Para descifrar el disco e iniciar la máquina virtual, el host debe formar parte de un tejido protegido autorizado o tener la clave privada de uno de los tutores de la máquina virtual. El almacenamiento de claves requiere una máquina virtual de la versión 8.

f) **Arranque seguro de Linux**

Las distribuciones de sistemas operativos Linux compatibles que se ejecutan en máquinas virtuales de generación 2 pueden arrancar con la opción de arranque seguro habilitada. Antes de arrancar la máquina virtual por primera vez se debe configurar la máquina virtual para que use la entidad de certificación UEFI.

g) **Seguridad basada en virtualización.**

i. Protección de credenciales: tiene como objetivo aislar y proteger datos confidenciales clave del sistema y del usuario frente a riesgos.

ii. Protección de dispositivos: proporciona un conjunto de funciones diseñadas para trabajar juntas con el fin de prevenir y eliminar el malware que se ejecuta en un sistema.

iii. Integridad de código configurable: garantiza que solo se ejecute código de confianza desde el cargador de arranque en adelante.

h) **Modo de bloqueo.** En el modo de bloqueo, solo se puede acceder a los hosts a través de las herramientas autorizadas. Se puede hacer uso de un modo de bloqueo estricto o el modo de bloqueo normal y se pueden definir usuarios con excepción para permitir el acceso directo a las cuentas de servicio, como agentes de copias de seguridad.

i) **Autenticación de tarjeta inteligente.** Las tecnologías de virtualización admiten el uso de autenticación basada en tarjeta inteligente en lugar de la autenticación de nombre de usuario y contraseña. Para incrementar los niveles de seguridad se puede configurar la autenticación de tarjeta inteligente para el acceso a las herramientas administrativas del hipervisor. También se admite la autenticación en dos fases, configurando al mismo tiempo la autenticación con nombre de usuario y contraseña, y la autenticación de tarjeta inteligente.

Se recomienda implementar estas y otras medidas de protección en entornos compartidos entre dos o más sistemas para proteger los recursos de cada sistema de forma aislada, como controladores de dominio, servidores de archivos confidenciales y sistemas con información personal de recursos humanos, entre otros.

7.2 HIPERCONVERGENCIA

Hoy en día prácticamente todos los organismos y empresas de cierto tamaño hacen uso de la virtualización en alguna u otra forma. Como ya se ha visto en el apartado anterior, no es extraño oír hablar de hipervisor, máquinas o redes virtuales. Sin embargo, es menos habitual hablar y encontrar infraestructuras de tipo convergentes o hiperconvergentes, ya que en muchos casos son tecnologías enfocadas en el mercado de los grandes proveedores de centros de datos.

En el apartado anterior se han abordado los conceptos básicos de la virtualización. En este apartado se abordarán los conceptos y tecnologías de hiperconvergencia, y se analizará la relación entre ellos, desde un punto de vista funcional, pero también desde un punto de vista de seguridad.

Las actuales tecnologías de virtualización están siendo adoptadas por todas las organizaciones para cubrir las necesidades actuales de los sistemas y aplicaciones debido a sus características de distribución de recursos, aislamiento de sistemas, capacidad de consolidación, opciones de seguridad, facilidades de administración e implementación, etc.

Se puede hablar de **hiperconvergencia como un paso más allá de la virtualización**. En una arquitectura virtualizada tradicional, a pesar de que las cargas de trabajo, los discos y las redes pueden estar virtualizados, los componentes físicos que soportan dicha arquitectura se siguen administrando de forma separada como elementos físicos.

Por este motivo, en una arquitectura virtualizada tradicional se aplican medidas de seguridad de forma separada:

a) Medidas de seguridad para el almacenamiento.

b) Medidas de seguridad para la red.

c) Medidas de seguridad para las cargas de trabajo o máquinas virtuales.

d) Medidas de seguridad para el perímetro.

La mayoría de las capas y componentes que forman parte de una arquitectura de virtualización tradicional se gestionan de forma separada e independiente. Cada fabricante implementa su propia consola de administración, con la consiguiente complejidad y dificultad para integrar nuevos componentes o ampliar la capacidad del conjunto del sistema: normalmente nos encontraremos con una consola para administrar el hipervisor, una o varias consolas para administrar la electrónica de red, una consola para administrar el almacenamiento, otra consola para administrar la seguridad perimetral, y así sucesivamente.

Por el contrario, una arquitectura hiperconvergente está compuesta como mínimo de una capa de **hipervisor, una red definida por software (SDN) y un almacenamiento definido por software (SDS).** Todo ello permite unificar los elementos físicos en capas lógicas, con una gestión centralizada de todo el conjunto en una única consola administrativa. Cada nodo del clúster constituye un bloque funcional que incorpora todos los componentes necesarios: proceso, red y almacenamiento.

Es por ello por lo que, las tecnologías de **hiperconvergencia proporcionan la agilidad y escalabilidad** necesaria para llevar a cabo la implementación de **soluciones basadas en una nube** sin tener que renunciar a la propiedad del hardware y la seguridad física del centro de datos propio. **Cuando se habla de hiperconvergencia, se habla también de nubes privadas, ya que estos dos conceptos están estrechamente ligados.**

Pasar de virtualización a hiperconvergencia no es un proceso rápido ni sencillo. **Requiere de mucha planificación e inversión en hardware específico. Pero, sobre todo, requiere adaptar las medidas de seguridad tradicionales al nuevo modelo de seguridad hiperconvergente.**

Las infraestructuras basadas en hiperconvergencia (HCI) están **definidas por software en su totalidad**, en donde se aíslan todas las operaciones relacionadas con el hardware del sistema y se unifican a nivel de hipervisor en un único bloque.

En cada bloque se integran todos los recursos necesarios de procesamiento, almacenamiento y comunicaciones para que sea autónomo o trabajo en un conjunto de clúster. Todas las funciones esenciales de una infraestructura de servidores se ejecutan en una capa de software estrechamente integrada, en lugar de utilizar un hardware diferente para cada tipo de función.

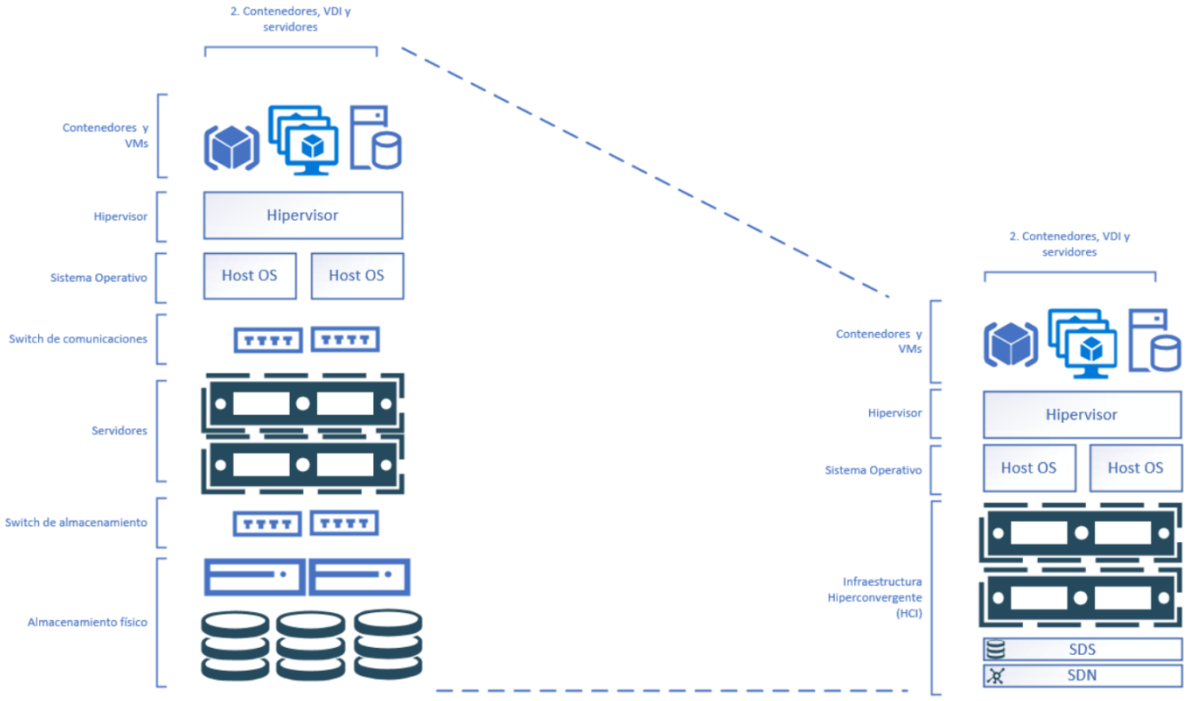

Ilustración 3. Arquitectura de virtualización tradicional y arquitectura hiperconvergente

Una arquitectura hiperconvergente se entrega como un paquete compacto y único, el cual ya dispone de todos sus componentes en un sistema preconfigurado previamente. Toda la infraestructura se ejecuta en una máquina virtual en la capa del hipervisor, bajo la cual se ubica el hardware actuando como un repositorio común de recursos.

Una infraestructura hiperconvergente permite:

a) Una **gestión centralizada** de todos los componentes virtuales a través de una única interfaz, reduciendo las tareas de administración.

b) **Automatización** de los principales procesos de despliegue, configuración y puesta en producción.

c) **Control detallado y continuo del uso de recursos,** monitorización de la salud del conjunto de sistemas y desencadenamiento de acciones ante posibles incidencias.

d) Un **mayor grado de escalabilidad horizontal** mediante la incorporación de servidores a la arquitectura sin necesidad de interrumpir el servicio.

e) En caso de catástrofe, como todos los componentes están representados de forma virtual, es posible **reemplazar *appliances* completos minimizando el riesgo** de pérdida de datos o interrupción del servicio.

f) Los sistemas hiperconvergentes incorporan elementos de **seguridad nativa basada en software**, como por ejemplo el cifrado de datos en reposo.

g) **Aceleración del tiempo de puesta en producción** de las aplicaciones y sistemas.

h) Mejora de la experiencia del usuario gracias a **optimizaciones *all-flash storage*** (tecnología de almacenamiento de datos basada en una memoria de alta velocidad que se programa electrónicamente) para generar tiempos de respuesta ultra rápidos.

Sin embargo, alguno de los **inconvenientes** de una infraestructura hiperconvergente:

a) Puede ser una **solución más restrictiva** a la hora de la selección del hardware, ya que los sistemas hiperconvergentes han de adquirirse como un bloque (hardware y software), lo cual limita la flexibilidad del sistema en caso de que se requiera actualizar uno de los componentes de la arquitectura del sistema hiperconvergente.

b) Así mismo, en caso de que se detecte algún fallo de hardware o de seguridad en uno de los componentes del sistema, **su actualización o sustitución puede ser más compleja** que si se dispone de un sistema tradicional o un sistema modular de arquitecturas virtuales.

c) La **gama de fabricantes y productos hiperconvergentes es aun relativamente escasa** en comparación con otras soluciones tradicionales de virtualización.

8. CONSIDERACIONES GENERALES DE SEGURIDAD EN SISTEMAS QUE MANEJAN INFORMACIÓN CLASIFICADA

Ante la necesidad de implementar más de un sistema que maneja información clasificada en una misma arquitectura virtual (ya sea tradicional o hiperconvergente), se debe tener en consideración que dichos sistemas compartirán recursos y componentes, además de una misma ubicación física. Sobre todos ellos, deberán aplicarse las medidas de seguridad necesarias físicas y lógicas, en cumplimiento de la Instrucción Técnica de Seguridad de las TIC CCN-STIC 301.

El aislamiento de un sistema que maneja información clasificada sobre otro que convive en la misma infraestructura, y también el aislamiento con respecto a la propia arquitectura de virtualización es la base sobre la que se fundamenta su seguridad y abre la posibilidad a que ambos sistemas convivan en entornos de nube privada.

Sin una definición clara de aislamiento, ni medidas estrictas de control entre los sistemas, no se podrán compartir recursos y componentes de las arquitecturas de virtualización entre sistemas que manejen información clasificada.

A continuación, se enumeran algunas directrices que deberán considerarse a la hora de diseñar e implementar arquitecturas de nube privada que unifiquen varios sistemas que vayan a manejar información clasificada:

a) Se podrán considerar arquitecturas virtuales que unifiquen diferentes ámbitos de clasificación de la información (RESERVADO NACIONAL, NATO SECRET, UE SECRET…) entre los que existan acuerdos de equiparación.

b) Se podrán considerar arquitecturas virtuales que unifiquen diferentes grados de clasificación de la información (SECRETO NACIONAL, RESERVADO NACIONAL, CONFIDENCIAL…).

c) Se podrán considerar arquitecturas virtuales que unifiquen diferentes ámbitos y grados de clasificación de la información (SECRETO NACIONAL, NATO SECRET, EU CONFIDENTIAL…).

d) Todos los sistemas que manejen información clasificada, incluidos en la arquitectura de virtualización, con independencia del ámbito o grado de clasificación al que pertenezcan, deberán estar acreditados por la Autoridad de Acreditación Nacional según dicta la "Política de Seguridad de las TIC (CCN-STIC-001)" donde se recoge la necesidad de la acreditación de los sistemas que manejan información clasificada.

e) A todos los efectos, los sistemas que residan en una misma arquitectura de virtualización deberán ser considerados sistemas independientes entre sí, cumpliendo el conjunto de requisitos de seguridad específicos tanto para el ámbito como para el grado de clasificación de la información que manejen.

f) Todo intercambio de información deberá ser tratado en función de lo indicado en la guía "CCN-STIC 302 Interconexión de sistemas de las TIC que manejan información clasificada en la Administración".

g) La arquitectura de virtualización deberá utilizar los procedimientos operativos de seguridad y poseer una configuración segura, atendiendo a los procedimientos y requisitos del sistema de mayor grado de clasificación, que resida en la misma.

h) Sistemas que manejen información clasificada no podrán compartir, en ningún caso, arquitectura de virtualización con sistemas que no manejen información clasificada.

i) La inclusión, en una arquitectura de virtualización, de sistemas con grado de clasificación DIFUSIÓN LIMITADA o equivalentes, deberá ser estudiada caso por caso.

j) Toda la administración relacionada con la arquitectura de virtualización deberá realizarse de manera independiente para cada uno de los sistemas que residan en ella. El personal administrador de virtualización deberá realizar una administración aislada y específica para cada uno de ellos. Además, deberán estar en posesión de las habilitaciones de seguridad necesarias.

k) Los componentes que conformen la arquitectura de virtualización (Software Defined Data Centers, Software Defined Networks y Software Defined Storage) deberán estar Incluidos en la Guía CCN-STIC 105 - Catálogo de Productos de Seguridad de las Tecnologías de la Información y Comunicación, CPSTIC como productos aprobados para el manejo de información Clasificada.

l) La introducción de la virtualización en sistemas ya existentes, se considerará un cambio mayor que implicará una reacreditación del sistema.

9. APLICACIÓN DE MEDIDAS DE SEGURIDAD EN ARQUITECTURAS VIRTUALES.

9.1 SEGURIDAD EN EL ENTORNO DEL HIPERVISOR

1. La infraestructura de hipervisor deberá ejecutar únicamente los roles y servicios específicos para ofrecer las funciones de virtualización. No se admite la instalación de programas, roles y otro software que no forme parte del rol de hipervisor.
2. Se deberá garantizar el aislamiento de las redes y componentes que participan de la comunicación entre nodos del hipervisor, de otro tipo de redes físicas o virtuales.
3. Se deberán implementar los medios de seguridad que garanticen que desde el sistema operativo anfitrión no se pueda acceder a la información sensible contenida en las máquinas virtuales.
4. La administración de la infraestructura de hipervisor deberá estar autenticada, controlada y auditada. Se requiere el empleo de usuarios nominales y grupos de acceso personalizados con privilegios concretos que garanticen una correcta segregación de roles, accesos y tareas ante todos los procedimientos operacionales.
5. Cualquier tipo de comunicación requerida para la administración de la arquitectura de

virtualización deberá utilizar mecanismos de cifrado robusto admitidos por el Centro Criptológico Nacional.

6. Se deberá configurar directivas que desconecten automáticamente las sesiones y ante un tiempo de inactividad, para evitar que existan comunicaciones establecidas y no controladas.
7. Se deberán configurar directivas que permitan el bloqueo de aquellas cuentas a las que se ha intentado acceder sin éxito en varias ocasiones.
8. En la medida de lo posible, se deberán establecer mecanismos que permitan la automatización de las configuraciones de seguridad a aplicar en cada uno de los hipervisores, de tal forma que se garantice un nivel de seguridad homogéneo y se reduzca la posibilidad de error humano en la aplicación de estas.
9. En caso de que la solución lo permita, se deberá implementar el arranque seguro UEFI para garantizar que el servidor rechaza la carga de aplicaciones o controladores no confiables.
10. Se deberá inhabilitar o restringir la posibilidad de hacer uso de medios físicos de almacenamiento externo, tanto en la secuencia de arranque como posteriormente.
11. Se deberán establecer medios para la detección de alertas de seguridad que permitan la prevención, identificación y respuesta frente a incidentes
12. La infraestructura de hipervisor deberá mantenerse debidamente actualizada con los parches y actualizaciones disponibles por el fabricante.
13. Se deberá establecer un método de registro de logs persistentes de seguridad que permita la trazabilidad de los eventos. Dichos registros deberían ser almacenados también en un sistema externo de gestión de logs y deberá estar protegido del acceso no autorizado.
14. Toda la infraestructura del hipervisor deberá estar correctamente sincronizada mediante un servicio de hora confiable y común para garantizar que la información entregada y almacenada a través de los ficheros de logs es fiable y ha registrado las marcas de tiempo correctas.
15. Se deberán establecer políticas de copias de seguridad que garanticen la continuidad del servicio en caso de incidente grave de seguridad.
16. Las copias de seguridad deberán estar cifradas en el almacenamiento de destino.

9.2 SEGURIDAD DE LAS HERRAMIENTAS DE ADMINISTRACIÓN

17. Existirán dos tipos de equipos de administración:
    a. Equipos empleados para la administración de la arquitectura de virtualización.
    b. Equipos empleados para la administración del inquilino en donde se aloja cada sistema.
18. En términos de nube privada, el espacio virtual de cada sistema posee, se denomina inquilino (*tenant*).
19. Por lo tanto, serán diferentes los equipos empleados para la administración de la arquitectura de virtualización que los equipos empleados para la administración de cada

inquilino.

20. Los equipos empleados para la administración de la arquitectura de virtualización deberán pertenecer solamente a una red aislada y dedicada, utilizada únicamente para dicho propósito.
21. Los equipos empleados para la administración de la arquitectura de virtualización formarán parte del sistema de virtualización y no podrán ser compartidos con otros sistemas.
22. Tanto los equipos empleados para la administración de la arquitectura de virtualización, como los equipos empleados para la administración de cada inquilino deberán haber sido instalados cumpliendo con las medidas de seguridad CCN-STIC específicas del sistema operativo y versión utilizados.
23. De forma predeterminada, el acceso a consolas gráficas y de comandos, deberá estar restringido y auditado.
24. Se deberán identificar y autorizar los equipos de administración desde los cuales se permitan conexiones a las consolas gráficas y de comandos.
25. Los usuarios que tengan acceso a los equipos empleados para la administración deberán poseer los permisos específicos para desempeñar únicamente las labores para las que están autorizados.
26. Las consolas gráficas y de comandos, o las herramientas de administración requeridas, deberán estar instaladas en sistemas operativos soportados por la solución para evitar errores en su funcionamiento y reducir el riesgo de vulnerabilidades.
27. Al igual que la infraestructura de hipervisor, se deberán mantener y actualizar las herramientas y consolas administrativas, instalando los parches específicos publicados por el fabricante, así como los del sistema operativo sobre el que están operando.
28. Se deberán proporcionar las herramientas de protección necesarias, tales como antivirus o antimalware, al sistema operativo desde el que se están realizando las tareas de administración.
29. En caso de utilizar más de un nodo hipervisor para la misma arquitectura de virtualización, se deberá implementar una consola centralizada de gestión y un servicio de directorio que permita unificar las cuentas de los administradores, así como procedimientos de administración y auditoría de accesos y operaciones realizadas en la infraestructura.
30. En todos los casos, será necesario identificar y definir roles y permisos según las necesidades operativas. En dichos roles será necesaria identificar claramente a qué elementos de la infraestructura tiene acceso cada usuario administrador.
31. Los usuarios deben ser únicos y nominales para permitir la trazabilidad de las actuaciones y la auditoría en el uso de privilegios.
32. La política de contraseñas a utilizar deberá establecer una cantidad mínima de caracteres, así como el uso de caracteres especiales, mayúsculas o números.
33. Se deberá reducir la superficie de exposición garantizando que en los equipos desde los cuales se realizan las tareas de administración solo se encuentran disponibles los puertos y servicios necesarios para dicha operativa y que éstos estarán filtrados para acceder

únicamente a la infraestructura que se requiere administrar.

34. Para el acceso a los equipos empleados para la administración de la infraestructura de virtualización o de los inquilinos, se deberá exigir el uso de un doble factor de autenticación, siendo insuficiente el empleo del método usuario/contraseña.
35. Se deberán implementar mecanismos de inicio de sesión único que reduzcan la cantidad de veces que se transmiten las credenciales de acceso en la red, y reducir así la posibilidad de que éstas sean interceptadas.

9.3 SEGURIDAD DEL ALMACENAMIENTO DEFINIDO POR SOFTWARE

36. El diseño del almacenamiento definido por software deberá garantizar el aislamiento lógico de cada inquilino que resida en la arquitectura de virtualización.
37. En ninguna circunstancia, el almacenamiento de un sistema que maneja información sensible o en un nivel de clasificación diferente deberá compartir espacio lógico con el almacenamiento de otro Sistema.
38. Se deberá implementar un canal seguro y dedicado para la comunicación entre los nodos responsables del almacenamiento definido por software. En esta comunicación viajan datos de replicación y sincronización del almacenamiento y deberá estar cifrada con protocolos y algoritmos de cifrado robustos y autorizados por el CCN.
39. Se deberá emplear un canal seguro y dedicado para establecer la comunicación entre el almacenamiento definido por software y los nodos de virtualización. Esta red no deberá ser accesible en ningún caso por las máquinas virtuales.
40. Para esta comunicación se deberá hacer uso solamente de los puertos, servicios y protocolos necesarios para el correcto funcionamiento del servicio. Así mismo, se deberán establecer mecanismos que limiten los dispositivos que pueden hacer uso de esta.
41. Se deberá mantener la infraestructura de almacenamiento, revisando e implementando periódicamente las actualizaciones que el fabricante publique, reduciendo la exposición ante vectores de ataque tratados por el fabricante en sus parches de actualización.
42. Los dispositivos de almacenamiento y los servidores que se conectan a ellos deberán cumplir con los requisitos de seguridad definidos en apartados anteriores tales como la existencia de mecanismos de trazabilidad, inventario y copias de seguridad de la información contenida.
43. Será responsabilidad del administrador del almacenamiento, o en su defecto del administrador de la arquitectura de virtualización, realizar copias de seguridad completas de todo el almacenamiento, así como diseñar y mantener planes de contingencia y recuperación en caso de desastre.
44. Las copias de seguridad del almacenamiento deberán viajar cifradas hacia su destino final y almacenarse de forma cifrada, garantizando la seguridad e inviolabilidad de los datos contenidos.

9.4 SEGURIDAD DE LAS REDES DEFINIDAS POR SOFTWARE

45. En el diseño de redes definidas por software se deberá garantizar el aislamiento lógico

entre los inquilinos, y entre éstos y la arquitectura de virtualización.

46. Dentro de cada inquilino se podrán definir entornos aislados mediante redes virtuales y en cada red virtual segmentos VLAN que permitan separar los diferentes servicios del sistema, según se requiera y se especifique en su correspondiente documentación de seguridad.
47. Como norma general, no se podrá establecer ningún tipo de comunicación entre inquilinos o entre sistemas que manejen información confidencial, salvo si se ha identificado una interconexión y se ha creado la correspondiente Declaración de Requisitos de Seguridad de la Interconexión (DRSI), tal y como se establece en la instrucción técnica para interconexiones CCN-STIC-302.
48. El acceso desde estaciones de trabajo físicas ya sea para administrar el sistema o para acceder a información, deberá estar protegido con protocolos y algoritmos de cifrado robustos y autorizados por el CCN, deberá estar controlado y auditado.
49. Se deberá aplicar la seguridad correspondiente tanto a los conmutadores físicos como a los virtuales y sus puertos, que pertenezcan a la red de gestión y redes de intercomunicación de la arquitectura de virtualización, así como las redes utilizadas por las máquinas virtuales.
50. Esta aplicación de seguridad incluirá medidas de prevención que consistirán en deshabilitar servicios o protocolos innecesarios para la infraestructura tales como Spanning Tree, SNMP o NetFlow. En caso de necesitar el uso de protocolos de esta índole, se deberán establecer métodos de configuración segura de los mismos como si de elementos o protocolos de una red física se trataran.
51. Como norma general, los conmutadores físicos y virtuales deberán rechazar el tráfico en modo promiscuo, así como la suplantación de dirección MAC, salvo que exista una necesidad de operación que así lo establezca.
52. Se deberán implementar mecanismos que garanticen el registro de eventos de seguridad y la monitorización del acceso a los componentes que pertenecen a la infraestructura de red virtual.
53. Se deberá asegurar que solamente tendrán acceso a estos elementos los usuarios administradores autorizados mediante controles de acceso basados en roles definidos y concretos.
54. Es recomendable utilizar mecanismos que mantengan los distintos elementos de la red en hora para garantizar que la información entregada y almacenada a través de los ficheros logs es fiable y ha registrado las marcas de tiempo adecuadas, así como para el correcto funcionamiento de los diferentes dispositivos.
55. Se deberán establecer mecanismos que permitan identificar e inventariar los diferentes elementos de red, tanto físicos como virtuales, que participan de la arquitectura de virtualización.
56. Se recomienda hacer uso de plantillas de configuración de los diferentes elementos de red, así como la copia de seguridad de estas para reducir el riesgo de errores de configuración que podría comprometer el funcionamiento de la infraestructura y generar vulnerabilidades.
57. Se deberá mantener la infraestructura de comunicaciones, tanto física como virtual,

revisando e implementando periódicamente las actualizaciones que el fabricante publique, reduciendo la exposición ante vectores de ataque tratados por el fabricante en sus parches de actualización.

9.5 SEGURIDAD DE LAS MÁQUINAS VIRTUALES

58. El sistema operativo invitado que ejecuta la máquina virtual está expuesto a los mismos riesgos de seguridad que si de una maquina física se tratara. Por tanto, las máquinas virtuales pertenecientes a un Sistema deberán implementarse siguiendo las normas y recomendaciones de las guías de seguridad CCN-STIC correspondientes.
59. Se deberá tomar una serie de medidas adicionales relativas al hardware virtual y a la configuración de la propia máquina virtual previos al arranque del sistema operativo que a continuación se detallan.
60. En caso de que la arquitectura de virtualización y los sistemas operativos de las máquinas virtuales lo permitan, se recomienda hacer uso de las medidas de seguridad avanzadas que ofrece el fabricante para los sistemas operativos modernos. Entre ellas se pueden encontrar:
    a. TPM 2.0 Virtual.
    b. Arranque seguro UEFI Secure Boot.
    c. Máquinas virtuales blindadas.
    d. Cifrado de los discos virtuales.
    e. Control de inquilino.
    f. Device guard y Credential Guard.
61. Se recomienda implementar, si la solución lo permite, el cifrado del almacenamiento virtual en, al menos, aquellas máquinas que almacenen información sensible.
62. Se recomienda implementar, si la solución lo permite, mecanismos propios de protección del software que se ejecuta en la propia máquina virtual.
63. Se deberán deshabilitar las funciones innecesarias a nivel de hardware virtual y las configuraciones de la máquina virtual que no vayan a ser utilizadas. Se debe tener en cuenta lo siguiente:
    a. Deshabilitar el acceso a los dispositivos virtuales que no resulten necesarios para los usuarios no administradores, especialmente dispositivos USB, unidades ópticas (CD / DVD Rom), unidades de diskette, etc.
    b. Deshabilitar aquellos elementos de hardware virtuales que no se vayan a ser utilizados tales como puertos serie o paralelos, o acelerador gráfico para tarjetas de video en máquinas virtuales que no requieren de aceleración.
    c. Se deberán controlar las funcionalidades que permiten la comunicación y entrega directa de información entre las máquinas virtuales y otras máquinas virtuales o entre las máquinas virtuales y el hipervisor que las contiene o el equipo de consulta.
    d. Se deberá evitar el uso de discos no persistentes independientes ya que, a través de éstos, se pueden realizar operaciones que no serán registradas, impidiendo la trazabilidad de las acciones llevadas a cabo.

64. Se deberán implementar, por tanto, los mismos métodos de seguridad, a emplear en máquinas físicas, tales como los siguientes:
    a. Se deberá mantener el sistema operativo invitado al día, en lo que a parches y actualizaciones de seguridad se refiere, del mismo modo que se debería hacer en un equipo físico con el mismo sistema operativo.
    b. Se deberá evitar el uso de puertos, servicios o protocolos innecesarios a través del sistema operativo invitado. Por lo que se deberá aplicar la seguridad necesaria para ello como si de una máquina física se tratara.
65. Se deberán implementar aquellas soluciones antivirus o antimalware, así como cortafuegos por software, que aplicarían en una máquina física equivalente.
66. Se deberán utilizar herramientas adecuadas que permitan el control, la trazabilidad, la monitorización y los registros de logs de forma persistente. Se debería hacer uso de servicios de logs externos para almacenar registros de información del sistema y seguridad.
67. Los usuarios que accedan a la máquina virtual deberán poseer permisos específicos para aquello que les está permitido y pertenecerán a grupos personalizados basados en roles.
68. Las máquinas virtuales deberán hacer uso de accesos con contraseñas robustas y, en la medida de lo posible, se establecerán métodos adicionales de autenticación. Deberá existir una política de bloqueo o desconexión por inactividad, así como un método de bloqueo ante varios intentos fallidos de acceso.
69. Se deberá hacer uso de un servicio de sincronización de hora o de las herramientas que proporcione la arquitectura de virtualización para garantizar la fiabilidad de los registros, así como el correcto funcionamiento de las máquinas virtuales.

9.6 SEGURIDAD DE LA INFORMACIÓN

70. Se deberán aplicar medidas de seguridad en la información contenida en discos duros y máquinas virtuales, así como en los elementos que participan de la infraestructura que puedan revelar información relativa a elementos de la infraestructura que permitan encontrar puntos vulnerables o modos de vulnerar la seguridad. La información deberá ser transportada por canales de comunicación seguros y con métodos de cifrado robustos.
71. La información contenida en elementos comunes y máquinas virtuales solamente deberá ser accesible por aquellos usuarios y equipos o servicios que deban acceder a la misma. Se deberá, por tanto, establecer una segmentación de red que permita el aislamiento de las diferentes redes que no tengan que intercomunicar con otras debido al tipo de escenario y sobre todo a la información que manejan o su grado de clasificación.

72. Aquella información de carácter compartido que deba ser accesible de forma remota deberá responder a los principios de aislamiento y seguridad expuestos. De este modo, será necesario deshabilitar aquellos puertos, protocolos o servicios que no resulten necesarios para el correcto manejo y almacenamiento de la información. Así mismo, tal y como se ha expuesto en la aplicación de medidas de seguridad en la capa relativa a máquinas virtuales, aquellas máquinas virtuales que contengan información, sobre todo si es sensible o clasificada, deberán responder a los métodos de aislamiento y control de accesos para evitar el filtrado de esta.
73. El control de accesos se deberá hacer a través de mecanismos que permitan la segregación de roles personalizada para establecer solamente los permisos específicos necesarios para el manejo correcto de la información, según se tenga acceso a ella para su lectura, escritura, eliminación o incluso modificación de dichos permisos específicos.
74. Se deberán mantener al día, en lo que se refiere a actualizaciones de seguridad, todos aquellos dispositivos o equipos que contengan información y los dispositivos desde los que se acceda a la misma.
75. Deberán existir mecanismos de monitorización del manejo de la información y registros de logs que permitan la trazabilidad de información relativa a qué y quién han accedido a, modificado o destruido la información. El nivel de detalle de estos registros dependerá de la criticidad y clasificación de dicha información. Así mismo, ésta se deberá poder almacenar en servidores dedicados de registro de eventos que permitan una mayor persistencia de dichos registros y que, por tanto, permitan una posterior trazabilidad en caso de pérdida, alteración o fuga de la información.
76. Por último, se deberá establecer un mecanismo que permita la ejecución, almacenamiento y recuperación de copias de seguridad de la información contenida en las máquinas virtuales y recursos o almacenes de datos, esa información copiada deberá, a su vez, cumplir con los métodos de seguridad de la información que se aplican a los datos de origen.

ANEXO A. BUENAS PRÁCTICAS GENERALES PARA LA IMPLEMENTACIÓN DE CENTROS DE DATOS VIRTUALES

La seguridad en la implementación de centros de datos virtualizados tiene la misma premisa que cualquier otro sistema tradicional, "**minimizar la superficie de exposición**" y "**asegurar todos los elementos y servicios desplegados**". No obstante, al tratarse de entornos con una infraestructura virtualizada supone que asegurar dicha superficie de ataque sea más difícil debido a la multitud de recursos compartidos y a los sistemas operativos que funcionan simultáneamente con sus propias aplicaciones sobre la arquitectura virtual implementada en un host de virtualización.

Es por ello por lo que, se debe realizar un **doble esfuerzo para reforzar la seguridad**, no solo del sistema, el cual puede contar con múltiples servicios ofrecidos por máquinas virtuales, si no también, un refuerzo de seguridad sobre la arquitectura de virtualización que permite la implementación de dichos sistemas virtualizados.

Una "**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 para el conjunto "hipervisor-anfitrión-invitado".

La principal cuestión de seguridad en lo que respecta a **la implementación segura de centros de datos virtuales**, es que se debe tratar al sistema como un centro de proceso de datos completo donde establecer medidas de seguridad perimetrales sobre el host de virtualización en este caso, y medidas de seguridad individuales para cada uno de los sistemas dentro del mismo host.

A continuación, se detalla una serie de medidas de seguridad generales para la implementación y administración segura de un centro de datos virtuales:

a) **Planificación**. Es recomendable realizar una correcta **planificación del sistema virtualizado,** así como la arquitectura de virtualización que va a albergar dicho sistema o sistemas. Para ello, se debe tener en cuenta un correcto dimensionamiento para la creación de máquinas virtuales del sistema a las necesidades reales y a los recursos de hardware disponibles en el host.

b) **Gestión de recursos**. Cuando en un mismo host de virtualización conviven varios sistemas, debe llevarse a cabo una correcta **gestión de los recursos** debido a que los hosts de virtualización no son sistemas ilimitados de recursos y una gestión no adecuada de los mismos puede implicar una degradación de todo el sistema o incluso la perdida de servicio en los casos más críticos. Esta medida se encuentra totalmente relacionada con el correcto dimensionamiento del sistema o sistemas virtuales.

c) **Almacenamiento**. Se debe diseñar un aislamiento lógico adecuado para cada, siguiendo los requerimientos de seguridad indicados en el apartado 9.3 SEGURIDAD DEL ALMACENAMIENTO DEFINIDO POR SOFTWARE.

d) **Datos críticos**. Es imprescindible **mantener seguros los datos críticos**, por lo tanto se recomienda cifrar los ficheros de máquinas virtuales, instantáneas y discos duros virtuales destinados al almacenamiento de la plataforma de virtualización, tal y como se indica en el apartado "9.6 SEGURIDAD DE LA INFORMACIÓN".

e) **Aislamiento**. Se debe garantizar el **aislamiento de los sistemas** de la arquitectura de virtualización, por ello, no se debe emplear una tarjeta de red física para dos propósitos diferentes, como puede ser gestionar la arquitectura de virtualización y administrar el sistema.

f) **Múltiples sistemas.** En caso de que existiesen **varios sistemas** dentro del mismo host de virtualización, se recomienda que la separación de la infraestructura de comunicaciones cuente con **uno o varios firewalls** ya sean físicos o lógicos, que permitan solo el tráfico de red autorizado para dicho sistema, y a su vez, separe y aísle cada uno de los sistemas, además de evitar el código dañino y los intentos de ataque de los sistemas operativos.

g) **Auditoria**. Se recomienda disponer de un registro de las tareas de administración de la infraestructura de virtualización, el cual posibilite en caso de sufrir algún incidente de seguridad, disponer de un registro que permita realizar un análisis forense del incidente sufrido.

h) **Roles de usuarios**. Se recomienda realizar una **segregación de los roles de los usuarios**, administrando y gestionando dichos roles de manera que usuarios con privilegios de administración sobre la arquitectura de virtualización no dispongan de permisos para la creación, gestión o incluso visionado (si la tecnología lo permite), de las máquinas virtuales alojadas en el host de virtualización.

i) **Planes de recuperación.** Es recomendable la implementación de una política de **copias de seguridad,** que respalde los sistemas, evitando la perdida de datos o la funcionalidad de las máquinas virtuales del sistema en caso de sufrir una catástrofe. Se recomienda establecer una **política de copias de seguridad** que contengan como mínimo, una copia completa de todas las máquinas virtuales del sistema alojado fuera del host de virtualización del sistema y que se actualice de forma periódica en función de las necesidades y criticidad del sistema.

j) **Mantenimiento de los sistemas.** No se recomienda en ningún escenario mantener **puntos de control** (snapshots) de las máquinas virtuales de los sistemas alojados en la arquitectura de virtualización, así como el empleo de dichos puntos de control como copias de seguridad. Solo se contempla el uso de puntos de control cuando una máquina virtual va a sufrir una alteración importante, como medida de precaución y marcha atrás. Una vez finalizados esos cambios y comprobado que el sistema funciona con normalidad, se deberá realizar un borrado seguro de los puntos de control creados.

k) **Ubicación de copias de seguridad.** También se recomienda que las copias de seguridad del sistema **no sean alojadas en la misma arquitectura de virtualización**, o que cada cierto tiempo se envíe una copia completa del sistema fuera de la arquitectura de virtualización para salvaguardar la información en caso de que ésta sufra una catástrofe. Dicha copia siempre debe estar cifrada independientemente del grado de sensibilidad o clasificación de la información que contenga dicha copia.

l) **Actualizaciones del fabricante.** Es recomendable, además de mantener el sistema con las **últimas actualizaciones** de seguridad, revisar e implementar periódicamente las actualizaciones que los fabricantes publican de los hosts de virtualización o de sus sistemas operativos, **reduciendo la exposición** ante vectores de ataque tratados por el fabricante en sus parches de actualización.

m) Se recomienda el **uso de plantillas de configuración para la creación de máquinas virtuales** para minimizar el riesgo de configuraciones erróneas y la pérdida de control

sobre el nivel de seguridad aplicado.

n) Se recomienda la creación de **imágenes preparadas de máquinas virtuales previamente bastionadas** y mantenidas con los últimos parches de seguridad y, a partir de éstas, crear plantillas específicas de aplicaciones según las diferentes necesidades operativas.