SEGURIDAD DE CABLEADO Y DATACENTER

Unidad 2

Seguridad de almacenamiento en el *datacenter*

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Eder Morán Heredia

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Trinidad Marshall

VALIDACIÓN

Experto disciplinar: Gabriel Urra Varas

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Welearn

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Configuran redes definidas por *software* considerando gestión y monitoreo de seguridad del *datacenter* basado en máquinas virtuales.

Fuente: Freepik. (s.f)

Introducción

¿Cuáles son las ventajas de la virtualización?

El panorama actual hace necesario buscar soluciones integrales a las necesidades que van presentando las **TIC** (Tecnologías de Información y comunicación). Esto trae como consecuencia que la solución más utilizada en la actualidad sea la **virtualización**, concepto acuñado en los años 60 bajo el contexto de los sistemas *mainframe* introducidos por IBM.

Uno de los más grandes retos que se presentan actualmente es el aseguramiento de este tipo de entornos, que, a diferencia de la infraestructura física, plantea nuevos desafíos. Al contrario de los espacios físicos, la virtualización basa su operación en que uno o varios servidores físicos pueden contener varios sistemas operativos hospedados en una misma plataforma. Es aquí donde la **seguridad de ambientes virtuales** juega un papel muy importante.

La virtualización de archivos, lo que esta representa flexibilidad para el administrador, conlleva una vulnerabilidad que puede ser usada para robar la máquina completa. En consecuencia, dichos equipos pueden ser víctimas de diversos tipos de ataques de parte de una máquina virtual hacia otro residente en el mismo equipo físico. Por lo tanto, en seguridad informática se toman medidas preventivas o de respuesta a eventos de este tipo.

La **seguridad virtual** se extiende más allá de las máquinas, los sistemas de almacenamiento y el espacio virtual. Se deben tomar medidas tales como mecanismos de autenticación, controles de acceso robustos, control de accesos y de operación,

corrección de vulnerabilidades e instalación de actualizaciones de seguridad, configuración de auditoría y escaneo de vulnerabilidades. En consecuencia, lo más importante para prevenir o evitar ataques es el uso de **VLAN** (Red de Área Local Virtual) para la separación del tráfico entre máquinas virtuales, además de otras medidas que serán vistas a continuación.

1. Redes Virtualizadas

En las redes virtuales es posible la comunicación entre usuarios, máquinas, servidores y otros dispositivos ubicados en distintos centros de datos y oficinas. Mientras que las redes físicas usan cableados y otros elementos de *hardware* para conectar las computadoras, las redes virtuales amplían estas funciones al usar la gestión de *software* para conectar las computadoras y servidores a través de la red.

Con el uso de versiones virtualizadas de las herramientas de red tradicionales, como *switches* y adaptadores de red, se logra un enrutamiento más eficiente y resulta más fácil cambiar la configuración de la red.

Estas diferentes funcionalidades permiten que los centros de datos abarquen diferentes ubicaciones físicas, y son más novedosas y eficientes para los administradores de red, que ahora tienen la posibilidad de hacer modificaciones sin tener renovarla o adquirir más *hardware*s. Ello hace posible la flexibilidad en el aprovisionamiento de la red conforme as exigencias y aplicaciones específicas.

Además, las funcionalidades de las redes de virtualización son capaces de alcanzar el traslado de cargas de trabajo a través de la infraestructura de la red sin que empeore la calidad del servicio.

1.1 Funcionamiento de las Redes Virtuales

En principio, se considera conectar dispositivos y máquinas virtuales mediante *softwares* independientemente de su ubicación. En una red física, las funciones de las capas 2 y 3 del modelo OSI ocurren en los *switches* y *routers* físicos. Además, es necesario el uso de

Tarjetas de Interfaz de Red Física (NIC o *Network Interface Card*) y adaptadores de red para la conexión de los ordenadores a la red.

Una aplicación de trabajo de *software*, denominada *switch* virtual o **vSwitch**, controla y dirige la comunicación entre la red física existente y a las partes virtuales de la red. A su vez, un adaptador de red virtual permite que los computadores y las máquinas virtuales se conecten a una red.

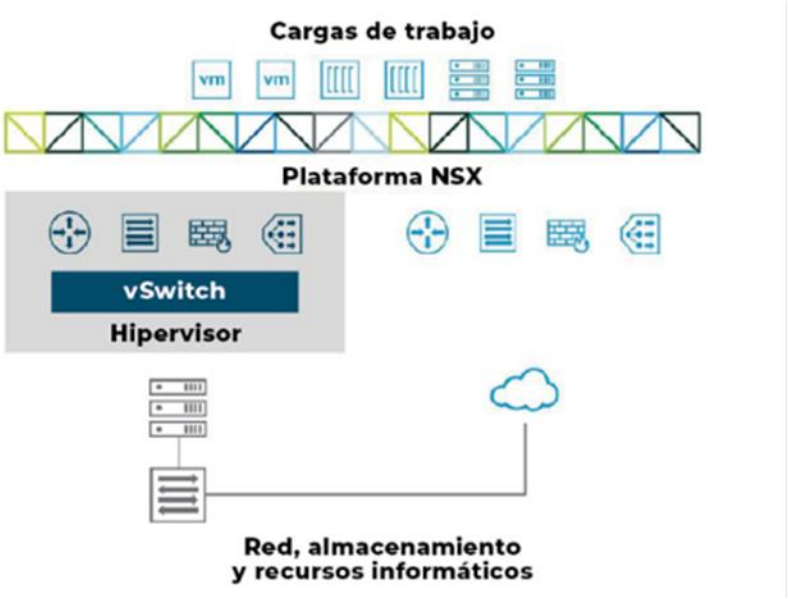


Figura 1: Virtualización

Fuente: encrypted-tbn0.gstatic (s.f)

En una red física, las **LAN** (red de área local) se crean para conectar varios dispositivos, recursos compartidos como el almacenamiento en red, empleando normalmente cables de *Ethernet* o *wifi*. Pero las redes virtuales les abren la posibilidad a las **LAN virtuales** (VLAn), donde la agrupación se configura a través del *software*. Es decir, las computadoras conectadas a diferentes *switches* de red pueden comportarse como si todas estuvieran conectadas, o a la inversa, las que comparten cableado pueden mantenerse en redes independientes en lugar de conectar las máquinas en forma física

mediante *hardwares* y equipos de cableado. Las redes virtuales ofrecen una gestión más centralizada y simplificada de la red. Al realizar actualizaciones o cambios, e incluso llevar a cabo pruebas, es posible acceder de forma remota a las distintas partes de red, lo que hace la gestión más económica y sencilla.

La virtualización de red hace referencia a la desvinculación de los recursos de red que generalmente se proporcionan en forma de *hardware*. También puede combinar varias redes físicas en una red virtual mediante *software* o dividir una red física en redes virtuales independientes y separadas. Además, desvincula los servicios de red del *hardware* subyacente y permite el aprovisionamiento virtual de toda la red.

Los recursos de la red física, tales como conmutadores o enrutadores, se agrupan y están accesibles para cualquier usuario través de un sistema de gestión centralizado. Esto hace posible la automatización de muchas tareas administrativas, lo que reduce errores y tiempos de aprovisionamiento y aumenta la productividad y la eficiencia de la red.

1.2 ¿Qué es y qué ofrecen las VPN?

Las VPN, o ***Virtual Private Network***, son tecnologías de red que permite una extensión segura de la red local (LAN o ***Local Area Network***) sobre una red pública o no controlada como internet. Se desarrollan mediante la encapsulación y la encriptación de paquetes de datos a distintos puntos remotos a través del transporte de datos soportado. Posteriormente, hacen que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada.

Al basarse en internet, esto significa una solución a bajo costo para la implementación de la red a larga distancia. Además, ofrece autenticación de usuarios o equipos

mediante cifrados, firmas digitales o claves de acceso para una identificación inequívoca. Asimismo, asegura la integridad de los datos enviados por el emisor, siendo estos exactos a los que recibe el receptor, y también otorgan una confidencialidad del cifrado. Esto permite que no sea interceptado o interpretado por ningún otro computador o red, y los datos solamente pasan del emisor al receptor.

1.2.1. Requerimientos de una VPN

Para la implementación de una VPN se debe establecer lo siguiente:

- **Set de Políticas de Seguridad**: sirven para la codificación de datos, pues no deben ser visibles por clientes no autorizados en la red.
- **Administración de Claves**: para asegurar la codificación entre cliente y servidor.
- **Compartir datos, aplicaciones y recursos**: con ello se facilita la protección centralizada de las operaciones virtuales y el control con una adecuada infraestructura.
- **Uso de un solo servidor de acceso y autenticación**: para tener control de quiénes ingresan, verificación de identidad y tener registro estadístico sobre acceso.
- **Administración de direcciones**: las VPN deben establecer una dirección para el cliente dentro de la red privada y debe asegurar que estas direcciones se mantengan así.
- **Soportes para múltiples protocolos**: debe manejar los protocolos comunes a la red Internet, como las **IP.**

1.2.2. Tipos de VPN

1. **VPN de acceso remoto**: establecido por usuarios que se conectan a una empresa desde sitios remotos usando internet como vinculo de acceso, una vez realizada la autenticación adquieren derechos de acceso similar a una de red local LAN.

2. **VPN Punto a Punto**: es usado para conectar oficinas remotas con una sede central. El servidor VPN está conectado permanentemente a Internet, acepta conexiones entrantes desde los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet y a través de esta al túnel VPN de la oficina central.

3. **VPN Interna (*over* LAN)**: funciona tal como una red VPN normal a diferencia que dentro de la misma red local LAN, en reemplazo del internet. Sirve para aislar zonas y servicios de la misma red interna, además de la mejora de características de seguridad de una red inalámbrica Wifi.

1.3 Protocolos usados en VPN

Dentro de los múltiples protocolos disponibles para su uso en las VPN, el conjunto estándar es **IPSec** usándose además otros protocolos como **PTP**, **L2F**, **SSL/TLS**, **SSH**, etc.

IPSec (***Internet Protocol Security***) es un conjunto de estándares para incorporar seguridad en IP, y actúa a nivel de capa de red, protegiendo y autenticando los paquetes IP entre los equipos participantes de la red. Esto proporciona confidencialidad, integridad y autenticación a través de algoritmos de cifrado, *hash* de llaves públicas y certificación digital. El IPSec tiene tres grandes componentes: dos de seguridad, **Autenticación de Cabecera IP** (AH) y **Carga de Seguridad de Encapsulado**

(ESP), y uno de seguridad **Intercambio de Llaves de Internet** (**IKE** o Internet Key Exchange).

En el protocolo **AH** es la porción de información de los mensajes emitidos que pasa a través de un algoritmo de *hashing* junto a la clave de autenticación de cabecera. Esta se anexa como cabecera al paquete IPSec al llegar a destino y los datos también se calculan por el mismo proceso de llave por medio del *hash*, y si es similar al de cabecera AH significa que el paquete esta autenticado.

El protocolo **ESP** tiene un funcionamiento similar cuya principal diferencia con AH es que el mensaje es cifrado a través de un proceso criptográfico con la llave ESP. Por lo tanto, solo puede ser cifrado por un receptor que conozca la llave.

El protocolo IKE tiene dos modos de funcionamiento, uno en modo transporte y otro en modo túnel:

- **Modo transporte**: el contenido dentro de un datagrama AH o ESP forman parte de la capa de transporte, por lo tanto la cabecera IPSec se inserta luego de la cabecera IP, antes de los datos que se desean proteger. Además, asegura la comunicación de extremo a extremo, pero entendiendo ambos el protocolo IPSec.

- **Modo túnel**: son datagramas IP completos que incluyen la cabecera IP original. En el datagrama IP se adjunta a la cabecera AH o ESP y luego otra cabecera IP para el direccionamiento de los paquetes a través de la red. Es el protocolo IKE estándar para la configuración de las VPN debido a sus características.

1.4 Implementación de VPN por *hardware*

Los procesos de **encriptación** y **desencriptación** se realizan a nivel físico en los puntos inmediatamente anterior y posterior al comienzo de la línea de comunicación. Para ello necesitaremos equipos que permitan realizar esta operación de forma transparente, generalmente se usan *routers* con VPN incorporada. Estos dispositivos llevan un incorporador, un procesador y algoritmos de encriptación y desencriptación. La ventaja del VPN por *hardware* es que el fabricante ya tiene configurada la implementación y su instalación es sencilla, ya que solo tenemos que intercalarlos en los puntos de salida y entrada en la línea de comunicación y activar en ellos la encriptación y desencriptación. Además, se instalan la configuración de contraseñas o certificación que servirá para la encriptación y desencriptación de la información.

Por otro lado, las VPN implementadas por *hardware* presentan la incomodidad de que el sistema de encriptación viene impuesto por el fabricante y depende del mismo para las actualizaciones.

Entre las problemáticas que se presentan en el uso de VPN por *hardware* están los *router* ***Wireless*** con encriptación mediante **WPA** y/o **WEP**. Esto se debe a que crean un túnel entre el *router* y la tarjeta ***Wireless*** que impide la lectura y modificación de la información. El medio de transporte se realiza por ondas electromagnéticas y por lo tanto la encriptación ocurre a través de la capa física.

Ventajas:

- La instalación de la configuración es relativamente sencilla.
- No necesita personal especializado y su mantenimiento es mínimo.
- Un único elemento puede habilitar varias VPN ubicadas en distintos sitios.
- El sistema es independiente de las máquinas conectadas a la red.
- No se necesitan máquinas especiales para realizar las VPN.

Desventajas:

- Depende de una tecnología externa y cerrada.
- El *firmware* de los sistemas es cerrado y depende del fabricante para modificaciones.
- Los sistemas de encriptación suelen ser cerrados y el fabricante usa un solo tipo.
- Muchas veces los elementos *hardware* de los extremos que componen la red privada deben ser iguales o del mismo fabricante.
- Solo sirven para realizar conexiones VPN dentro de la misma red (intranet) o solo fuera de la red, pero no pueden ser realizados al mismo tiempo.
- La seguridad se implementa desde los extremos de las VPN siendo inseguro el camino que recorre la información desde el ordenador hasta las VPN.

2. Máquina Virtual e Hypervisor

La información que se desea proteger en un *datacenter* reconoce diversos niveles de sensibilidad, es decir, el grado de importancia que tienen los datos en las empresas. A ello se le llama **criticidad de la información**. Además, existen niveles variados de **severidad** y **probabilidad de compromiso**, a menos que los niveles de seguridad para ciertos datos estén prescritos por ley (por ejemplo, seguridad nacional o privacidad) y/o requieran alineación con compromisos regionales o internacionales. La definición de los niveles de seguridad queda a discreción de la organización particular. Esto no significa necesariamente que el cumplimiento de los requisitos legales requiera categorías de clasificación independientes.

3. Redes seguras definidas por *softwares* y *hardwares* en un *datacenter* virtual

Las **Redes Definidas por *Software*** (SDN o ***Software Defined Networking***), también llamadas Redes Programables y Automatizadas, se presentan como una propuesta que brinda mayor velocidad, mayor cobertura, infraestructura ágil y mejores costos en plataformas *Cloud IT*. Esto evita que el administrador de red gestione a bajo nivel por medio de la separación del plano de control y el plano de datos. Entre los desafíos que enfrentan las empresas al implementar SDN, están diferenciar la red actual con la red SDN y conocer los fundamentos de la red SDN.

El desarrollo de SDN se inicia aproximadamente en los años 90 donde se incluyeron las funciones programables en la red. En el período 2001-2007 se separa el plano de control y de datos, mejorando a partir de la etapa del 2007-2010 con la creación del primer **API**, o interfaz de programación de aplicaciones, llamada Open Flow, desarrollado por la Open Networking Foundation (ONF). Se presenta como una interfaz abierta, con diversas maneras de separación del plano de control y de datos para que sea escalable, y en donde la virtualización juega un rol importante en esta evolución de SDN.

3.1 ¿Por qué surge la SDN?

Las SDN surgen como respuesta al problema que tenían los *datacenter* de no poder responder a patrones de tráfico que se comporten de manera diferente a los picos de demanda. Frente a esta situación, se establecen dos alternativas: escalar a una red más cara empleando tiempo de configuración o adecuarse a una red dinámica.

Las SDN se viabiliza hacia los clientes que quieren cambios rápidos y en corto plazo. Se usan actualmente en redes sociales, por lo que tienen mayor demanda o requieren de cambios repentinos (por ejemplo, trabajar sobre tráfico geográfico). Se direccionan hacia los dispositivos móviles, tienen visualización de dispositivos de red y se instalan los servicios en la nube.

3.2 Arquitectura SDN

La conceptualización de las Redes Definidas por *Software* (SDN) se fundamenta en un modelo compuesto por tres capas: el Plano de Aplicación, el Plano de Control, y el Plano de Datos.

En el Plano de Aplicación, las SDN reinventan y automatizan de manera óptima la infraestructura de redes. Su arquitectura tiene por objeto desagregar los Planos de Control y datos en dispositivos de redes como *switches* y *routers*.

El Plano de Control es el encargado de tomar decisiones respecto al tráfico que interactúa con cualquier dispositivo de red, mientras que el Plano de Datos es el que ejecuta las tareas de transporte de paquetes de datos.

En la figura 2 se visualiza la arquitectura de las Redes Definidas por *Softwares*, compuesta conceptualmente por estas tres capas mencionadas anteriormente. También existen **API** que comunican estas tres capas: **API Northbound** (sentido norte) y **API Southbound** (sentido sur). El primero está por encima del Plano de Control, retransmitiendo información a las aplicaciones y la lógica de negocio. El segundo, *Southbound*, está por debajo, realizando la transmisión a los conmutadores y enrutadores para mejorar la gestión de cambios dinámicos en tiempo real. Esto permite

mayor flexibilización y mejor control de la red SDN, además soportan gran variedad de aplicaciones y servicios.

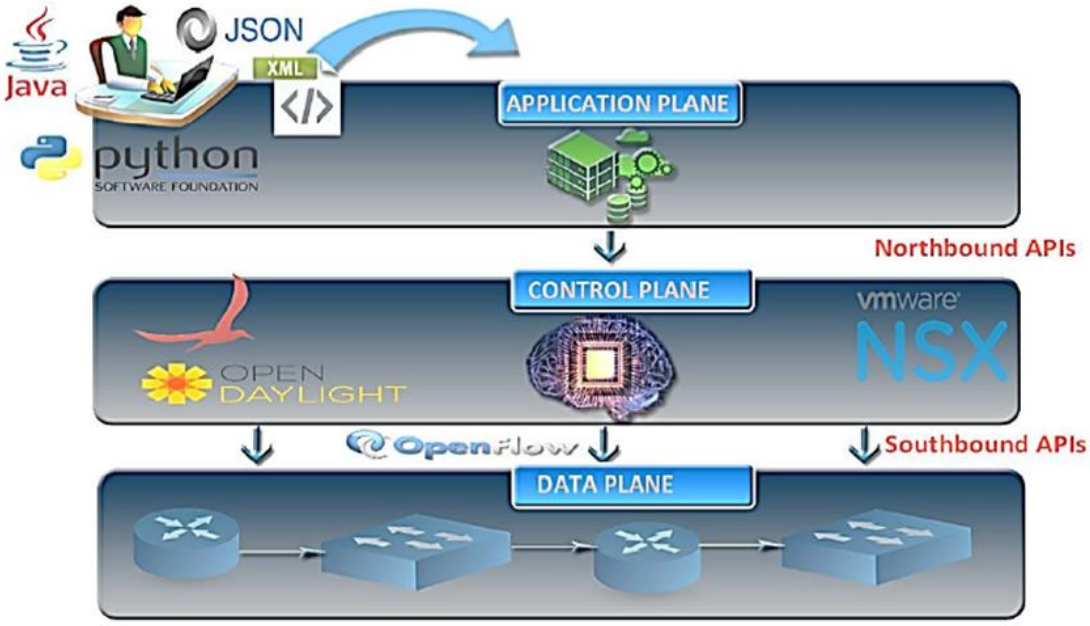


Figura 2: Elementos de Arquitectura de las redes SDN

Fuente: Barrera, M.A; Serrato, N.; Rojas, E; Mancilla, G. (2019).

3.2.1. Capa de Datos

También llamada **Capa de Infraestructura**, se compone de todos los dispositivos de la red, entre ellos los *switches*, *routers* y *access point*, que se encargan de transportar los datos de los usuarios que circulan en la red. Estos dispositivos no cuentan con una funcionalidad predefinida y fija, sino que se caracterizan por tener un *set* de instrucciones dadas por el plano de control. Así un mismo un *hardware* podría funcionar como un *router* o como un *firewall* según como sea definido en la gestión de la red.

3.2.2. Capa de Control

Se encarga de centralizar el control de todo el flujo de información que circula por el ***Data Plane***. Esta contiene las políticas de reenvío o desvío de datos, tablas de flujo, y posee una visión general de toda la red de un controlador SDN. Existen las API Southbound como el protocolo OpenFlow. Esto permite que un controlador como **Opendaylight** o **NSX** envíe el conjunto de políticas y configuraciones a todos los dispositivos que conforman el plano de datos. Su importancia es vital para realizar de manera taxativa la separación de las funciones de los planos de datos y de control. Por otro lado, las API Northbound, al igual que el **API Restful** o **SDMN API**, que definen un lugar central de la infraestructura para mediar las políticas de aplicaciones globales y las políticas de red, permiten comunicar la Capa de Aplicación con la Capa de Control.

3.2.3. Capa de aplicación

En este plano se realiza el desarrollo de aplicaciones de comunicación e interacción con toda la arquitectura de manera veloz con el apoyo de las API Northbound. Estos logran la comunicación de esta capa hacia las capas subyacentes y tienen la capacidad de obtener una perspectiva más abstracta de la red sabiendo desde la cantidad y distribución de los dispositivos hasta la recolección de estadísticas de comportamiento de la red. En ella se toman decisiones sobre su administración, siendo necesario para su desarrollo a través de plataformas de código abierto que aportan a la estandarización, codificación segura y portabilidad. En tal sentido, el desarrollo de aplicaciones con arquitectura **REST**, o *Representational State Transfer*, ha ganado terreno a SDN aportando beneficios con aplicaciones orientadas a servicios sin importar el lenguaje de programación.

4. Red de d*atacenter* virtual

El establecimiento de la **Computación en la Nube** (*Cloud Computing*) se basa en la entrega de servicios de **Tecnologías de la Información** (TI) de baja demanda. El propósito de ello fue alinear mejor las TI con las operaciones de negocios. La Computación en la Nube tiene dos requisitos fundamentales: aplicaciones virtualizadas y un soporte e integración sin fisuras entre componentes, servidores, redes, almacenamiento e hipervisor. Los servicios de TI se habilitan mediante modelos tecnológicos tales como la **Infraestructura como Servicio** (IaaS), **Plataforma como Servicio** (PaaS) y ***Software* como Servicio** (SaaS), que forman parte del concepto de computación en la nube.

La externalización de estos servicios permite aumentar la capacidad de los departamentos de TI para centrarse en la capa de negocio y reducir aún más los costes internos en inversiones tecnológicas.

Un **Centro de Datos Virtual** es un conjunto de recursos en la nube diseñados específicamente para cubrir las necesidades de negocio de las empresas, sin preocuparse de la infraestructura tecnológica necesaria para la implementación. Estos recursos incluyen capacidad de proceso, memoria, almacenamiento y ancho de banda.

Las compañías pueden hacer que estos recursos *Virtual Datacenter* estén aptos para la instalación de aplicaciones, unidades de negocio y proyectos bajo demanda sin tener que preocuparse de la capacidad física de la plataforma. Este nuevo concepto de implementación técnica se conoce como IaaS, o **Infraestructura como Servicio**.

4.1 *Virtual Data Center* frente a la infraestructura tradicional

La Infraestructura de las empresas también se une a la nube con el fin de aumentar la escalabilidad y ahorrar costos. Es, sin duda, la base operativa de la misma, sin infraestructura propia o contratada a un tercero. Prácticamente ninguna empresa actual podría trabajar en esto, por lo que existe una necesidad de servidores que alojen las plataformas de las empresas, bases de datos, páginas web, envío y recepción de correos electrónicos, CRM y un sinfín de utilidades informáticas que cualquier empresa utiliza.

Se debe tener en cuenta la velocidad de crecimiento de una empresa moderna para disponer de una mayor infraestructura en cualquier momento. Se vuelve de vital importancia la utilización del recurso del ***Virtual Data Center*** (VDC), convirtiéndose en una opción muy interesante tanto para pequeñas como grandes empresas.

Los VDC son un ejemplo de los servicios IaaS en la nube, con el cual podemos crear varios **Servidores Virtuales Privados** (VPS) en diferentes países del mundo. Además, se pueden crear redes de interconexión en segundos, aumentar o disminuir los recursos y todo lo que nos ofrezca un proveedor de VDC.

Los VDC son servicios IaaS llevados al extremo, donde simulamos que tenemos nuestro propio *datacenter* físico, pero con las ventajas de la virtualización y la externalización de infraestructura informática, con sus beneficios y desventajas.

Dado que la infraestructura es nuestra, debemos de elegir los servidores, *routers*, *switches*, *firewalls*, etc. Necesitamos comprar todo esto, alojarlo en algún sitio (en las instalaciones de la empresa o en algún centro de procesamiento de datos), montar toda

la infraestructura, conectarlo, instalar todo lo necesario y poner en marcha los equipos y el *software*.

¿Qué significa esto?

Significa que el gasto en infraestructura, contratos de servicios (internet, energía eléctrica, seguridad, etc.) y mano de obra técnica es realmente elevado. A partir de la evolución de la nube y la aparición de los servicios IaaS, los VDC son el producto más demandado en la nube tanto por pequeñas como grandes empresas por sus grandes beneficios:

- **Reducción de costos**: ahorramos las inversiones iniciales, la mano de obra técnica de instalación y montaje, selección de los equipos, etc.
- **Rapidez de despliegue**: podemos crear tantos servidores VPS como queramos en cuestión de segundos.
- **Escalabilidad**: aumentamos y disminuimos el tamaño de los servidores con un par de clics, lo que no permite adaptar nuestra infraestructura a la necesidad real de la empresa.
- **Seguridad**: las nubes empresariales de proveedores fiables son extremadamente seguras, muchos más que la infraestructura física.
- **Gestión centralizada**: A través de un panel web tenemos control absoluto sobre infraestructura, gestionando todo desde un único lugar.
- **Balanceo de carga en tiempo real**: implantación de unos balanceadores de carga en cuestión de segundos repartiendo la carga entre los diferentes servidores virtuales que decidamos, sin complicaciones ni configuraciones.

- **Máxima contingencia**: en los VDC podemos tener copias de los servidores VPS de la empresa prácticamente al mismo tiempo que el original. Esto significa que, si tenemos un problema con algún servidor, podríamos recuperar una imagen anterior rápidamente

5. Sistemas de Monitoreo de Equipamiento y Servidores Virtuales

Monitoreo: es el uso de un sistema de monitoreo constante de los servicios en una red de equipos, en busca de fallas, para notificar a los administradores de red. Esta notificación es por vía correo, mensajes de texto u otro tipo de mensajes.

Un sistema de monitorización de cualquier dispositivo que se encuentra conectado a nuestra red tiene las funciones de obtener datos desde sus monitores que ya vienen predefinidos o la creación de alguno que cumpla con nuestras necesidades. Para poder monitorear se pueden usar **SNMP** en sus dos formas, *Polling* o *Trapping*, y la monitorización en servidores hace uso de agentes instalados previamente

5.1 Herramientas Para el Monitoreo de Redes

5.1.1. Zabbix

Viene con un interfaz que nos permitirá la monitorización y representación de los datos, configuraciones de monitores alertas y la administración de los usuarios. Permite visualizar la gravedad de un incidente y en base a esta configuración se tomarán acciones. Se pueden armar plantillas sobre las cuales se determinará el monitor y el disparador de alerta correspondiente. **Zabbix** almacena los valores que se obtuvieron de la monitorización de la base de datos **MySQL** y a partir de esto se realizarán las gráficas.

5.1.2. SolarWinds

Proporciona una administración de configuración accesible y sencilla, en forma independiente o se integrada con **SolarWinds NPM**. Es una herramienta que administra los archivos de la configuración de nuestra red por medio de una interfaz web. Permite acceder a la configuración de los dispositivos y de alertas sobre cualquier cambio que se efectúe. No es necesario un inicio de sesión por *telnet* o SSH con el dispositivo para cambiar algún parámetro de configuración todo en tiempo real.

5.1.3. Cacti

Una herramienta para monitorear los archivos y presentar estadísticas de redes y servidores. Está basada en RRDTool, dando cierto énfasis en la interfaz gráfica. Toda la información del monitoreo se guarda en una base de datos **MySql** y su interfaz está basada en el lenguaje de programación **PHP**. Entre las funciones de monitoreo que tiene en medir la carga de **CPU** y su capacidad. Emite alertas basándose en umbrales y estructura de manera jerárquica, usa **SNMP** para la captura de datos (o por medio de ***Scripts***).

5.1.4 Nagios

Usada actualmente por los administradores de sistemas y de red para comprobar la conectividad de los *hosts* y garantizar que los servicios de la red están funcionando como se esperaba. Es una herramienta orientada a la supervisión de los recursos de red, enviando notificaciones por vía correo electrónico, mensajes de texto, *popups*, etc. Su función es la de observar y verificar los comportamientos de los servicios de la red tales como **hhtp**, **SQL**, **SSH**, etc. O al del *host* como *router*, *switch*, impresora u otros.

5.2 Servidores Virtuales

La **virtualización** se define como la ejecución de varios sistemas operativos simultáneos en forma aislada en un solo sistema. En general se utiliza un **hipervisor** que es una capa de *software* o subsistema que ejerce control sobre el *hardware* permitiendo la ejecución múltiples sistemas operativos invitados en una sola máquina física llamada **anfitrión**.

5.3 Hipervisor

Para la virtualización de una máquina virtual existen dos formas de llevarlo a cabo, una se denomina **Hipervisor de tipo 1** y la otra **Hipervisor de tipo 2**. Para ambas el *hardware* debe funcionar igual que una máquina real y se debe poder instalar sobre ella cualquier sistema operativo.

5.3.1. Hipervisor Tipo 1

Es una primera forma para virtualizar una máquina virtual en donde el sistema operativo es el único proceso que se ejecuta en modo ***kernel***. Su función es hacer copias de su propio *hardware*, a lo cual se denomina máquina virtual. Su ejecución funciona de una forma semejante a los procesos de un sistema operativo normal. Algunos hipervisores tipo 1 conocidos son **VMware ESXi**, **Xen**, **Citrix XenServer** y **Microsoft Hyper-v Server**. Entre la virtualización de tipo 1 se pueden distinguir a su vez dos subtipos:

1. **Arquitectura monolítica**

La arquitectura monolítica es compleja, ya que cuando una máquina virtual realiza una llamada al *hardware*, el *hardware* virtualizado la redirecciona hacia los *drivers* en el

hipervisor. Posteriormente, enruta esa llamada al recurso real, como por ejemplo el VMware ESXi. El proceso de una llamada al *hardware* en un sistema virtualizado usando un hipervisor de tipo monolítico es el siguiente:

- El *hardware* emulado debe interceptar la llamada.
- El **Monitor de Máquina Virtuales** (VMM) redirige las llamadas hacia los *drivers* de dispositivos que operan dentro del hipervisor, lo cual requiere de varios cambios de contexto en el código de llamada.
- Los *drivers* del hipervisor enrutan la llamada hacia el dispositivo físico. Este funcionamiento implica desarrollar drivers específicos para el hipervisor de cada componente *hardware*.

2. Arquitectura micro-kernelizada

Esta arquitectura es más sencilla porque las máquinas virtuales no requieren de *drivers* específicos, accediendo directamente al *hardware* por medio de los *drivers* usados por el hipervisor. De esta manera el hipervisor será como una capa transparente dedicada a separar y administrar las distintas máquinas virtuales. Así se puede aumentar el rendimiento mediante la reducción de códigos intermediarios y el número de cambios de contexto. Además, se puede aumentar la estabilidad de los sistemas al existir menos componentes, disminuyendo la superficie de trabajo del hipervisor.

5.3.2. Hipervisor tipo 2

Esta segunda forma de virtualizar una máquina virtual se denomina hipervisor funciona encima de un sistema operativo anfitrión. De esta forma, el sistema operativo funciona

como un programa de usuario donde las líneas de código se procesan y se sitúan en el caché para su ejecución. Un hipervisor tipo 2 conocido es **VirtualBox**.

5.4 Paravirtualización

Otra forma de virtualizar un sistema operativo es la **paravirtualización**, que consiste en hacer modificaciones al código fuente del sistema operativo invitado, de manera que no efectúe llamadas sensibles, sino que se realicen llamadas al hipervisor. Utiliza una interfaz en donde se registran las operaciones a las cuales pueden acceder o llamar los **SO**. Este interfaz forma una API (Interfaz de Programación de Aplicaciones), de tal forma que el hipervisor se transforma en un **microkernel**. Estas usan instrucciones sensibles por motivos de falta de acceso al código fuente del sistema operativo invitado en el caso de *Windows,* o por las diversas distribuciones de *Linux*.

5.4.1. Ejemplos de Hipervisores

1. **KVM** (Máquina Virtual basada en el *Kernel*)

   Es un hipervisor de tipo 1 que se usa para lograr una virtualización completa para *Linux* en arquitecturas **x86** y posee extensión de virtualización para **Intel VT** y **AMD-*v***. Su estructura consta de un módulo de núcleo **kvm.ko** que brinda infraestructura de virtualización de núcleo y un módulo especifico de procesador, **KVM-Intel.ko** o **KVM-amd.ko**.

   KVM es un *software* de código abierto, el componente de espacio de usuario de KVM se incluye en la línea principal de **QEMU**.

Figura 3: Logo de KVM

Fuente: i.blogs.es (s.f)

2. Qemu

Es un emulador y una máquina de virtualización que permite la creación de máquinas virtuales dentro de un sistema operativo. El uso de QEMU como emulador de máquinas virtuales permite utilizar sistemas operativos y programas en una máquina diferente. Si se utiliza en modo *kernel* se ejecutará con el hipervisor **Xen** o **KVM**, si se usa con KVM se pueden usar arquitecturas **x86 Power PC**.

Figura 4: Logo de Qemu

Fuente: libdepo.github.io (s.f)

3. VirtualBox

Es una solución de virtualización con sistemas operativos invitados, un hipervisor tipo 2. Fue desarrollado en Innotek Sun Microsystems y en la comunidad Linux. Puede ejecutar máquinas virtuales de 32 y 64 bits **Linux**, **Microsoft Windows**, **Solaris**, **BSD** o **IBM OS/2** en *hosts* Microsoft Windows, Mac OS, Linux y Opensolaris.

Figura 5: Logo VirtualBox

Fuente: encrypted-tbn0.gstatic.com (s.f)

4. VMware

Es uno de los primeros en ofrecer soluciones para sistemas operativos Windows como Linux. Tiene soluciones de virtualización en todos los niveles y para todas las necesidades. Este compuesto de un sistema operativo que suministra el entorno de gestión, administración y ejecución al *software* hipervisor (hipervisor tipo 1), y de los servicios y servidores que permiten la interacción con el *software* de gestión y administración de las máquinas virtuales.

Figura 6: Logo de WMware

Fuente: pngwing (s.f)

Permite ejecutar sistemas operativos dentro de un mismo *hardware* de manera automática. De esta forma se aprovechan los recursos de todas las máquinas virtuales conectadas a la red la mayor parte de las instrucciones. Se ejecutan directamente sobre el *hardware* físico, también permite importar maquinas físicas para su uso como máquinas virtuales. Dependiendo de su versión este puede ser un hipervisor de virtualización completa o paravirtualización.

Posee algunas versiones tales como:

- VMware ESX Server.
- VMware Vsphere.
- VMware Player.
- VMware Server.
- VMware WorkStation.

5. Citrix XenServer

Es un hipervisor de tipo 1 que adiciona una gestión eficiente de Windows y Linux en el uso de máquinas virtuales. Ofrece una plataforma extremadamente económica para aplicaciones de escritorios y la consolidación de servidores Citrix crea nuevas características. Este fue el primer hipervisor en integrar gráficos virtualizados con **NVIDIA GRID vGPU**, y al introducir en memoria caché de lectura para apalear el almacenamiento de **E/S** aumenta el rendimiento.

Figura 7: Logo de Citrix XenServer

Fuente: sergiocambrablog (2015)

Soporta la virtualización de **GPU Intel GVT-g**, un aGPU incorporada a la CPU que no requiere *hardware* adicional. Se integra con la concesión de licencias de **XenApp/XenDestokp**; no se requieren licencias **Xen Server** para apoyar proyectos de

virtualización. Ofrece GPU de paso a través de virtualización e implementaciones de GPU que son superiores a las implementaciones que se basan en interceptación basados en *hardware* como **VMware vSGA**. Optimiza el escritorio de Citrix los gráficos, las cargas de trabajo y las cargas de trabajo en la nube, como **XenApp** y **XenDestokp**, con un precio más competitivo.

6. Hyper-V

El hipervisor Hyper-V permite la administración de un entorno informático virtualizado usando tecnología de virtualización integradas en ***Windows Server***. Dentro de los componentes de instalación incluyen el hipervisor de *Windows*, el servicio de administración de máquinas virtuales de Hyper-V, el proveedor de **WMI** de virtualización, y otros componentes de virtualización como el **Bus de Máquina Mirtual** (VMbus), el **Proveedor de Servicios de Virtualización** (VSP) y el **Controlador de Infraestructura Virtual** (VID).

Figura 8: Logo de Hyper-V

Fuente: access.on.ca (2020)

Las herramientas de administración de Hyper-V se componen de lo siguiente:

- **Herramientas de administración basadas en la interfaz gráfica de usuario**: contienen un administrador de Hyper-V, un complemento ***Microsoft Management Console*** (MMC) y un administrador de conexión.

- **Cmdlets específicos de Hyper-V para powerShell-Windows Server 2012**: ***Cmdlets*** es la funcionalidad más pequeña de ***Shell***, incluye un módulo de Hyper-V que entrega accesos de la línea de comandos a toda la funcionalidad disponible den la **GUI** (Interfaz Gráfica de Usuario).

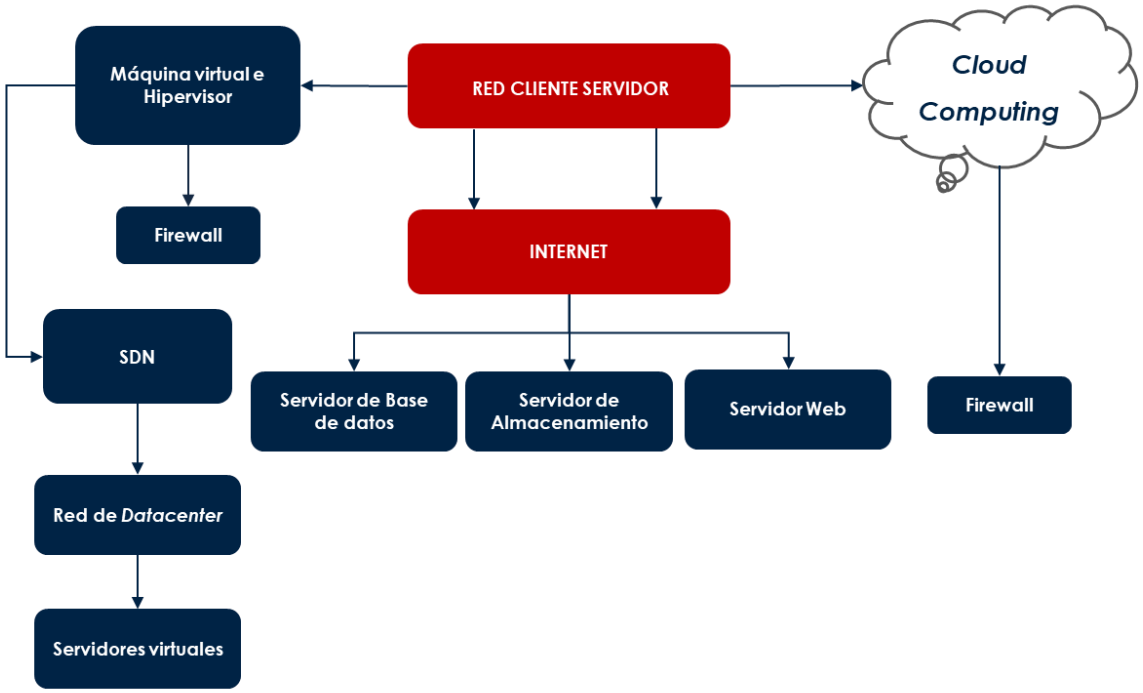
7. Proxmox

Es una muy fuerte plataforma de virtualización. Es una solución **GNU** que ofrece servicios similares a los más populares productos de virtualización empresarial como **VMware vSphere**, **Citrix Xen Server**, **Microsoft Windows Hyper-V.**

Siendo Proxmox libre de costo se puede instalar en servidores físicos y construir un clúster sin límites en la cantidad de servidores físicos, *sockets* de procesador, puentes físicos, **Puentes de Alta Comunicación** (iSCSi), entre otros.

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana: Seguridad de almacenamiento en el *datacenter*.



¿Cuáles son las ventajas de la virtualización?

- Permite un aislamiento de las particularidades de los dispositivos.
- Conseguimos que el usuario vea los recursos que necesita como si fueran dedicados.
- Nos permite homogenizar todos los recursos, por lo que se llega a estandarizar procedimientos y configuraciones.

- Mejora la tolerancia a fallos.
- Aporta con el ahorro de costos, mayor eficiencia, flexibilidad y soporte al uso dinámico de procesos.
- Disminución de energía eléctrica y aumento de la capacidad de respuesta.

Referencias bibliográficas

- Abts, D. (2011). *High performance datacenter networks: architectures, algorithms, and opportunities*. Obtenido de https://bit.ly/3oqlVSL

- Mark A. Sportack. (2003). *Fundamentos de enrutamiento IP*. Madrid: Pearson Educación.

- TIA (2005). *TIA Standard: Telecommunications Infrastructure Standard for Data Center*. Obtenido de https://manuais.iessanclemente.net/images/9/9f/Tia942.pdf