

Redes definidas por software en centros de datos y en la nube

ASIR Modalidad Presencial

Julián Morón Ridao

Tutor del TFG

ÍNDICES

ABSTRACT

El principal objetivo de este proyecto consistirá en realizar la investigación sobre las redes definidas por software que es nuestro tema principal, además de luego enfocarlo en su uso, aplicaciones, funciones relevantes etc para los centros de datos y la nube. Donde algunos de los apartados que vamos a tratar consisten en los fundamentos de las redes definidas por software, su impacto en los centros de datos y en la nube, limitaciones de este tipo de redes, análisis de estudios de caso, integración en redes 5G, futuro de estos sistemas, sostenibilidad en los centros de datos, normativas y estándares, vulnerabilidades de estas redes entre otros.

The main objective of this project will be to carry out research on software-defined networks, which is our main topic, and then focus on their use, applications, relevant functions, etc. for data centers and the cloud. Some of the sections that we will cover consist of the fundamentals of software-defined networks, their impact on data centers and the cloud, limitations of this type of networks, analysis of case studies, integration in 5G networks, the future of these systems, sustainability in data centers, regulations and standards, vulnerabilities of these networks, among others.

JUSTIFICACIÓN DEL PROYECTO

Mi principal motivación a la hora de la elección de mi tema para este proyecto se basa principalmente en mi gusto por las redes y todo lo que significa en la actualidad. Además, todos los conocimientos que he ido adquiriendo a lo largo de estos 2 años del grado superior de ASIR. En el ámbito de la tecnología, podemos decir que la red es un aspecto crucial que siempre se debe tener en cuenta, es la raíz de muchas soluciones o problemas actuales. Sobre todo, me quiero centrar en las redes definidas por software ya que aportan soluciones más flexibles y eficientes. Mi proyecto va dedicado a diversos públicos, porque mi intención es dar a conocer aspectos claves sobre el tema que sean fáciles de entender y comprender para personas que no saben mucho de tecnologías y redes, pero les gusta todo lo relacionado y también para aquellas personas investigadoras o desarrolladores/ingenieros que trabajen con redes y puedan informarse sobre temas que no comprendan. Hay aplicaciones actuales como Cisco ACI y VMware NSX que trabajan con estas redes y su implementación en entornos de la nube y centros de datos.

INTRODUCCIÓN

Las redes definidas por software ayudan a poder mejorar la gestión y operaciones de muchas de las infraestructuras actuales, ya que algunas de las principales funciones que aportan son:

* Gestión de redes automatizadas
* Permite integrar funcionalidades con el uso de inteligencia artificial
* Implementar análisis en tiempo real
* Administrar de forma eficiente nuestros recursos

Consecuentemente también permite solucionarnos diversos problemas como:

* Las posibles brechas o fracturas en la seguridad de nuestra red
* Falta de control sobre algunas funcionalidades de red
* Poca flexibilidad para la gestión de la red
* Posibles limitaciones en algunos sistemas

Algunos de los requisitos que quiero que tratar con mi proyecto son los siguientes:

- Fundamentos de las redes definidas por software, su arquitectura, protocolos...

- Impacto de las redes definidas por software en los centros de datos y la nube, como su gestión, computación...

- Comparación con el sistema de redes tradicionales en cuanto a eficiencia, seguridad ...

- Posibles limitaciones de este tipo de redes

- Futuro de este sistema de redes

- Análisis de posibles estudios de caso

- Integración con tecnologías actuales como IA, machine learning, Edge computing...

- Automatización de la red

- Integración en redes 5G

- Sostenibilidad en centros de datos

- Normativas y estándares

- Seguridad dentro de las redes definidas por software

- Vulnerabilidades dentro de las redes

- Virtualización de las funciones de red

- Relación de las redes definidas por software y la virtualización de red

- Complementación de SDN y NFV

- Herramientas y plataformas para SDN

- Costes de implementación

OBJETIVOS

Listado de objetivos que se plantean resolver. Requisitos.

Se debe presentar un **RFTP** inicial para acompañar a la propuesta.

R – Requisitos: Lo que debe hacer el programa expresado en lenguaje coloquial.

F – Funciones: Desglose de las características asociadas o subrequisitos de cada requisito. Expresado en leguaje técnico.

T – Tareas asociadas a cada funcionalidad. Deben describir completamente su alcance.

P – Pruebas. Demostración o prueba planificada para cumplir cada tarea.

Ejemplo:

R01 – El programa debe solo debe permitir entrar a las personas que han dado sus datos.

R01F01 – El usuario debe registrarse en el sistema.

R01F01T01 – Crear una tabla usuarios en la base de datos.

R01F01T01P01 – Introducir un dato de prueba.

R01F01T02 - Diseñar un html que permita rellenar los campos de registro.

R01F01T02P01 – Visualizar la pantalla login.html

...

R01F02 - El usuario debe introducir nombre y clave para poder entrar

...

DESCRIPCIÓN

A continuación, está el diagrama de funcionamiento de una red usando SDN, en este caso implementada con Cisco. Usando servidores, PCs, routers y switches multilayer. Además de segmentar la red en diferentes VLANs ya que con esto podemos conseguir mejoras en relación con la eficiencia y la seguridad del tráfico de los datos. El esquema consta de 2 partes:

* Capa de acceso: Donde hemos logrado implementar 4 VLANs, cada VLAN está conectada a los switches multilayer para poder gestionar la comunicación interna de cada segmento.
* VLAN1 (192.168.10.0/24 representado con el color verde): Red para usuarios generales
* VLAN2 (192.168.11.0/24 representado con el color azul):

Red para un grupo determinado de usuarios que queramos

* VLAN3 (192.168.12.0/24 representado con el color rosa):

Red destinada para otro tipo de usuarios

* VLAN4 (192.168.13.0/24 representado con el color amarillo):

Granja de servidores

* Capa de distribución: Lo que hemos hecho es utilizar los switches multilayer, de manera interconectada ya que de esta manera conseguimos crear una topología redundante para conseguir garantizar la disponibilidad la de la red y balanceo de carga. También usamos los router para manejar la conectividad de la red, que están interconectados con la capa de distribución y consiguen poder manejar la conexión entre las VLANs y la salida a redes externas usando diferentes protocolos de enrutamiento.

DISEÑOS

Diagrama de red

Gráfico, Gráfico de líneas

El contenido generado por IA puede ser incorrecto.

Ilustración Diagrama SDN

TECNOLOGÍA

|  |  |
| --- | --- |
| Ilustración Herramienta Cisco | **Cisco**  Cisco es una herramienta muy utilizada en la actualidad para poder crear simulaciones de redes informáticas, pudiendo diseñar y configurar redes virtuales.  En mi casa he tenido que utilizar Cisco para la creación de un esquema que cumpla el modelo de una red SDN |

METODOLOGÍA

**Metodología usada** y justificación de la misma.

Se presentarán dos planificaciones, una valoración inicial y previa a la implementación del proyecto y otra final con el tiempo real dedicado a cada parte del RFTP. Se analizarán las desviaciones.  
El tiempo se expresará en horas. Debe existir una totalización final.

**Diagrama de Gantt** (Microsoft Project o similar). Real, contrastable con GIT, RFTP y Casos de uso.



**Presupuesto.** Con detalle de horas, indispensable si se realiza en grupo, y coste total del desarrollo por cada requisito.

**README y GIT.**

# Fundamentos de las redes definidas por software (SDN)

## ¿Qué son las redes definidas por software?

Las redes SDN, son un tipo de red que destacan por utilizar controladores de software que permiten ser utilizados con interfaces de programación de aplicaciones, que son las conocidas API, que serán de gran ayuda para poder comunicarse con la infraestructura de hardware para dirigir todo el tráfico de la red. Haciendo uso del software, SDN nos permite crear y operar una serie de redes de superposición virtuales que se utilizan en conjunto con una red de superposición física. Las SDN nos ofrecen la posibilidad de entregar entornos con aplicaciones como código y poder llegar a minimizar el tiempo necesario de manipulación para la administración de la red. Una de las principales características de este tipo de red y que la hace destacar, esque separa el plano de control del plano de datos, pudiendo así realizar una gestión de forma centralizada y programable para los dispositivos de la red como podrían ser switches, routers, firewalls ... Gracias a este enfoque, conseguimos mejoras en cuanto a la flexibilidad, tiempo de administración, implementación de medidas de seguridad de forma dinámica entre otras muchas.



Ilustración Ejemplo SDN

## ¿Por qué se usan este tipo de redes en la actualidad?

Actualmente, las empresas sobre todo en el sector tecnológico se interesan en las SDN porque les permite poder aportar los beneficios que ofrece los servicios de la nube para la implementación y administración de las redes. Además de que, si contamos con la opción para virtualizar redes, las empresas podrán contar con una mayor eficiencia al hacer uso de herramientas y tecnologías como podrían ser un SaaS (Software como servicio), IaaS (Infraestructura como servicio) y otros servicios que ofrece la nube para poder ser integrados a través de una API a su correspondiente SDN. Otra característica importante para las empresas, esque también pueden hacer segmentaciones de diferentes redes virtuales usando una única red física o viceversa, diferentes redes físicas para una única red virtual, por eso decimos que las empresas actualmente tienden a usar este tipo de red, debido a que es una manera de poder controlar eficazmente el tráfico y posibilidad a la escalabilidad si llegase a ser necesario.

## Arquitectura de las SDN

La arquitectura de las SDN incluye 3 capas principales que son: El plano de aplicación, el plano de control y el plano de datos.

* Capa de aplicación: Esta es la capa superior de la arquitectura SDN, encargada de poder definir el comportamiento que queremos que tenga la red. Las aplicaciones para esta capa pueden incluir herramientas para controlar el tráfico de datos, políticas de seguridad o superposiciones de redes virtuales.
* Capa de control: La principal función de esta capa es ser responsable de poder aplicar las políticas y reglas definidas en la capa anterior (capa de aplicación). Casi siempre suele estar implementada como un controlador central que llega a comunicarse con los dispositivos de red en el plano de datos.
* Plano de datos o capa de infraestructura: Se forma por todos los dispositivos físicos de red, como podrían ser enrutadores y conmutadores, que forman parte del plano de datos. Todos estos dispositivos son los encargados de reenviar todo el tráfico de red a través de la red.

Ilustración Arquitectura SDN

## Modelos de redes SDN

* SDN Centralizada:

Se caracteriza por tener un único controlador centralizado encargado de gestionar toda la red, siempre estará actuando como el “cerebro” de nuestra infraestructura. Este tipo de controlador posee una visión global de toda la red y envía instrucciones detalladas a los dispositivos de red para saber cómo deben enrutar el tráfico, aplicar políticas de seguridad u optimizar el rendimiento.

#### Características:

- Escalabilidad limitada: Cuando la red va creciendo, el controlador centralizado puede convertirse en un posible cuello de botella.

- Punto único de fallo: En caso de que el controlador centralizado llegase a fallar, toda la red se vería afectada.

- Gestión simplificada: La parte de la configuración y administración de la red, se vería simplificada al poder centralizar las tareas en un único punto.

- Visión global unificada: Permite una perspectiva completa de todo el estado de la red, llegando a facilitar bastante la toma de decisiones.

##### Ventajas:

- Mejora en la seguridad: Si implementamos políticas de seguridad centralizadas podremos llegar a mejorar la protección de la red.

- Reducción de costos: La centralización de toda la gestión pueden reducir significativamente los costes operativos.

- Facilidad a la hora de la implementación: Gracias a su simplicidad, este modelo se convierte en una opción muy atractiva para las redes pequeñas y medianas.

Aplicaciones:

- Redes para pequeñas y medianas empresas

- Redes de campus educativos

- Redes de centros de datos con una topología simple

* SDN Distribuida:

Está formado por múltiples controladores distribuidos, encargados de gestionar las diferentes partes de una red, de esta forma se divide las responsabilidades y conseguimos que aumente la flexibilidad. Cada controlador tiene la función de encargarse de un segmento en específico de la red, ayudándose entre sí para poder conseguir una gestión total.

Características:

- Mayor complejidad: Debido a la gestión y coordinación de diversos controladores.

- Mejor resiliencia: Si un controlador nos da errores, el resto podría seguir controlando sus segmentos de la red.

- Escalabilidad superior: Se adapta mejor al crecimiento de la red, distribuyendo la carga entre diferentes controladores.

- Flexibilidad mayor: Consiguiendo así una gestión más granulada de la red, ya que permite que se adapte mejor a las topologías complejas.

Ventajas:

- Mayor disponibilidad: La distribución de la gestión, consigue reducir el impacto de fallos en un solo controlador de la red.

- Escalabilidad sin límites: Ya que permite facilitar bastante el crecimiento de la red sin verse afectado su rendimiento.

- Adaptación a redes complejas: Hace una gestión granular en entornos que tienen topologías complejas.

Aplicaciones:

- Redes de proveedores de servicios (ISP)

- Redes de grandes empresas con topologías complejas

- Redes de centros de datos a gran escala

SDN Híbrida:

Este modelo consigue combinar algunos elementos de la SDN centralizada y distribuida, ya que intenta buscar un equilibrio entre la centralización de la red y la flexibilidad. Además, un controlador centralizado gestiona toda la red, mientras que los controladores distribuidos son los encargados de los segmentos específicos.

Características:

- Aprovecha las ventajas de ambos modelos: Consigue combinar la visión global de la SDN centralizada con la flexibilidad que aporta la SDN distribuida.

- Se adapta a necesidades específicas: Puede adaptarse a necesidades particulares que una empresa desee.

- Escalabilidad y resiliencia: Permite el crecimiento de la red sin verse involucrada la disponibilidad de la red.

Ventajas:

- Mejor optimización: Ya que consigue mejorar la gestión del tráfico, aplicando diferentes políticas avanzadas para las partes donde haga falta.

- Reducción de costos y riesgos: Al minimizar las posibles interrupciones de la red, ya que mantiene ciertos segmentos funcionando con su arquitectura tradicional.

Aplicaciones:

- Redes grandes con topologías complejas y una serie de necesidades específicas

- Redes de necesiten una gestión granular en unos segmentos en concreto

- Redes de empresas que busquen lograr un equilibrio entre la centralización y la flexibilidad

Características de las SDN:

Existen una serie de características que consigue diferenciar a las SDN de las arquitecturas de redes tradicionales:

* Virtualización: También permite virtualizar los recursos de la red, lo que permite para los administradores poder crear redes virtualizadas bajo demanda. Pudiendo llegar a resultar muy útil en aquellos entornos de computación en la nube, en los que la demanda de recursos de red podría ser muy dinámica.
* Abstracción: Para las arquitecturas SDN, el plano de control estaría separado del plano de datos, que es el encargado de reenviar el tráfico. Pudiendo ayudar esto para cambiar fácilmente el funcionamiento de la red sin poder afectar a los dispositivos encargados del reenvío del tráfico.
* Programabilidad: Esto permite llegar a controlar mediante programación el comportamiento de la red usando una API u otras herramientas para el desarrollo del software. Llegando a facilitar la automatización de las tareas de la red y su posible integración con otros sistemas.
* Flexibilidad: Los cambios que puede sufrir la red, pueden realizarse sin tener que reconfigurar físicamente los dispositivos de la red, pudiendo permitir a los gestores de red reaccionar con rapidez ante la evolución de las necesidades y sus circunstancias.

# Impacto de SDN en centros de datos y la nube

Actualmente las redes definidas por software. También conocidas como SDN, están siendo bastante revolucionarias en cuanto a la forma en que se llegan a gestionar y operar los centros de datos. Esta innovadora tecnología nos permite poder separar el plano de control, del plano de datos, lo que permite ofrecer mayor flexibilidad y capacidad para poder gestionar todo el tráfico que se encuentra dentro de la red de interconexión con los centros de datos. En cuanto a la interconexión con los centros de datos, SDN permite una gestión mucha más efectiva del tráfico, consiguiéndolo gracias a optimizar el uso de ancho de banda disponible para después ser ofrecido a las aplicaciones que se consideran más sensibles para los usuarios finales. Las organizaciones que utilizan múltiples centros de datos se benefician del uso de las SDN ya que les permite poder aplicar políticas para la gestión de conexiones entre diferentes centros de datos, logrando de este modo, grandes eficiencias relacionadas con los costos y también consiguiendo poder asignar recursos de manera limitada para el ancho de banda, en las zonas que se consideren más importantes. El uso de SDN para la interconexión de centros de datos, proporciona una mayor escalabilidad, permitiendo llegar a ajustar rápidamente la arquitectura y la capacidad de la red según las necesidades de las aplicaciones y diferentes servicios. Además, gracias al uso de SDN se nos facilita la implementación de políticas de seguridad y calidad de servicio, lo que significa una mejora en la protección de los datos. Con la adopción de las nuevas tecnologías emergentes para la interconexión de centros de datos, se están consiguiendo una serie de beneficios bastantes significativos para las empresas y organizaciones. De la misma manera se está notando un crecimiento de la computación en la nube, haciendo que las empresas opten por implementar una solución de multicloud, utilizando múltiples proveedores de servicios en la nube pública. Esta nueva tendencia supone plantear nuevos desafíos en términos de interconexión con los centros de datos, ya que es necesario establecer conexiones eficientes además de seguras con los proveedores de servicios en la nube. La conectividad multicloud hace referencia a la capacidad de poder interconectar centros de datos con los diferentes proveedores de servicios en la nube. Llegando a permitir a las empresas mover los datos y cargas de trabajo entre diferentes nubes de manera transparente y eficiente. Además, debemos de saber que la conectividad multicloud ayuda a mejorar la redundancia y la resiliencia, ya que los datos y las aplicaciones pueden estar respaldados en diferentes ubicaciones geográficas. Por último, la interconexión de centros de datos dentro del contexto del IoT[[1]](#footnote-1) facilita el procesamiento y análisis de grandes volúmenes de datos generados por dispositivos IoT, lo que nos permite poder incorporar aplicaciones y servicios de inteligencia artificial.

Gráfico, Gráfico de líneas

El contenido generado por IA puede ser incorrecto.

Gráfico

El contenido generado por IA puede ser incorrecto.

Ilustración 6 Costes SDN

Ilustración 5 Evolución SDN

## Beneficios de SDN en centros de datos

|  |  |
| --- | --- |
| Beneficio | Descripción |
| Reducción de costes | Permite poder disminuir los gastos destinados el hardware y su mantenimiento |
| Automatización | Hace posible la configuración de la red sin necesidad de intervención manual |
| Flexibilidad | Facilidad a la hora de la creación de redes virtuales dinámicas |
| Mayor seguridad | Implementación de forma dinámica las reglas de seguridad de la red |
| Optimización del tráfico | Consigue mejoras de la eficiencia del uso del ancho de banda en la red |

# Impacto de SDN en la latencia y el rendimiento

|  |  |  |
| --- | --- | --- |
| Métrica | Antes de SDN | Después de SDN |
| Latencia media (ms) | 16 | 4 |
| Tiempo de recuperación ante fallos (s) | 28 | 5 |
| Ancho de banda utilizado (%) | 65 | 90 |
| Tiempo de respuesta de las aplicaciones (ms) | 200 | 100 |

# 

# Beneficios de SDN en la nube

|  |  |
| --- | --- |
| Beneficio | Descripción |
| Optimización | Consigue priorizar el flujo de datos y también mejoras en las entregas de servicios basados en la nube |
| Conectividad MultiNube | Prioriza la integración y comunicación entre diferentes nubes (privada, pública e híbrida) |
| Agilidad de implantación | Permite poder aprovisionar las redes virtuales en cuestión de segundos en los entornos de nubes híbridas |
| Reducción de costes | Disminuye el consumo de recursos físicos y gastos en hardware |
| Seguridad avanzada | Implementación de políticas de seguridad centralizadas |
| Automatización | Facilita las tareas de gestión y configuración de redes en la nube |
| Optimización de los recursos | Se consiguen mejoras al utilizar el ancho de banda y una reducción en el colapso de la red |
| Escalabilidad | Posibilidad de crecer y adaptarse de manera dinámica a la gran demanda de tráfico en la nube |

# Automatización de la red mediante SDN

## ¿Qué es la automatización de red?

La automatización de red es ese proceso que se encarga de poder automatizar toda la configuración de red, su administración, sus pruebas necesarias, la implementación y la operación de dispositivos físicos y virtuales dentro de una red. La automatización de la red nos permite que los equipos de operaciones de red como NetOps [[2]](#footnote-2) configuren, ajusten, protejan e integren todo la infraestructura de red y los servicios de aplicaciones que sean más rápidos que cuando los usuarios lo hacen de manera manual.

## ¿Cuál es la importancia de la automatización de red?

Consideramos la automatización de la red como un proceso con mucha importancia ya que ayuda a mejorar la eficiencia, la seguridad, la escalabilidad y la innovación dentro de la red. Algunos de los beneficios más importantes son:

### Eficiencia: Consiguiendo poder reducir los tiempos y los esfuerzos necesarios para realizar tareas repetitivas y complejas, como serían el despliegue, la monitorización y el mantenimiento de la red. También minimiza los errores humanos y las inconsistencias que puedan llegar a causar problemas de rendimiento o disponibilidad de la red.

* Seguridad: Permite mejorar la seguridad de la red al tener que aplicar políticas y controles consistentes para toda la infraestructura. La infraestructura de red también facilita la detección y respuesta a las posibles amenazas, al permitir una visibilidad y una auditoría completas de las actividades y todos los cambios en la red.
* Escalabilidad: Puede escalar la red según las demandas del negocio, al proporcionar una mayor flexibilidad y agilidad para poder adoptarse a los cambios. Permitiendo de esta forma adaptarse también a las nuevas tecnologías.
* Innovación: Se fomenta la innovación al poder liberar recursos humanos y financieros que se puedan dedicar a actividades más estratégicas y creativas. Haciendo posible que los equipos de NetOps puedan colaborar mejor con los equipos.

## Como afectan las SDN a la automatización de la red

Las SDN influyen de manera significativa a la hora de tener que automatizar la red de las siguientes maneras:

* Flexibilidad y escalabilidad: Las SDN permiten que las empresas puedan adaptarse rápidamente a los cambios sin necesidad de tener que modificar nada del hardware. Esto se consigue mediante:
* Separación del plano de control y el plano de datos: Al tener centralizado el control en un software, los dispositivos de red se convierten en una serie de elementos que se limitan a solo ejecutar las instrucciones que manda el controlador.
* Configuración dinámica: Las políticas de red se encuentran definidas en el controlador y después se aplican de forma automática a el resto de los dispositivos.
* Escalabilidad horizontal: Permitiendo que se puedan agregar nuevos dispositivos o servicios a la red, debido a que el controlador de SDN los integra de forma automática según las políticas que hayamos definido.
* Agilidad operativa: Facilita la gestión dinámica para los sistemas, consiguiendo mejoras en la eficiencia de operación de las redes. Permitiendo:
* Gestión centralizada: Con el controlador SDN conseguimos proporcionar una visión global de toda la red, permitiendo que los administradores de red puedan tomar decisiones rápidas.
* Automatización de tareas: Algunas tareas como la configuración de equipos, la implementación de políticas de seguridad o la recuperación ante posibles fallos se podrán automatizar consiguiendo así reducir errores y ahorrarnos tiempo.
* Control centralizado: Permite que los administradores de red puedan definir y controlar el comportamiento de los dispositivos de red mediante software, en vez de tener que configurar los equipos individualmente. Esto se consigue a través de:
* Controlador SDN: Se considera el cerebro de la red, ya que todo parte a través de aquí donde se toman las decisiones globales y después de implementan las políticas.
* Visibilidad global: El controlador de la red tiene una visión completa de la red, lo que nos permite poder facilitar las tareas de monitorización y resolución de posibles problemas.
* Implementación de políticas: Todas las políticas de red se consiguen aplicar de manera razonada en toda la infraestructura de la red.
* Programación y automatización: El uso de SDN nos permite poder programar las redes, gracias a esto podemos eliminar la necesidad de configuraciones manuales. Se podría lograr con:
* Scripts y APIs: SDN consigue poder utilizar interfaces de programación o scripts para automatizar las tareas de red.
* Configuración dinámica: Todas las configuraciones de la red, al estar definidas en el controlador, se aplican de manera automáticamente a los dispositivos de la red.
* Respuestas dinámicas: SDN ofrece soluciones que responden de manera inmediata a las posibles necesidades de la red, lo que es un aspecto crucial para la automatización. Incluyendo:
* Recuperación frente a fallos: En caso de posibles fallos en algún enlace o dispositivo, SDN consigue poder redirigir automáticamente el tráfico para una ruta alternativa, reduciendo los tiempos de inactividad.
* Optimización del tráfico: SDN se encarga de tener que ajustar dinámicamente las rutas y prioridades que tenga el tráfico, para intentar evitar en lo posibles las congestiones y permitir mejoras en el rendimiento de la red.
* Adaptación a posibles cambios: Gracias a SDN conseguimos que la red pueda adaptarse de manera rápida a todos los cambios en la posible demanda o los requisitos que necesiten las aplicaciones

## Herramientas para la automatización de red usando SDN

Existen diversas aplicaciones encargadas de la automatización de red, siendo algunas de las más destacadas son Ansible, Puppet y Chef donde centran su mayor beneficio para la resolución de diferentes problemas que se presentan cuando existen múltiples cambios en la red, sobre una o varias entidades, donde existen problemas como ausencia de registros y sistemas de control o discrepancia de archivos.

### Ansible

Esta aplicación permite el” configuration provisioning”, que hace referencia a la manera de desplegar cambios o poder aprovisionar la configuración, de forma simultánea en diversos equipos cuando se hayan realizado ya los cambios necesarios en el archivo de configuración del sistema. Algunas de las características más importantes son:

* Ofrece soporte para Linux y Mac
* Es Open-source y también tiene versión de pago
* Arquitectura sin agentes, confiando en SSH o NETCONF para hacer cambios en los equipos
* Logotipo, nombre de la empresa

  El contenido generado por IA puede ser incorrecto.Usa un modelo Push, donde Ansible envía la configuración a los cambios a los equipos.

Ilustración 7 Ansible

### Puppet

Es una herramienta encargada de la automatización de configuraciones y gestión de infraestructuras, que nos permite poder administrar servidores y redes de forma centralizada. Se usa para instalar software, gestión de archivos o configuraciones de forma eficiente y automática. Destacan características como:

* Se puede instalar en Linux
* Ofrece una versión Open-source
* Posee una arquitectura basada en agentes, aunque también tiene una versión sin agentes conocida como Puppet Proxy
* Usa un lenguaje declarativo e imperativo, es decir se declara paso a paso las acciones

Un dibujo con letras

El contenido generado por IA puede ser incorrecto.

Ilustración 8 Puppet

### Chef

También es una herramienta de gestión de configuraciones, donde se usa para poder definir y administrar servidores y redes de una forma eficiente. Actualmente está siendo muy usada gracias al aumento de las redes SDN, la gestión centralizada y el despliegue en entornos en la nube. Algunas características importantes son:

* Tiene una arquitectura cliente/servidor
* Hay una versión Chef Zero, la cuál es útil para testing inicial
* Es una arquitectura basada en agentes como Puppet
* Posee un sistema de automatización total

Logotipo, nombre de la empresa

El contenido generado por IA puede ser incorrecto.

Ilustración 9 Chef

# Virtualización de las funciones de red y su relación con SDN

## ¿Qué es la virtualización de funciones de red?

La virtualización de funciones de red, también conocida como NVF (Network Functions Virtualization), es un proceso de arquitectura de red que consiste en trasladar funciones de red como el equilibrio de la carga y el cifrado del hardware físico a las máquinas virtuales. NFV ayuda a las organizaciones a poder reducir costes y optimizar la implementación de los servicios. La arquitectura NFV utiliza la virtualización y las máquinas virtuales para crear una red ágil que sea escalable, personalizable además de gestionable a través de un único panel. El uso de un panel de control centralizado permite a los operadores de red automatizar el aprovisionamiento y la orquestación de recursos de red y una rápida respuesta a las demandas de la red. NFV responde frente al crecimiento número de empresas que buscan poder mantener el control de su infraestructura de red mientras migran de hardware físico a recursos virtualizados y de cloud computing.

## Arquitectura NFV

La arquitectura NFV establece una base, un proceso y una estrategia para llevar a cabo la virtualización de las funciones de red. Su arquitectura consta de 3 capas:

### Funciones de red virtualizadas (VNF): Las VNF son los servicios que se estaban ejecutando en el hardware físico. El enrutamiento, los firewalls, la configuración IP o los programas de intercambio de archivos son tipos comunes de funciones de red virtualizadas. Cuando se virtualizan, estos servicios pueden vincularse en un proceso llamado “encadenamiento de servicios”. El encadenamiento de servicios ayuda a los operadores de red a poder automatizar el aprovisionamiento de recursos para cada servicio de red. Si disponemos de una visión centralizada de todas las funciones proporciona a los operadores un mayor control de la red y permite poder dirigir el tráfico y las cargas de trabajo a los servidores disponibles, lo que reduce el riesgo de interrupciones del servicio.

* Infraestructura de virtualización de funciones de red (NFVI): La infraestructura NFV está formada por los servidores, el almacenamiento, los conmutadores y los recursos informáticos necesarios para crear los entornos NFV. Para poder abstraer las funciones de red del hardware físico, los operadores de red crean una capa de virtualización mediante el uso de un software llamado hipervisor. Un hipervisor o monitor de máquina virtual (VMM), crea una capa de software capaz de segmentar múltiples máquinas virtuales a partir de una única máquina física. Estas máquinas virtuales pueden funcionar juntas en su propio sistema operativo. NFVI ofrece conectividad para crear una red unificada a partir de múltiples máquinas físicas y virtuales.
* Gestión, automatización y orquestación de redes (MANO): NFV MANO es el marco básico para gestionar la implementación, el aprovisionamiento, la monitorización y el rendimiento de las funciones de red virtualizadas. Además de también crear una interfaz para que NFVI se comunique e interactúe con los sistemas de soporte operativo (OSS) y los sistemas de soporte empresarial (BSS) existentes. MANO se divide en tres subsecciones:
* Orquestación de NFV: Utiliza tecnologías de virtualización para implementar nuevas funciones de red y poder suministrar recursos a las VNF existentes. La orquestación de NFV también sirve para autenticar las solicitudes de recursos NFVI.
* Gestor de infraestructuras virtualizadas (VIM): Consigue optimizar el ciclo de vida de software, los recursos virtuales y la red física. Las instancias VIM pueden gestionar múltiples recursos NFVI o especializarse en un aspecto concreto según sea necesario. Un VIM mantiene un registro de recursos virtuales y físicos que permite a los operadores de red mantener las operaciones e implementar nuevos servicios
* Gestor de funciones de red virtualizada: Permite poder estandarizar las funciones de red virtual y aumenta la interoperabilidad de las funciones de SDN. La gestión de VNF influye la instanciación o creación de instancias, el escalado, la actualización y la terminación de funciones de red virtualizadas.

Diagrama

El contenido generado por IA puede ser incorrecto.

Ilustración 10 Infraestructura NFV

## Beneficios de NFV

Para aprovechar los beneficios de la virtualización de funciones de red, los equipos de TI[[3]](#footnote-3) deben reconocer y abordar algunos retos, en particular los problemas de visibilidad y seguridad que pueden acompañar a la NFV. Los entornos NFV suelen tener que requerir herramientas de monitorización más complejas para controlar las distintas máquinas virtuales, las funciones y el tráfico que circula por la red. Las funciones virtualizadas también están más expuestas a los ciberataques y al malware que el hardware físico almacenado en un centro de datos, y deben protegerse de formas diferentes. Las empresas que deseen implementar NFV deben acompañar esta transición con prácticas de supervisión y seguridad sólidas y específicas de la NFV para poder proteger sus datos e infraestructuras. Algunos beneficios son:

* Reducción de costes: NFV ayuda a poder reducir los costes de varias maneras. Por un lado, reduce la cantidad de hardware que debe adquirir una organización y el espacio de almacenamiento necesario para albergarlo. Además de ampliar el ciclo de vida del hardware de red, ofreciendo a las organizaciones un mayor rendimiento de las inversiones en infraestructuras. La NFV también consigue reducir el consumo de energía de los centros de datos.
* Escalabilidad mejorada: Las soluciones NFV permiten que las organizaciones puedan impulsar el crecimiento empresarial y a planificar el futuro gracias a la escalabilidad que proporciona la virtualización. El escalado con hardware físico requiere el transporte y la configuración de máquinas y técnicos para hacerlo, mientras que la virtualización permite el aprovisionamiento rápido y remoto de la infraestructura. NFV también puede simplificar la implementación de actualizaciones de red.
* Implementación más rápida: La virtualización de funciones de red sirve de ayuda a las organizaciones a poder acelerar el lanzamiento de nuevos servicios, aplicaciones y actualizaciones a través de una red virtualizada. Las redes virtuales permiten a los operadores de red automatizar la implementación de características y aplicaciones a través de un proceso denominado implementación continua. Una vez que los cambios en el código superan una serie de pruebas predefinidas, las actualizaciones pasan a estar disponibles para los usuarios.

# Retos de la virtualización de las funciones de red

La NFV ofrece muchas ventajas, aunque también conlleva algunos retos, como podrían ser:

* Aunque los despliegues de virtualización de funciones de red a gran escala suelen ser económicos, el mayor reto viene con la fiabilidad.
* Cuando se necesita un reajuste de procesos que actualice las redes anteriores utilizando NFV, gestionar simultáneamente la infraestructura virtual y la tradicional puede resultar difícil.
* El fallo de un componente individual durante el despliegue de la NFV puede llegar a producir fallos tanto en el hardware como en el software, lo que afecta a la capacidad de recuperación.
* En el modelo NFV, es difícil poder contener y aislar el malware. Es fácil que el malware se desplace entre los componentes y los dañe.

# SDN frente a NFV

Las redes definidas por software y la virtualización de red comparten elementos comunes, pero sirven a funciones y casos de uso distintos. Ambas funciones son enfoques definidos por software que se centran en la creación de una capa virtualizada por encima de una red física que se puede utilizar para flexibilizar las redes. Sin embargo, las SDN se centran en los centros de datos, mientras que la NFV está más orientada a las redes de área extensa, conocidas como redes WAN y a los proveedores y operadores de servicios de red. Mientras que la NFV virtualiza las funciones de red y se utiliza para poder reducir la necesidad de dispositivos físicos, la SDN ayuda a las organizaciones a centralizar la gestión de la red y a mejorar el enrutamiento del tráfico de la red. Las SDN lo llegan a conseguir desacoplando el plano de control del plano de datos subyacente, que es el motor que mueve los paquetes de datos. Esta centralización permite una gestión más precisa de los recursos de la red basada en políticas específicas de la organización y un uso más eficiente del aprovisionamiento automatizado. Los operadores de red pueden llegar a poder implementar herramientas de automatización, equilibrar dinámicamente la carga y suministrar una serie de recursos en función de las condiciones en tiempo real, lo que reduce la latencia y aumenta la prestación de servicios. Las funciones de red virtuales pueden implementarse en un ecosistema SDN. Donde utilizadas conjuntamente, SDN y NFV ayudan a crear redes ágiles y flexibles, que puedan ser capaces de gestionar entornos virtuales complejos.

## Comparación técnica entre SDN y NFV

|  |  |  |
| --- | --- | --- |
| Característica | SDN | NFV |
| Enfoque | Permite separar el plano de control del plano de datos para una gestión centralizada | Virtualiza las funciones de red a través de software, permitiéndose poder eliminar el hardware |
| Arquitectura | Controlador centralizado con switches programables | VNF (Virtual Networks Functions) aplicado a servidores |
| Objetivo | Conseguir una mejora del control y la gestión que se hace de la red | Llegar a poder tener una implementación y escalabilidad de las funciones de red de manera optima |
| Flexibilidad | Alta, ya que nos permite poder programar la red de forma dinámica | También elevada, porque soporta despliegues rápidos y dinámicos en las funciones de red |
| Usos | Para balanceos de carga, gestión de tráfico... | Firewall virtual, optimización de redes WAN... |

# Importancia de la seguridad en redes definidas por software

La gran transición a las redes SDN consiguió poder traer grandes beneficios, pero también introdujo nuevos desafíos relacionados con la seguridad. La naturaleza centralizada del control en SDN puede ser un objetivo bastante atractivo para los atacantes, quienes podrían llegar a aprovecharse de las vulnerabilidades para comprometer toda la red y exponerla a ciertos peligros y vulnerabilidades. Por ello, la seguridad en redes SDN debe ser una prioridad desde el diseño hasta su implementación. Además, debemos saber que uno de los mayores beneficios de SDN es su capacidad para poder implementar políticas de seguridad de una manera rápida y eficiente. Al tener todo el control centralizado, las políticas pueden ser aplicadas de manera uniforme en toda la red, reduciendo así la posibilidad de configuraciones erróneas que podrían ser explotadas por los atacantes. También SDN nos permite obtener una mejor visibilidad del tráfico de red, facilitando la detección anticipada de las actividades sospechosas.

## ¿Cómo podemos mejorar la seguridad de las SDN?

Hay diferentes métodos con lo que podemos lograr una seguridad más eficiente, entre los más usados estarían:

* Monitoreo y análisis del tráfico: Hacer uso de un monitoreo continuo del tráfico de la red es crucial para poder identificar y reducir las amenazas de seguridad. Las herramientas de análisis de tráfico pueden ser utilizadas para detectar patrones inusuales que podrían indicar una violación de seguridad. Además, hay que tener en cuenta que la implementación de sistemas de detección de intrusiones (IDS) pueden ayudarnos a identificar y responder de una manera rápida a las actividades detectadas como maliciosas.
* Uso de cifrado: El cifrado es una herramienta muy esencial a la hora de tener que proteger la comunicación entre los diferentes componentes de SDN. Existen protocolos como SSL/TLS que deben ser utilizados para cifrar todo el tráfico entre el controlador y los dispositivos de red, pudiendo así asegurar que los datos no sean interceptados o modificados por los atacantes cuando se encuentran en transmisión.
* Implementación de autenticación y autorización: La seguridad en redes SDN empieza desde tener una autenticación sólida y una autorización. Actualmente las empresas deben utilizar protocolos de autenticación que sean robustos como lo son RADIUS o TACACS, con los que conseguimos poder garantizar que solo los usuarios autorizados puedan acceder al controlador SDN. Además de que es crucial tener que implementar también políticas de autorización que sean estrictas para limitar los privilegios de los usuarios según sus roles.
* Segmentación de redes: Esta es una práctica efectiva para poder limitar el impacto de un ataque. Al tener que dividir la red en diferentes segmentos más pequeños, se puede contener el acceso no autorizado y minimizar la posible propagación de amenazas. En los entornos SDN, la segmentación de redes puede conseguirse de forma dinámica, pudiendo así adaptarse rápidamente a las amenazas que surjan.

## Retos comunes de la seguridad en la SDN

* Integración con infraestructuras legadas: La integración de SDN con infraestructuras de red legadas puede llegar a presentar desafíos de compatibilidad y seguridad. Ya que es esencial planificar cuidadosamente la transición a SDN para garantizar una integración fluida y segura que no comprometa a la infraestructura existente.
* Complejidad para la gestión de políticas: A medida que las redes se van volviendo más complejas, la gestión de políticas de seguridad puede convertirse en un desafío. Las organizaciones deben poder asegurarse de que sus políticas de seguridad sean claras, consistentes y fáciles a la hora de gestionarlas para evitar configuraciones erróneas que podrían ser explotadas.

## Herramientas para aumentar la seguridad en SDN

* Soluciones de seguridad de confianza cero: Las arquitecturas de confianza cero están ganando una gran popularidad al ser utilizadas como un enfoque efectivo para poder mejorar la seguridad de las SDN. Este modelo consta del principio de no confiar en nada dentro o fuera de la red por defecto y verifica continuamente cada solicitud de acceso. Si llegamos a implementar una arquitectura de confianza cero se puede conseguir ayudar a reducir significativamente el riesgo de los accesos no autorizados y violaciones de seguridad.
* Firewalls definidos por software: Son una herramienta muy poderosa para la seguridad de las redes SDN. Este tipo de firewalls nos permiten tener un control granular del tráfico de la red, asegurando que solo el tráfico autorizado pueda atravesar la red. Además, su implementación puede ser automatizada para poder adaptarse rápidamente a las amenazas.
* Uso de inteligencia artificial: Juega un papel crucial en la mejora de la seguridad de este tipo de redes. Esta tecnología puede usarse para analizar grandes volúmenes de datos, identificar patrones sospechosos y poder predecir amenazas potenciales antes de que lleguen a ocurrir. Al tener que integrarlas en el sistema de seguridad de las SDN, las empresas pueden mejorar significativamente su capacidad de respuesta ante amenazas.

# Ciberseguridad en SDN

La ciberseguridad dentro de las SDN consta de 5 pilares básicos, que son: confidencialidad, disponibilidad de la información, autenticación, no repudio e integridad. Los profesionales que trabajan con este tipo de redes deben ser capaces de proteger los datos y los terminales, además de poder realizar comunicaciones a través de una red protegida. La ciberseguridad en las redes SDN tiene un potencial tremendo a nivel de uso de la red. Por este motivo, se comienzan a crear procesos inteligentes de detección de intrusos, sistemas de prevención para las intrusiones y un análisis programado de la propia red. Los sistemas podrán alcanzar un nivel muy alto de robustez frente a los ataques de los ciberdelincuentes en muy poco tiempo y ahí estaremos nosotros para poder ofrecer el mejor servicio.

Implementación de medidas de seguridad en SDN

|  |  |  |
| --- | --- | --- |
| Medida de seguridad | Reducción del riesgo | Mejora del tiempo de respuesta |
| Uso de cifrado | 90% | 70% |
| Segmentación de la red | 70% | 65% |
| Monitoreo del tráfico | 80% | 55% |
| Autenticación y autorización | 75% | 63% |
| Firewalls definidos por software | 86% | 74% |

Resultados de seguridad en SDN

|  |  |  |
| --- | --- | --- |
| Objetivo | Antes de implementar seguridad en SDN | Después de implementar seguridad en SDN |
| Reducción del tráfico malicioso | 35% | 85% |
| Efectividad de los  firewall | 55% | 94% |
| Tiempo de detección de ataques | De 2 a 3 horas | Menos de 5 minutos |
| Costos de mitigación de ataques | Alto | Bajo |

# Vulnerabilidades dentro de las SDN

Las redes SDN han conseguido revolucionar las infraestructuras de red, al conseguir poder reparar el plano de control del plano de datos, permitiendo gracias a esto poder tener una gestión centralizada. Sin embargo, debemos saber que este nuevo tipo de redes permite nuevas vulnerabilidades que debemos saber resolverlas para conseguir una red segura. Las vulnerabilidades dentro de las SDN se encuentran en varios niveles de sus infraestructuras. Donde podrían ser problemas de accesos no autorizados a controladores, fallos en las APIs... Es muy importante entender estos tipos de vulnerabilidades y cómo pueden afectar a nuestro sistema.

Tipos de vulnerabilidades

Las principales vulnerabilidades actuales para las SDN incluyen:

* Explotación de APIs: Es importante saber, que las interfaces de programación que usamos podrían llegar a ser vulnerables a ataques externos sino están bien protegidas.
* Accesos no autorizados: Una de las más importantes, ya que, si los atacantes consiguen cualquier tipo de acceso a nuestro sistema, podrían empezar a cambiar políticas de red incluso poder acceder a datos importantes.
* Fallos en la configuración: Esto puede ocurrir, ya que, si realizamos sin darnos cuenta una mala configuración, podemos dejar a la red expuesta a posibles ataques que comprometan su seguridad e integridad.

Amenazas para las SDN

* Ataque de denegación de servicios (DoS): La seguridad de las redes SDN se enfrenta a un gran desafío, que es la vulnerabilidad que recibe el controlador frente a los ataques DoS. Donde el controlador, al tener que centralizar todo el control de la red, se vuelve el objetivo para los ataques. Los atacantes lo que intentarán lograr es intentar saturar el controlador con tráfico maliciosa, hasta dejarlo por completo fuera de servicio.
* Interceptación de comunicaciones (Man in the Middle): Lo primero que debemos saber esque la comunicación entre los dispositivos de la red y el controlador es muy importante. Por lo tanto, sino protegemos a el controlador lo suficiente, un atacante podría lograr interceptar los mensajes, para después modificarlos, alterando así el comportamiento de nuestra red sin ser detectado.
* Accesos no autorizados: Gracias a la centralización y automatización en las redes SDN, esto permite poder facilitar el acceso no autorizado a recursos críticos del sistema. Donde los atacantes podrán usar vulnerabilidades en la infraestructura SDN para poder obtener privilegios elevados, para facilitar el avance de sus ataques. Comprometiendo de esta forma la seguridad de toda la red. Para hacer frente a estas amenazas es esencial una estrategia de seguridad que sea sólida.
* Ataques al controlador: El controlador SDN, es considerado como el cerebro de toda la red, ya que es el encargado de tener que gestionar y configurar los equipos de la red. Debido a esta centralización, se convierte en un objetivo atractivo para los atacantes. Si se realiza un ataque exitoso al controlador, se puede llegar a ver toda la red comprometida, permitiendo así la manipulación del tráfico, interrupción de servicios y la exposición de datos considerados sensibles.
* Manipulación del tráfico y suplantación: Las SDN también se encuentran presentes dentro de los riesgos de manipulación del tráfico de la red. Pudiendo conseguirse gracias a la suplantación de identidades o modificaciones de flujos de datos. Esto permite que los atacantes puedan lograr interceptar y alterar el tráfico, redirigiéndolo a destinos no autorizados, comprometiendo de esta forma la integridad de los datos.

TRABAJOS FUTUROS

Trabajos de ampliación y mejora proyectados.

CONCLUSIONES

Conclusión profesional del proyecto.

REFERENCIAS

Según las normas APA.  
Cada referencia se acompañará de un texto descriptivo con el apartado del proyecto asociado.  
  
**Formato:**

Autor, A. A. (Año de publicación). Título de la página. Recuperado de URL

**Ejemplo:**  
*Aplicado en la investigación del tema de la web.*

Smith, J. (2023). La importancia del reciclaje en la conservación del medio ambiente. Recuperado de <https://www.ejemplodepagina.com/>

**Otro ejemplo:**

*Aplicado para realizar las vistas de la base de datos.*  
Oracle Corporation. (s. f.). Oracle Database 19c Documentation. Recuperado de https://docs.oracle.com/en/database/oracle/oracle-database/index.html

1. El Internet de las cosas (IoT) es un concepto que se refiere a la interconexión de dispositivos físicos a través de Internet para que puedan capturar, enviar y recibir datos sin necesidad de intervención humana. [↑](#footnote-ref-1)
2. Es un enfoque moderno para la gestión y operación de redes, que combina automatización, virtualización y análisis avanzado para mejorar la eficiencia y fiabilidad de la infraestructura de red. [↑](#footnote-ref-2)
3. Las tecnologías de la información es el conjunto de herramientas, procesos y sistemas utilizados para gestionar, procesar, almacenar y transmitir información en entornos digitales. [↑](#footnote-ref-3)