Implementación de una red virtualizada empleando tecnologías de administración para el control de acceso a los servicios

T.S.U. Osdair Jaimes Nava, T.S.U. Estefhany Hernández Ortiz, T.S.U. María Isabel Rodríguez Flores, T.S.U. Jim Eduardo Amaro Pulido, I.S.C. Michel Orozco Carrera. I.T.I Erik Gerardo Martínez Galindo.

[a] Universidad Tecnológica del Centro de Veracruz 94910, 20193L001016@utcv.edu.mx, Cuitláhuac, Veracruz y México.
[b] Universidad Tecnológica del Centro de Veracruz 94910, 20193L001075@utcv.edu.mx, Cuitláhuac, Veracruz y México.
[c] Universidad Tecnológica del Centro de Veracruz 94910, 20193L001060@utcv.edu.mx, Cuitláhuac, Veracruz y México.
[d] Universidad Tecnológica del Centro de Veracruz 94910, 20193L001010@utcv.edu.mx, Cuitláhuac, Veracruz y México.
[e] Universidad Tecnológica del Centro de Veracruz 94910, michel.orozco@utcv.edu.mx, Cuitláhuac, Veracruz y México.
[f] Universidad Tecnológica del Centro de Veracruz 94910, erik.martinez@utcv.edu.mx, Cuitláhuac, Veracruz y México.

Resumen

Esta investigación tiene como objetivo la implementación de una red virtualizada empleando tecnologías de administración como SDN (Software Defined Networking, Redes Definidas por Software) y NFV (Network Functions Virtualization, Virtualización de Funciones de Red), llevándola a cabo en un servidor físico con sistema operativo Debian 11, con la finalidad de poseer una infraestructura adecuada para el control de acceso a los servicios y un ahorro de energía en el cual, se aprovecha la máxima capacidad del servidor manteniendo un menor consumo de energía. El desarrollo de una red virtualizada empleando un servidor físico ofrece un despliegue de funciones de red de una manera virtual y quitando la dependencia de hardware propietario, que a su vez permite un mejor ofrecimiento de aplicaciones y servicios en un período de tiempo más corto; por consiguiente, con la innovación de funciones de red virtualizada, podemos reemplazar los nodos de una red física por nodos virtuales. Además, el desempeño de la tecnología SDN (Software Defined Networking, Redes Definidas por Software), el cual actúa como el administrador de la red utilizando otras herramientas de orquestación como Open Mano, OpenDaylight y OpenStack; y la tecnología NFV (Network Functions Virtualization, Virtualización de Funciones de Red), que actúa como la herramienta para crear y separar las redes, routers virtuales, nodos virtuales, la creación y despliegue de instancias, es decir, máquinas virtuales, guían la gestión de los recursos de la red y la seguridad en ella.

Palabras clave – Infraestructura, servidor físico, Tecnologías de administración, Virtualización de red.

Abstract

This research aims to implement a virtualized network by using administration technologies such as SDN (Software Defined Networking) and NFV (Network Functions Virtualization), on a physical server with Debian 11 operating system, in order to have an adequate infrastructure for controlling access to services, and energy savings which takes advantage of the maximum capacity of the server while maintaining a lower energy consumption. The development of a virtualized network by using a physical server offers a deployment of network functions in a virtual way, and removing the dependency on proprietary hardware, which allows a better delivery of applications, and services in a shorter period of time, therefore, through the innovation of virtualized network functions, we can replace the nodes of a physical network by virtual nodes. On the other hand, the performance of SDN (Software Defined Networking) technology which acts as the network manager by using other composition tools such as Open Mano, OpenDaylight and OpenStack; and NFV (Network Functions Virtualization) technology, which act as the tool of creating and separating networks, virtual routers, virtual nodes, creating, and deploying instances, that is virtual machines, guide the management of network resources and network security.

Keywords *– administration technologies, infrastructure, network virtualization, physical server.*

1. INTRODUCCIÓN

Actualmente las infraestructuras de TI (Tecnologías de la Información) son un activo estratégico tanto en organizaciones como en proveedores de servicios tecnológicos, pero la masiva aparición de nuevos protocolos o servicios impulsan a las empresas a realizar cambios en la arquitectura de las redes actuales debido a que este tipo de arquitecturas no se adaptan bien a las necesidades de algunas de las tendencias como son el cloud computing [1] o el internet de las cosas (IoT, Internet of Things), lo que genera una constante demanda de nuevos recursos en la red.

La implementación de los nuevos protocolos o servicios se dificulta por la falta de capital para los costos financieros y operativos, además de la falta de conocimiento ante situaciones complejas. Pero es necesario que las empresas sean capaces de realizar cambios en la red tradicional para poder cumplir con las demandas del usuario final y alcanzar sus objetivos empresariales.

A partir de lo anterior, se propone como solución desarrollar e implementar una red virtualizada mediante un servidor físico, que se fundamenta en SDN (Software Defined Networking, Redes Definidas por Software) y NFV (Network Functions Virtualization, Virtualización de Funciones de Red) [2], para cubrir las demandas mencionadas y permitir el logro de los objetivos de cada organización. Además, contribuye a la reducción en gastos operativos y administrativos, y a disminuir significativamente el consumo de energía eléctrica y el espacio físico necesario.

2. CONTENIDO

Metodología PPDIOO

Para el desarrollo de este proyecto de investigación, se siguió la metodología PPDIOO ("Prepare, Plan, Design, Implement, Operate and Optimize", lo que en español se traduce como "Preparar, Planificar, Diseñar, Implementar, Operar y Optimizar"), creada por Cisco en el año 2008. Esta metodología es utilizada por diversos proyectos en el área de redes y telecomunicaciones [3] y está dividida en seis fases que se detallan a continuación.

P (Preparar)

En esta primera fase, se examinaron las tecnologías que se pondrán en funcionamiento para satisfacer los requerimientos del diseño de red final.

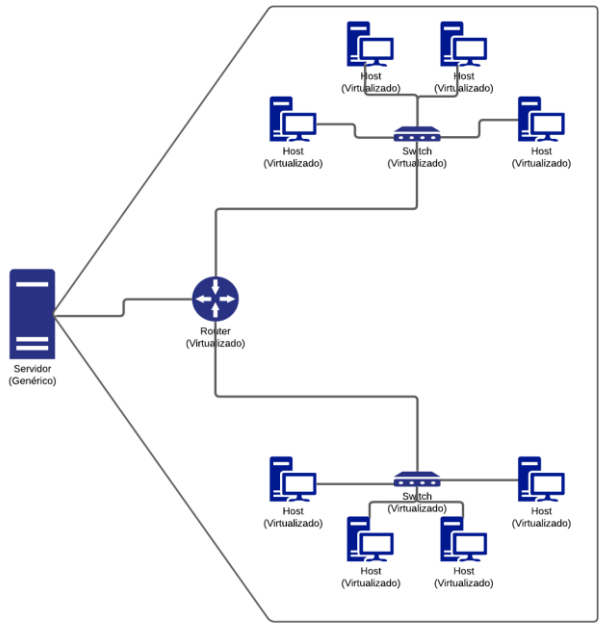

Figura 1. Diseño de la infraestructura de la red virtualizada final.

Para iniciar, se discutieron diversos temas, empezando por el ensamble de un servidor con hardware y software adecuado para virtualizar una red, posteriormente, se consideraron los dispositivos que serían empleados, llegando a la conclusión de que los routers y switches con los que se trabajarán deberían ser virtuales, mientras que los hosts finales pueden compartir esta característica o ser físicos. En cualquiera de estos dos escenarios, se podrá trabajar con ellos sin problema alguno.

Como objetivo principal se pretende el desarrollo de una infraestructura virtualizada que mantenga comunicación, y que sea administrada por las redes definidas por software (SDN, Software Defined Networking), de este modo, se puede "programar y automatizar" la red [4], definiendo aspectos como la dirección del tráfico y la comunicación subyacente. Con la virtualización se pueden sustituir dispositivos de hardware dedicados y costosos, como routers, switches, equilibradores de carga, entre otros.

Algunos riesgos y restricciones que se detectaron fueron: que Debian 11 no cuenta con una documentación completa y extensa para la instalación y configuración de servicios enfocados a herramientas como SDN (Software Defined Networking, Redes Definidas por Software) y NFV (Network Functions Virtualization, Virtualización de Funciones de Red) [5]. Así mismo, estas tecnologías no han sido explotadas ampliamente, por lo tanto, no se tiene algún registro de todas las capacidades con las que cuentan.

P (Planear)

En esta fase, se llevó a cabo la identificación de los requerimientos que serían necesarios implementar, determinando así, la forma en que las nuevas tecnologías se pueden desarrollar para su uso en la red establecida:

1. Primero, se realizó un estudio de campo para analizar los dispositivos de red que se utilizan en una infraestructura de centro de datos, en el cual se vio la necesidad de implementar tecnologías nuevas y actuales para brindar un mejor ahorro en procesos, energía, recursos monetarios, administrativos, entre otros.
2. Se identificaron las tecnologías correspondientes a implementar en la arquitectura de red con el fin de satisfacer las necesidades solicitadas.
3. Se valoraron los requerimientos solicitados, separándolos por requisitos funcionales y no funcionales.
4. A partir de los requisitos mencionados anteriormente, se establecieron herramientas para validar las pruebas del funcionamiento del sistema, con las que se pretende asegurar el cumplimiento de los objetivos que se aspiran obtener.
5. Posteriormente, se realizó una inspección acerca del sitio dónde se ubicaría el equipo, para determinar que éste cumpla con los aspectos necesarios como lo que es la temperatura, humedad, ambiente, entre otros. Además, se consideraron las instalaciones eléctricas, especificaciones de hardware y software que se requieren para el buen funcionamiento del servidor.

D (Diseñar)

Se realizó el bosquejo físico y lógico de la red en donde se muestra el diseño con detalle de ésta, con la finalidad de elegir la distribución apropiada de cada equipo a implementar.

Diseño Físico

El diseño de la red es totalmente genérico ya que se adapta a cualquier tipo de PYME (Pequeña y Mediana Empresa) y a su vez está basado en el modelo jerárquico de tres capas de Cisco (núcleo, distribución y acceso) [6], mismas que se relacionan entre ellas para ofrecer una interconexión escalable, rentable y estable para la empresa o entorno en que se implementa.

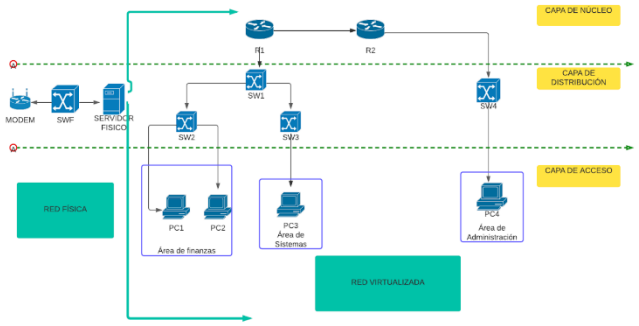

Figura 2. Diseño físico de la infraestructura de red.

Capa de núcleo
Dentro de la capa de núcleo se encuentran situados los enrutadores más eficientes, puesto que mueven información en la red lo más rápido posible. Así mismo, los conmutadores que operan en la capa central reciben y envían los paquetes proporcionando confiabilidad y tolerancia a fallos, logrando que exista escalabilidad en caso de que la red crezca.

Capa de distribución
Se encuentra entre la capa de acceso y la de núcleo. Su propósito principal es proporcionar una definición de límites mediante la implementación de listas de acceso y otros filtros. De este modo, la capa de distribución define las políticas de la red. A su vez garantiza que los paquetes son enrutados correctamente entre las subredes y las VLAN (Virtual Local Area Network, Red de Área Local Virtual) que estén operando con ella.

Capa de acceso
Situada en la parte inferior. Los conmutadores de la capa de acceso se encargan de garantizar la llegada de los paquetes a los dispositivos finales. La incorporación de inteligencia en los switches de capa de acceso permite que las aplicaciones funcionen de manera más eficaz y segura en la red.

Diseño Lógico
Para este diseño se realizó el cálculo de direcciones IP a utilizar; haciendo uso del subnetting y tomando como referencia una dirección IP (Internet Protocol, Protocolo de Internet) inicial de clase C.

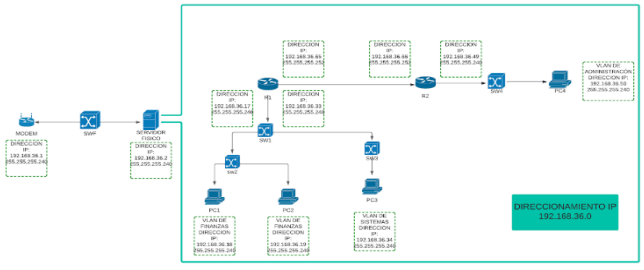

Figura 3. Diseño lógico de la infraestructura de red.

I (Implementación)
Involucra la puesta en marcha de la solución, es decir, la instalación y configuración de las tecnologías mencionadas.

Para el cumplimiento de esta fase se estableció el sistema operativo de software libre Linux Debian 11.

Con la intención de facilitar la integración de las nuevas tecnologías, se establecieron servicios previos. Para la transferencia de archivos entre el servidor y una máquina cliente, se utilizó el protocolo FTP (File Transfer Protocol, Protocolo de Transferencia de Archivos). Primero se implementó a través de repositorios oficiales de la distribución. Después, se realizaron cambios en los parámetros del fichero de configuración. Luego, se efectuaron los cambios con el reinicio del sistema operativo.

Además, en esta fase, se instalaron dos protocolos de acceso remoto, SSH (Secure Shell) y RDP (Remote Desktop Protocol, Protocolo de Escritorio Remoto), para controlar a distancia los cambios realizados en la máquina servidor. De igual forma, se inició con la instalación desde los repositorios oficiales de ambos protocolos. Seguido de esto, para SSH (Secure Shell), se agregaron reglas para filtrar las conexiones entrantes al servicio. Posteriormente se comprobó el estado funcional del servicio. En el caso de RDP (Remote Desktop Protocol, Protocolo de Escritorio Remoto), se agregaron los usuarios que harán uso del protocolo; a continuación, se habilitó e inició el servicio de escritorio remoto y de igual manera con el protocolo SSH (Secure Shell), se añadieron reglas para filtrar las conexiones entrantes al servicio.

```
root@SinOrg:~# sudo mn --switch ovsbr --test pingall
*** Creating network
*** Adding controller
*** Adding hosts:
h1 h2
*** Adding switches:
s1
*** Adding links:
(h1, s1) (h2, s1)
*** Configuring hosts
h1 h2
*** Starting controller
c0
*** Starting 1 switches
s1 ...
*** Waiting for switches to connect
s1
*** Ping: testing ping reachability
h1 -> h2
h2 -> h1
*** Results: 0% dropped (2/2 received)
*** Stopping 1 controllers
c0
*** Stopping 2 links
..
*** Stopping 1 switches
s1
*** Stopping 2 hosts
h1 h2
*** Done
completed in 0.389 seconds
root@SinOrg:~#
```

Figura 4. Creación de la infraestructura de red (Fuente: Elaboración propia empleando mininet).

Con la intención de virtualizar las funciones de red, se hizo uso del emulador **mininet** [7], el cual permite crear redes con hosts, switches, controladores, routers y enlaces a un alto

nivel. En primer lugar, se obtuvo el código fuente de la siguiente dirección: https://github.com/mininet/mininet, una vez realizado, se continuó con la instalación de mininet junto a sus dependencias necesarias. Además, se verificó la funcionalidad básica del emulador como se muestra en la figura 4.

Con respecto al controlador SDN (Software Defined Networking), se emplea Open Day Light (ODL) cuyas características son las mostradas en la tabla 1. Para su integración es necesario que previamente se cuente con java 8 ya que este es compatible con ODL en su versión de lithium seleccionada para utilizar la versión gráfica.

Tabla 1. Características de Open Daylight.

	ODL
Soporte OpenFlow.	OF v1.0.
Virtualización.	Mininet y Open v Switch.
Lenguaje de desarrollo.	Java.
Provee REST API	Sí.
Interfaz Gráfica	Web.
Soporte de plataformas	Linux, Mac OS, Windows.
Soporte de OpenStack	Sí.
Multiprocesos	Sí.
Código abierto	Sí.
Documentación	Media.

Para la integración de los servicios de red propuestos, se desarrolló una topología con un script personalizado de acuerdo con la finalidad de esta. Posteriormente se realizó la emulación de los dispositivos que se especificaron de acuerdo con el script, ejecutando el archivo.py.

Para establecer una conexión entre el controlador y el emulador, primero se ejecutó una topología a la que se le especificó el tipo de controlador, su dirección IP (Internet Protocol, Protocolo de Internet), el puerto y también el uso de OVS (Open vSwitch), así como también de OpenFlow. Se ejecutó un ping para establecer la conexión entre todos los dispositivos y además para hacer visibles los hosts cliente en ODL (Open Day Light). Para comprobar esta conexión se debe recargar la topología en la interfaz gráfica de ODL (Open Day Light), como se muestra en la figura 5. Cabe hacer mención que para establecer una conexión entre una red virtual y una red física se configuró NAT (Network Address Translation, Traducción de Direcciones de Red) en el script de la topología permitiendo así que la primera tuviera conexión a internet, como se muestra en la figura 5.

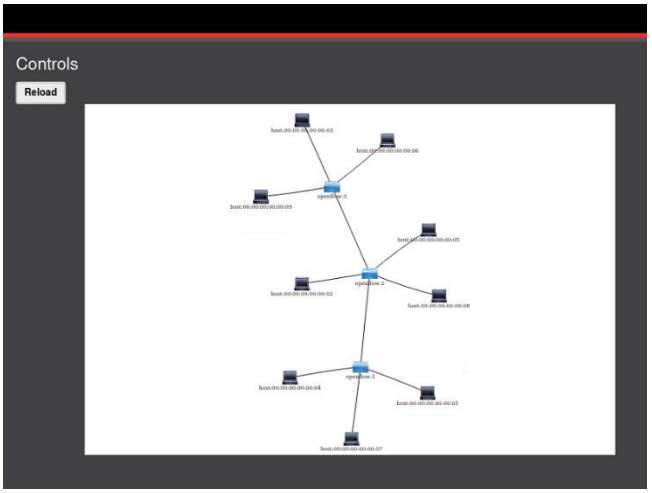

Figura 5. Visualización de la Infraestructura empleando OpenDaylight (Fuente: Elaboración propia empleando mininet y OpenDaylight).

O (Operar)

En esta fase se monitorean los componentes de la red, se administran las actualizaciones y desempeño, mientras que se corrigen los errores encontrados. Para ello, se realizó la instalación del software wireshark que permite tener un monitoreo constante de los dispositivos intermediarios, así como de la red.

Wireshark es un analizador de paquetes de red, con él, se puede capturar todo tipo de información que pasa a través de una conexión [8]. Teniendo eso en cuenta, se puede utilizar para realizar análisis y solucionar problemas encontrados en algún enlace entre los dispositivos o alguna conexión realizada en los hosts.

Esta herramienta fue empleada para corroborar que no existiera una pérdida de paquetes o de comunicación entre los dispositivos que ya se habían creado, reafirmando el envío y tránsito de paquetes en la topología generada, como se muestra en la figura 6. Hay que mencionar que se puede visualizar el tráfico que existe de manera interna, así como, la que se dirige hacia el exterior.

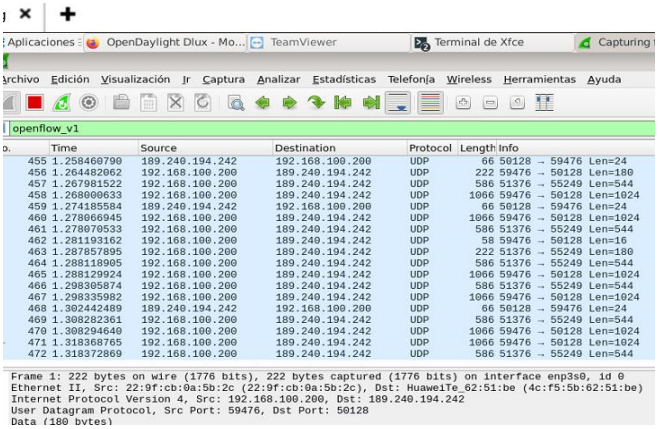

Figura 6. Analizador de paquetes empleando wireshark (Fuente: Elaboración propia empleando Wireshark).

Posteriormente, se realizó una conexión de manera interna-externa, comunicando la infraestructura virtual con internet, logrando hacer ping con los servidores DNS (Domain Name System, Sistema de Nombres de Dominio) de Google. Para lograr realizar esta tarea, primero, se le otorgaron los permisos de escritura y lectura correspondientes a la topología de red virtual, después de agregar dichos permisos, se ejecutó el script para generar toda la infraestructura de red, una vez que ha cargado y virtualizado todos los dispositivos, se procede a realizar un ping del host 1 a internet.

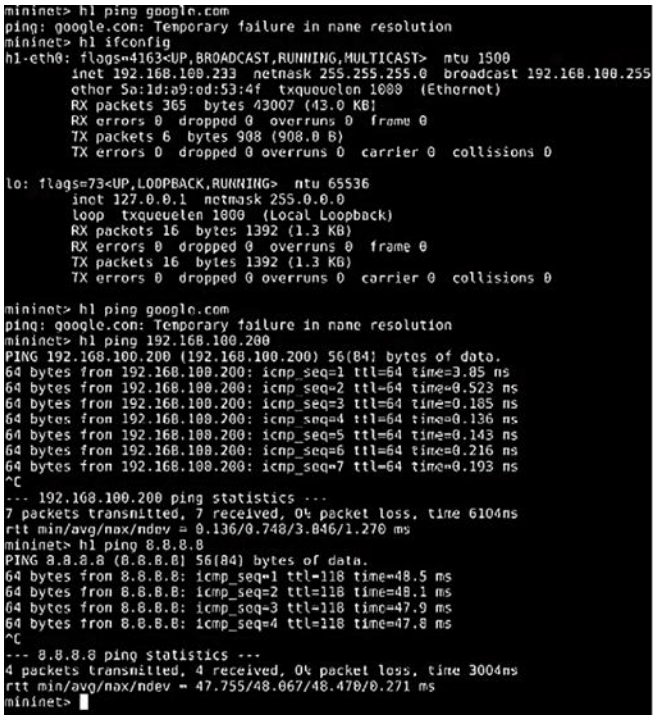

Figura 7. Comunicación exitosa de la infraestructura de red con la dirección IP (Internet Protocol, Protocolo de Internet) de Google.

O (Optimizar)

De acuerdo con la fase anterior se realizaron las correcciones pertinentes, puesto que al poner en funcionamiento la infraestructura se observaron áreas de mejora para obtener un mejor rendimiento. Algunos de los cambios realizados fueron en los scripts que se emplearon para el desarrollo y la creación de la infraestructura, ya que se encontraban comandos que no eran necesarios para los programas y las tecnologías manejadas.

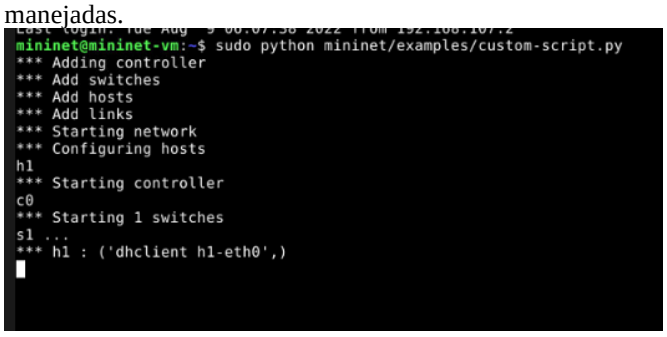

Figura 8. Cambios realizados en la topología.

3. CONCLUSIONES Y RECOMENDACIONES

El uso de tecnologías de administración y acceso a los servicios, trabajando en conjunto, son de suma importancia para los administradores de red, ya que éstas facilitan el trabajo de configuración y operación de la infraestructura. Dichas tecnologías son óptimamente viables para todas las pequeñas y medianas empresas, pues además de ser una tecnología nueva y de gran progreso, es el futuro de muchas empresas ya que facilita el uso y la administración de la red.

Software Defined Networking, en español “Redes Definidas por Software” (SDN) y Network Function Virtualization, en español “Virtualización de Funciones de red” (NFV) son capaces de crear una infraestructura de red completa sin la necesidad de adquirir diversos dispositivos físicos. La ventaja que estas tecnologías presentan es que ayudan a reducir a gran escala los gastos de adquisición de dispositivos, gastos operativos, gastos de consumo eléctrico y ahorro del espacio físico, es decir no es necesario que se emplee un site o cuarto de telecomunicaciones, ya que únicamente se necesita un servidor que cuente con las capacidades adecuadas para poder implementar las tecnologías ya mencionadas, aunque hay que tener en cuenta que las características de cada dispositivo, así como de la infraestructura pueden variar de acuerdo a lo que el cliente requiera.

Una red virtualizada con SDN (Software Defined Networking) y NFV (Network Functions Virtualization, Virtualización de Funciones de Red) tiene varias ventajas y desventajas:

Tabla 2: Ventajas y desventajas de implementar una infraestructura virtualizada

INFRAESTRUCTURA VIRTUALIZADA	
VENTAJAS	DESVENTAJAS
Flexibilidad: este tipo de arquitectura facilita los cambios y adaptaciones a las necesidades del negocio, ya que permite que los recursos de red pueden ser asignados o desasignados según sea necesario.	**Complejidad:** se necesitan habilidades técnicas especializadas para implementar y gestionar la red virtualizada.
Ahorro de costos: se reduce la necesidad de adquisición de hardware al virtualizar los dispositivos y funciones de red, disminuyendo así los costos de operación y mantenimiento. Al reducir la adquisición de máquinas físicas, también se reduce el consumo energético.	**Rendimiento:** la virtualización de la red puede agregar latencia, lo que afecta la velocidad y eficiencia de las comunicaciones.
Mejora de la experiencia del usuario: la	**Requerimientos de hardware y software:** SDN

virtualización de la red permite la implementación de políticas de calidad de servicio (QoS) y una mejor asignación de recursos de red para mejorar la experiencia del usuario.	(Software Defined Networking) y NFV (Network Function Virtualization) pueden requerir actualizaciones de hardware y software existentes, lo que puede resultar costoso. A medida que aumenta el número de máquinas virtuales, otros componentes del ecosistema de TI, en particular, el almacenamiento y las redes, se verán afectados por la capacidad adicional.
Innovación: es rápida la implementación de nuevas funciones y servicios de red.	**Fallos en la red:** ya que la red está más centralizada y depende más del software, puede aumentar la probabilidad de fallos en esta. Por ejemplo, si se daña el disco duro se dañarán todas las máquinas virtuales que se encuentran en él.
Escalabilidad: se pueden agregar nuevos recursos de manera rápida.	**Interoperabilidad:** las arquitecturas de este tipo pueden requerir la interoperabilidad de múltiples tecnologías, lo que puede ser difícil de lograr. Además, no existe estandarización alguna en cómo se crean o gestionan los entornos virtuales, por lo que resulta complicado cambiar de proveedor de servicios cada cierto tiempo.
Automatización: al gestionarse la red de forma automatiza, se pueden reducir los errores humanos y aumentar la eficiencia en la configuración y gestión de está.	
Optimización de la seguridad: una infraestructura centralizada permite ejercer una protección más efectiva. Los archivos, la información y datos dejan de alojarse de manera local en distintos equipos y pasan a almacenarse comúnmente en data centers.	

El emplear redes definidas por software representa un incremento de eficiencia, adaptabilidad, tolerancia a fallos y un mejor control de acuerdo con costos y administración, que, sin lugar a duda, será el futuro al que diversas empresas se inclinarán. Pero también puede aumentar la complejidad y los requisitos de hardware, que son de gran importancia considerar si se decide implementar una red virtualiza con tecnologías como SDN (Software Defined Networking, Redes Definidas por Software) y NFV (Network Functions Virtualization, Virtualización de Funciones de Red).

4. REFERENCIAS

[1] “Mell y Grance - The NIST Definition of Cloud Computing.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[2] “Hervás y Comellas - Software Defined Networking.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: https://upcommons.upc.edu/bitstream/handle/2099.1/21633/?sequence=4

[3] “Morales_CHJA-Torres_LN-SD.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/74675/Morales_CHJA-Torres_LN-SD.pdf?sequence=1&isAllowed=y

[4] “Javier - 2015 - Redes definidas por software (SDN), un nuevo mundo.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: http://polux.unipiloto.edu.co:8080/00002241.pdf

[5] “Rao - A State-of-the-Art Survey.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: https://in.nec.com/en_IN/pdf/NTI_whitepaper_SDN_NFV.pdf

[6] “UPS - TTS377.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/20390/1/UPS%20-%20TTS377.pdf

[7] “MiniNet host talking to Internet | Tech and Trains”. https://techandtrains.com/2013/11/24/mininet-host-talking-to-internet/ (consultado el 20 de enero de 2023).

[8] “185b0a_7a101ef808a548e9add8d5c0b7070514.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: https://fcc08321-8158-469b-b54d-f591e0bd3df4.filesusr.com/ugd/185b0a_7a101ef808a548e9add8d5c0b7070514.pdf

[9] “1390-6712-maskay-6-01-00029.pdf”. Consultado: el 20 de enero de 2023. [En línea]. Disponible en: http://scielo.senescyt.gob.ec/pdf/maskay/v6n1/1390-6712-maskay-6-01-00029.pdf