ISSN: 1692-7257 - Volumen 1 – Número 37 - 2021

Revista Colombiana de
Tecnologías de Avanzada

Recibido: 10 agosto 2020
Aceptado: 11 septiembre 2020

SEGURIDAD EN REDES SDN Y SUS APLICACIONES

SECURITY IN SDN NETWORKS AND THEIR APPLICATIONS

Ing. Robin Tapiero[*], Ing. Alejandro Gonzalez[**], Ing. Norberto Novoa [***]

[*] **Universidad Distrital Francisco José de Caldas,** Ingeniería, Ingeniería Telemática.
Cl. 68d Bis A Sur #49F - 70, Bogotá, Colombia.
3 23 93 00 Ext 5003.
E-mail: {retapierot, edgonzalezc}@correoudistrital.edu.co.

Resumen: Las redes SDN (redes definidas por software) son el avance que se estaba esperando desde que las necesidades del mercado empezaron a sobrepasar la capacidad de procesamiento que la infraestructura de las redes tradicionales ha estado ofreciendo. Actualmente las conexiones en la nube y el internet de las cosas requieren más conexiones de dispositivos en la red y un mejor control de tráfico, estimulando la mejora continua de la misma, por este caso, se hizo necesario la implementación de una nueva red que sea escalable y que brinde mejores servicios de los que ofrece actualmente las redes tradicionales, garantizando aspectos como integridad, confiabilidad, disponibilidad de la información y análisis de tráfico. El presente artículo, expone una revisión descriptiva de la arquitectura de las redes SDN, su enfoque en la seguridad y las aplicaciones que ejecutan estas redes en la actualidad.

Palabras clave: Software-Defined Networking (SDN), IoT, Network Function Virtualization (NFV), ONF, OpenFlow.

Abstract: SDN (software defined networks) are the advance that has been expected since the needs of the market began to exceed the processing capacity that the infrastructure of traditional networks has been offering. Currently the connections in the cloud and the Internet of Things require more device connections in the network and better traffic control, stimulating continuous improvement of it, in this case, it became necessary to implement a new network that is scalable and offering better services than traditional networks currently offer, guaranteeing aspects such as integrity, reliability, availability of information and traffic analysis. This article presents a descriptive review of the architecture of SDN networks, its focus on security and the applications that these networks are currently running.

Keywords: Software-Defined Networking (SDN), IoT, Network Function Virtualization (NFV), ONF, OpenFlow.

1. INTRODUCCIÓN

Desde que las organizaciones fueron aumentando su demanda en infraestructura, los administradores de redes, tuvieron que enfrentar el reto de mantener con un óptimo funcionamiento toda la red [1], tarea que no es nada fácil por las continuas solicitudes de escalamiento, interoperabilidad, alta disponibilidad, entre otros aspectos, que se han dado gracias a las múltiples solicitudes de los usuarios en las aplicaciones de negocio, saturando el funcionamiento de la red y quedando atrás frente a las necesidades de crecimiento que exigen las organizaciones [2].

Lo que hace necesaria la llegada de las redes SDN como una solución ante esta problemática, gracias a la infraestructura que se ofrece [3], donde se desagrega el plano de datos del plano de control, centralizando toda la administración en un nodo que se encarga de gestionar el flujo de información que circula por la capa de control [4], por medio de tablas de flujo y los lineamientos de seguridad de la red por medio del protocolo OpenFlow que permite gestionar la red como un todo [5], no como un número de dispositivos individuales que gestionar, es el propio servidor el que gestiona a los switches que deben enviar los paquetes. Centralizando las ordenes de envió de paquetes en el plano de control. Se evidencian los problemas de seguridad que aun afrontan las redes SDN y como las aplicaciones que las articulan, han venido lidiando con estos inconvenientes [6], además del desarrollo que han presentado en los últimos años para tecnologías como IoT, Data centers y 5G, que han ido madurando el trabajo de las redes SDN y proyectan la desaparición de las redes tradicionales para dar pasa a la red del futuro [7].

2. METODOLOGIA

Para desarrollar los temas de este artículo de revisión se emplea el método descriptivo [8], que busca a través de la descripción exacta, conocer la arquitectura y procesos que conforman las redes SDN como foco de estudio [9], especificando las propiedades más relevantes a través de un análisis, sin alterar el factor de estudio. Para esto plantearemos unos ítems, los cuales se irán desarrollando a profundidad y relacionando unos a otros. Con base en esta metodología de estudio, se evidencia que en los últimos años se ha incrementado el crecimiento de las redes SDN y su importancia como tema de investigación, por consiguiente, aspectos como la arquitectura y seguridad [10], son temas que han ido evolucionando a través de diversos estudios que permitieron ofrecer un mejor servicio con respecto a las redes tradicionales y sus actuales desventajas [11]. En consecuencia, se desarrollarán subtemas que contendrán lo siguiente: en Arquitectura SDN capa de datos, capa de control y capa de aplicaciones, en seguridad se destacará el trabajo de la capa de control SDN, sus diferentes avances por medio del protocolo OpenFlow y su proyección [12], en aplicaciones articuladas por SDN se mencionarán los diferentes avances, que tecnologías como IoT, data centers y 5G han desarrollado por medio de las redes SDN y su énfasis en la parte de seguridad [13].

La búsqueda del material de estudio se compone por diversas fuentes de investigación como bases de datos de la IEEE, BDIGITAL y Google Scholar. Basando esta búsqueda en palabras clave como redes SDN, arquitectura de redes SDN, seguridad en redes SDN y aplicaciones con redes SDN. Como muestra de estudio y análisis de material de investigación, se limitó geográficamente la búsqueda de material al continente europeo, asiático y americano, adicional a esto se tomó como valides temporal de fuente de información a los artículos y material de estudio con vigencia no menor al año 2013 para garantizar una fuente de información valida y confiable de las redes SDN y su continuo desarrollo desde la última década.

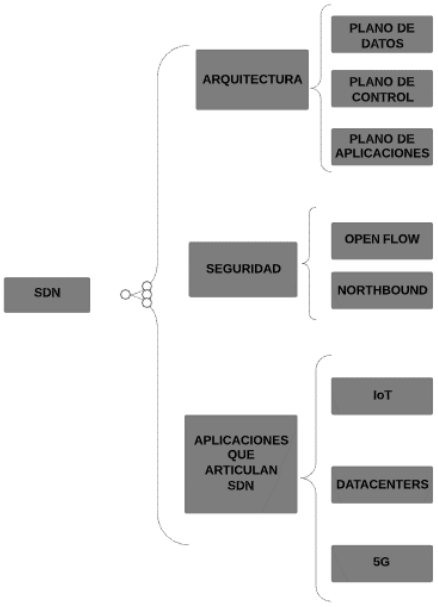

Figura 1: Modelo de investigación para el estado de arte desarrollado. Fuente: elaboración propia.

3. ARQUITECTURA SDN

El Desde el 2013 se introdujo el concepto SDN (Redes definidas por software) y NFV (virtualización de funciones de red) con lo que se buscó simplificar la arquitectura de la red y su operación facilitando el escalamiento, despliegue de modificaciones, inserción de nuevos servicios, acortar tiempos de respuesta y centralizar su administración [14], dando como resultado una red más eficaz y con un mayor retorno económico. Esto como método de respuesta a las continuas dificultades que han tenido las OTT (over the top de libre transmisión), alto tráfico de datos, el internet de las cosas y los servicios en la nube que están acabando a las redes tradicionales por su continuo crecimiento y demanda de infraestructura, reflejando la pobre arquitectura que brindan las redes tradicionales [15].

Las redes definidas por software (SDN) se componen por tres capas: plano de datos, plano de control y plano de aplicación, estas tres capas permiten la automatización de la red y una mejor administración de los recursos que se integren dentro de su arquitectura, centralizando su administración, automatizándola y garantizando su escalabilidad [16], situación que no se presentan en las redes tradicionales que, por su diseño, no es escalable ni rentable. Por medio de esta arquitectura se permite desagregar los planos de control y datos de los dispositivos de red como switches y routers [17]. El plano de control tiene la funcionalidad de tomar decisiones respecto al tráfico que interactúe con cualquier dispositivo de red, el plano de datos realiza el transporte de paquetes de datos en la red [18] y el plano de aplicación se compone por las aplicaciones de negocio del usuario final.

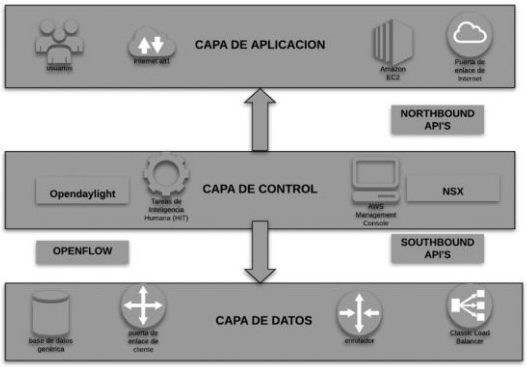

Figura 2: Elementos de la Arquitectura de las redes SDN. Fuente: elaboración propia.

3.1 Capa de Datos

También se le conoce como capa de infraestructura, está conformada por los nodos que se encargan de la conmutación y encaminamiento de paquetes reemplazando a dispositivos de red como switches, routers y access point que eran los encargados de la información que viaja por la red [19]. Esta capa puede ser reprogramable por la capa de control, la cual por medio de un set de instrucciones y reglas puede configurar la funcionalidad de la capa de datos en modo de router o firewall según se requiera a través de la API OpenFlow.

3.2 Capa de control

Esta capa tiene como función centralizar todo el flujo de información que circula por la capa de control, esto gracias a que configura y administra los nodos dirigiendo correctamente el flujo de tráfico, por medio de políticas que establecen las tablas de flujo en la red, reenvió o desvió de datos, teniendo un panorama amplio de toda la red [20]. Estas políticas se establecen por medio del protocolo OpenFlow, que permite a controladores como Opendaylight o NSX enviar las políticas y configuraciones que se designaron para el plano de datos, también están API's como Restful O Northbound que discriminan las políticas de aplicación globales y las políticas internas de la red, esto permite comunicar a la placa de aplicaciones con la capa de control [21].

3.3 Capa de aplicación

Esta capa contiene todas las aplicaciones de negocio del usuario final y se comunica por medio de la API Northbound (hacia arriba) con la capa de control, permitiendo simplificar y automatizar las tareas de configuración, ofreciendo servicios y provisionando al usuario de ingresos diferenciados según el perfil que tenga y el servicio que vaya a consumir, obteniendo estadísticas que plasmarán su comportamiento en la red, para luego tomar decisiones sobre esta información [22]. Garantizando su seguridad y portabilidad ya que es funcional en cualquier sistema operativo.

4. APLICACIONES ARTICULADAS CON SDN

4.1 IoT (Internet de las cosas)

IoT ha tomado un gran auge en su desarrollo gracias a las soluciones prometedoras que ha ofrecido en la diversidad tecnológica integrando redes SDN, capaz de intercomunicarse de una manera eficiente de un nodo a otro a nivel geográfico y centralizando, todo hacia un mismo punto de administración, siendo esto una gran tentación para la industria de la tecnología, que desean implementar esta novedosa solución, sin olvidar los enormes cambios a nivel de infraestructura que la IoT requiere pare ser implementada y las brechas de seguridad que son una amenaza para su ejecución [23].

Debido a esto la tecnología IoT con redes SDN aún sigue siendo un dominio inmaduro que no ha logrado establecerse como una solución tecnológica confiable y esto ha prevenido a los inversionistas de patrocinar este tipo de investigaciones, donde el mayor reto es ofrecer una seguridad confiable de las redes SDN al usuario, diferente al tipo de seguridad que ofrecen hoy en día las redes tradicionales, ya que, al darse un ataque al nodo principal, esto puede comprometer la arquitectura de toda la red SDN [24], viéndose afectada con aspectos como:

Protección de recursos limitados y recursos desatendidos: los nodos de IoT en su gran mayoría están dispersos a nivel geográfico y desatendidos, siendo esto una vulnerabilidad, para ser víctima de un ataque físico del cual no tendría ninguna posibilidad de salvarse [25]. Adicional a esto, el hecho de tener un nodo físico a una larga distancia incurre que la arquitectura física que implemente, sea de gran calidad y capacidad para que pueda ser auto sostenible, un ejemplo claro es la regulación energética de la batería con la que se alimente el nodo y una interfaz que permita el continuo monitoreo del nodo, que garantice su correcto funcionamiento. Lo que deja como evidencia la poca seguridad con la que cuentan este tipo de nodos durante su tiempo de actividad debido a los recursos que son requeridos para sustentar su actividad.

Monitoreo del estado de seguridad: IoT fue diseñado con la noción de ser un gran sistema de interconexión que aloje un enorme sistema distribuido que a su vez contenga subsistemas, donde el que se encarga de la recopilación de datos y agregación de contenido es el nodo administrador que gestiona los recursos de cada nodo de la red [26]. La nube cumpliría un papel de gran importancia en este diseño, ya que, al ser nodos dispersos, la autenticación de los nodos para actualizaciones y validaciones de seguridad se debe hacer por certificaciones que se realizarían por medio de métodos de criptografía y los equipos no cuentan con la arquitectura suficiente para soportar ese alto procesamiento debido a la complejidad significativa que estos métodos requieren.

Disponibilidad de servicios: los proyectos a los que busca dirigirse IoT son a ciudades inteligentes, redes inteligentes, salud, transporte y la industria, en donde la disponibilidad del servicio juega un papel sumamente importante, un simple reinicio no puede ser contemplado como una solución ante alguna eventualidad, por lo tanto, cuando IoT solucione sus problemas de seguridad, será concebida como una gran solución tecnológica que promoverá un alto impacto en la sociedad [27].

4.2 Tecnología móvil 5G

La red definida por software (SDN) es considerada por la tecnología móvil 5G, como el futuro de toda su infraestructura por las prometedoras soluciones que ambiciona ofrecer, no obstante su avance ha sido poco notorio hasta el momento debido a los problemas de seguridad que no ha logrado superar en redes móviles definidas por software (SDMN), si bien los retos en seguridad que afronta son grandes, su potencial en infraestructura es lo suficientemente fuerte como para superar todos estos obstáculos consolidándose como una red poderosa y segura [28]. Se ha trabajado y logrado avances en un controlador de seguridad que se relaciona con el controlador de red SDN [29], ofreciendo servicios de seguridad que garantizarían su correcto funcionamiento para los usuarios finales de las redes móviles [30].

Los avances en el desarrollo de una aplicación demo workflows son de alto impacto para dar solución a los problemas de seguridad que presenta la red SDN en la tecnología 5G [31], ya que se ofrecen cadenas de servicios parametrizadas de acuerdo con la necesidad de la aplicación, teniendo en cuenta aspectos relevantes como carga de red, demanda de usuario y necesidades del operador [32], estos servicios se envían a través de un optimizador de cadena por medio de una GUI [33], al ser exitosa la petición, se envía una respuesta a la GUI con la solución, minimizando tiempos de latencia de extremo a extremo, controlando el tráfico por medio de reglas de flujo [34].

Esta aplicación también garantiza la integridad de los servicios, permitiendo modificar cadenas de servicios sin alterar las demás, gracias al identificador o ID, que permite reconocer la cadena

de servicios que se desea actualizar, al generarse un despliegue de una solicitud de cadena de servicios, un subconjunto de los conmutadores en el dominio WAN SD (red WAN definido por software), desencadena la capacidad de adaptación dinámica, redirigiendo el tráfico a través de otros conmutadores disponibles [35].
SDN busca centralizar la administración de la red a través de un controlador permitiendo generar mejores ventajas de implementación de seguridad a la red móvil, gracias a los atributos que ofrece SDN en seguridad como lo son inteligencia lógicamente centralizada, programabilidad y abstracción [36]. Mejorando la arquitectura que ofrece SDN, se busca implementar una cuarta capa, que sería la encargada de la seguridad de la red, que incorpora un agente en el borde inalámbrico, para prevenir ataques por este medio, además de permitir una mayor escalabilidad en la red, sin embargo, el acoplamiento de una cuarta capa no es tan fácil, ya que una falla en esta capa de seguridad podría paralizar toda la red, dejándola expuesta a los ataques del medio [37].

4.3 Data centers

Los Data centers llegaron a solucionar los problemas de tecnologías como aplicaciones en la nube, migración de máquinas virtuales o copias de seguridad [38], ya que procesan un alto tráfico de datos en nodos distribuidos a nivel geográfico y prestan servicio 24/7 [39]. Por esta razón, aspectos como la arquitectura que implementa, costos, consumo y confiabilidad, entran a tener una gran relevancia en su ejecución [40]. Los DC (Data Centers) requieren de técnicas inteligentes de control de tráfico intra – DC e inter – DC, por lo tanto, el plano de control, que es el encargado de administrar políticas y administrar al plano de datos, debe tener gran cuidado con aspectos como disponibilidad, madurez, preferencia del operador y requisitos funcionales como el tráfico intra – DC que debe ser de control flexible, adaptativo al reenvió de entradas y políticas de contexto dinámico [41].
Se han enfocado estudios en opciones de planos de control que se adaptan a los requerimientos que solicitan los Data centers, como un protocolo extendido Open Flow flexible para el control de la red y de interfaz abierta, un cambio de etiqueta multiprotocolo generalizado (GMPLS) con cálculo de ruta (PCE) opcional [42], ya que ofrece madurez, soporte de grado de operador y multidominio para controlar redes ópticas, migraciones lentas y retorno económico, por medio del plano de control heterogéneo que integra GMPLS, PCE y SDN. Se proporciona coordinación, configuración y gestión automatizada, este plano permite la simplificación de red y una mejor integración con los sistemas operativos [43].

Si bien la administración del plano de control se basa en un nodo central que administra los servicios, recursos y políticas de seguridad [44], los nodos se deben segmentar o dividir en múltiples subdominios para asegurar la escalabilidad de la red [45]. Para esto existen dos modelos de interconexión que son los enlaces fronterizos y los nodos fronterizos, donde los enlaces fronterizos representan el modelo de dos nodos de red, residentes en diferentes dominios que están interconectados por un enlace compartido [46], además ninguna entidad del subdominio, debe tener visibilidad a la topología de la red, por políticas de seguridad y el enlace de nodos fronterizos donde más de un nodo que pertenece a un diferente dominio, están comunicados para fines de interconexión [47].
Un controlador SDN como entidad centralizada y con total visibilidad de los subdominios Open Flow y GMPLS, opera toda la red como un dominio único (como se muestra en la figura 3), en este modelo el controlador SDN centralizado, separa localmente los dominios para permitir el aprovisionamiento por medio de interfaces dedicadas en puntos de demarcación definidos, programando conexiones cruzadas a través de OpenFlow, requiriendo el establecimiento de segmentos a los nodos de limite GMPLS por medio de la interfaz de aprovisionamiento, o encargando la tarea de aprovisionamiento a un ASPCE [48].

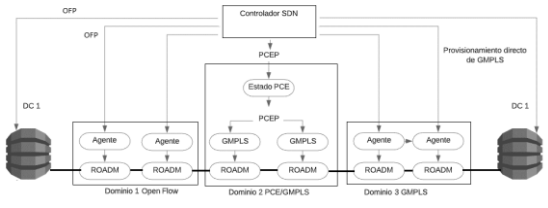

Figura 3: Modelo controlador SDN para dominios heterogéneos OpenFlow/GMPLS con protocolo OpenFlow, PCEP y aprovisionamiento GMPLS. Fuente: elaboración propia.

5. SEGURIDAD

Los mecanismos de respuesta ante las amenazas que comprometen la funcionalidad de la red SDN, como los ataques de fuerza bruta, Phishing, DDos, ataques de amenaza persistente (APT) o Ramsonware, son poco efectivos [49], ya que muchas veces el usuario realiza un simple reinicio para volver al sistema a un estado seguro [50]. Este tipo de soluciones en un Data Center, un centro médico o una industria, son deficientes debido a su funcionalidad critica, puesto que se debe garantizar la disponibilidad del servicio en todo momento y en cada subsistema que integre a la red SDN [51], debido a que se centraliza la administración en un nodo principal que al ser atacado dejaría en estado crítico a todo el sistema [52]. Por lo tanto, el plano de control que es el encargado de asignar las políticas de seguridad que se implementarán en la red, debe contemplar las acciones de respuesta antes las amenazas que a las que se expone el sistema [53].

Se han desarrollado mecanismos de seguridad para mitigar las amenazas a las que se enfrenta la red SDN, manejando filtros de reconocimiento que analizan el contenido y la valides de los paquetes, como lo hace el Gateway que es la primera línea de seguridad que se presenta en la red, siendo la responsable de certificar la fuente de los paquetes que viajen por la plataforma [54]. Siendo tan importante esta labor de la puerta de enlace, el plano de control debe confirmar de alguna manera la asertividad del Gateway, este tipo de validaciones sobre contenidos de paquetes es una tarea bastante rigurosa y sensible para la seguridad de la red, por lo que se ha querido implementar la tecnología Blockchain que realiza la verificación de paquetes de una manera instantánea y ha sido implementada por organizaciones públicas y privadas, debido a su potencial en tecnología que se enfoca en un modelo estructural de datos distribuido a prueba de manipulaciones de réplica y que se comparte con los subdominios de la red [55].
La estructura de datos implementada genera un Hash de seguridad que se crea al momento de detectar el paquete y este Hash contendrá el ID de la información que contenga dicho paquete, con esto si se llega a modificar algún dato de la información del paquete, el Hash original se podrá comparar con el Hash que se genera por la modificación que se realice y al comparar los Hash, se evidenciará que el paquete detectado fue alterado con respecto a la información original del paquete [56].
El Hash de seguridad se genera en el contenido del bloque o en su encabezado, contiene un subconjunto del registro general de transacciones realizado por todos los subdominios interconectados que posean acceso al sistema y que incluya una referencia al Hash de los bloques anteriores. Por medio de este método se genera un enlace entre bloques que se conecta en forma de cadena, como se muestra en la figura 4.

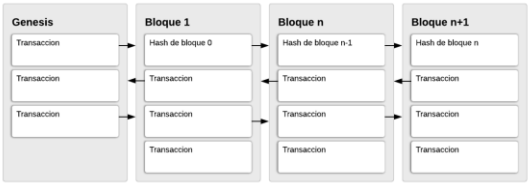

Figura 4: Cadena de bloques Blockchain. Fuente: Elaboración propia.

Como se puede observar, el único bloque con una estructura ligeramente diferente es el primer bloque, al que se le conoce como Genesis y el cual es el encargado de permitir la distribución con todos los clientes que tengan acceso a la red Blockchain, además puede usarse como una clave para el contenido encriptado de la red [57]. Por medio de este proceso los nodos de la red son capaces de analizar el contenido almacenado en la estructura de datos, lo que permite una impresión en tiempo real del estado de la red [58]. La estructura de datos que utiliza Blockchain es distribuida, lo que permite que los nodos pertenecientes a la red se puedan comunicar de manera instantánea, los nodos que tengan autorización de rastreo pueden validar los datos almacenados en los paquetes que ingresen al sistema, sin importar el volumen de información, se dispone de una base de datos distribuida y encriptada totalmente confiable ya que se actualiza constantemente debido a su estructura distribuida [59].

Las Blockchain son de total confiabilidad en cuanto a la integridad de sus datos, ya que los algoritmos que implementan son robustos y no permiten que se vulneren, adicional a esto las cadenas Blockchain, capturan las modificaciones que se realicen a los paquetes, por lo que el Hash de seguridad recibiría modificaciones y se detectaría la amenaza de manera inmediata, el bloque Genesis al ser el nodo principal de la cadena, es el más fuerte, por lo que

vulnerar su seguridad es bastante complejo [60]. Estas características de seguridad hacen del Blockchain, un método eficaz para el plano de control en la red SDN [61].

5.1 OpenFlow

El estándar más popular de los administradores de redes SDN, es OpenFlow, ya que permite controlar de manera más efectiva las tablas de enrutamiento de forma remota [62]. Este protocolo OpenFlow se desarrolló en 2007 por parte del sector académico y empresarial, con ayuda de las universidades de Stanford y California, actualmente la Open Networking Foundation (ONF) se encarga de la definición del estándar. OpenFlow registra el flujo de paquetes por medio de la tabla Flow table que almacena datos del paquete como lo son: Dirección de origen, dirección de destino, puerto de origen, puerto de destino, DSCP, ID usuario, ID proyecto y numero de protocolo [63].

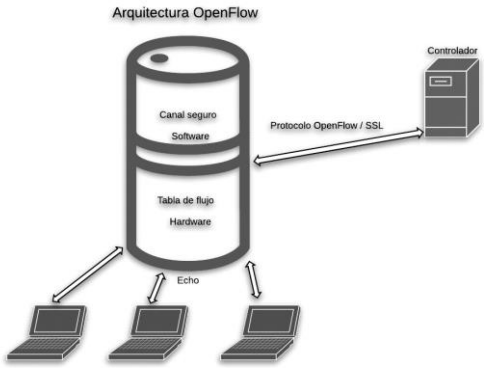

Figura 5: Arquitectura OpenFlow. Fuente: Elaboración propia.

El respaldo de la información para la organización siempre ha sido un tema de gran importancia, por medio de la orquestación en la nube se dirige a la composición de los elementos en el sistema, que respaldan las actividades de la red, proporcionado coordinación y administración de los servicios [64]. Esto con el fin de reducir el uso de la arquitectura de la red, dejando la gestión del sistema más aprovechable para el administrador de redes, que se puede encargar de optimizar la seguridad del plano de control que es el nodo principal de la red y por lo tanto sería el punto más considerado a atacar por las amenazas externas de la organización. Considerando que al ser este el punto principal de administración y gestión de la red debe contar con todos los niveles de seguridad necesarios y contar con planes de acción frente a los riesgos que se puedan generar en la actividad de la red [65].

6. CONCLUSIONES

En este artículo se ha desarrollado una revisión de las categorías más relevantes del modelo de red SDN, permitiendo un marco de referencia para futuras investigaciones. Para esto se realizó la descripción de la arquitectura y de las capas de red, contextualizando al lector en la funcionalidad de sus componentes y de la importancia de cada uno de estos. Las aplicaciones que articulan redes SDN como IoT, Data centers y 5G, fueron documentadas, además se tuvo un énfasis en la problemática de seguridad que ha tenido SDN, ya que su modelo de administración centralizado implica un gran riesgo si se llega a recibir un ataque a este nodo, implicando la caída de toda la red y la negación de servicios. Se han ido implementando desarrollos para subsanar este peligro, por medio de políticas de seguridad que se encargan de prevenir todo tipo de ataques al core de la red, por medio del protocolo OpenFlow que permite gestionar la red como un todo, facilitándole al administrador de la red, la gestión de los dispositivos de hardware y software.

REFERENCIAS

[1] Cinco factores que frenan la instalación de redes de los operadores, El financiero, diciembre 2019. [En línea]. Disponible en: https://www.elfinancierocr.com/tecnologia/cinco-factores-que-frenan-la-instalacion-de-redes-de-losoperadores/S6OKPK6YK5DJTPSZK6S74B3DLM/story/

[2] W. Haisang, "From Clean Slate to SDN," Huawei Corp, octubre 2019. [En línea]. Disponible en: https://www.huawei.com/en/industry-insights/outlook/europe-strengths-encourage-digital-investment.

[3] T. Nadeau and K. Gray, An Auhoritative Review of Network Programmability. Technologies. 2013.

[4] D. Maldonado, "Diseño e implementación de una aplicación bajo una Arquitectura SDN," Pontif. Univ. Javeriana-Bogotá, pp. 1–80, 2014.

[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "OpenFlow," ACM

SIGCOMM Comput. Commun. Rev, vol. 38, no. 2, p. 69, Doi:10.1145/1355734.1355746. marzo 2016.
[6] Stanford University, "Ethane: una arquitectura de protección para redes empresariales". Octubre 2019 [Online]. Disponible en: http://yuba.stanford.edu/ethane/.
[7] Radius Stories at the Edge, "Redes y seguridad" marzo 2018. [Online]. Disponible en: https://www.vmware.com/radius/topic/network-security/.
[8] R. Hernández Sampieri, C. Fernández Collado, and M. D. P. Baptista Lucio, Metodología de la investigación. Bogotá: MC GRAW HILL. 2014. PP. 92-100.
[9] Open Networking Foundation, "Arquitectura de las redes definidas por software (SDN)," noviembre 2019. [En línea]. Disponible en: www.opennetworking.org.
[10] B. Valencia, S. Santacruz, and L. Y. B. J. J. Padilla, "Mininet: una herramienta versátil para emulación y prototipado de Redes Definidas por Software 1 Mininet". Entre ciencia e ingeniería, Vol. 17, pp. 62–70, 2015.
[11] M. I. Hamed, B. M. Elhalawany, M. M. Fouda, and A. S. T. Eldien, "A Novel Approach for Resource Utilization and Management in SDN", International Computer Engineering Conference (ICENCO), 2017, pp. 5–7.
[12] B. Pandya, "Framework for Securing SDN Southbound communication", International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2017, pp. 6–9.
[13] A. Jalili, H. Nazari, S. Namvarasl, and M. Keshtgari, "A Comprehensive analysis on Control Plane Deployment in SDN: In-Band versus Out-of-Band solutions" IEEE 4th International Conference on Knowledge-Based Engineering and Innovation (KBEI), 2017, pp. 1025–1031.
[14] L. Richarson and S. Ruby, "RESTful Web Services". EEUU: O'REILLY, 2008, PP 94-102.
[15] K. Pentikousis, Y. Wang, and W. Hu, "Mobile Flow: Toward Software-Defined Mobile Networks," IEEE Commun. Mag, vol. 51, 2013, pp. 44–53.
[16] J. Tourrilhes, P. Sharma, S. Banerjee, and J. Pettit, "SDN and OpenFlow Evolution: A Standards Perspective," Computer (Long. Beach. Calif), vol. 47. 2014, p. 22–29.
[17] W. Zhou, L. Li, and W. Chou, "SDN Northbound REST API with Efficient Caches". International Conference on Web Services, 2014, p. 257–264.
[18] W. Zhou, L. Li, M. Luo, and W. Chou, "REST API Design Patterns for SDN Northbound API". 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, p. 358–365.
[19] SDX Central, "What is VMware NSX and VMware SDN Network Virtualization?", noviembre 2019. [En línea]. Disponible en: https://www.sdxcentral.com/vmware/definitions/what-is-vmware-nsx/.
[20] P. Morreale and J. Anderson, "Software Defined Networking," Univ. Politec. Catalunya, noviembre 2014. p. 1–67.
[21] B. Y. Yoon and J.-H. Lee, "Transport SDN Architecture for Distributed Cloud Services", 12th International Conference on Optical Internet 2014. pp. 14–15
[22] L. Cui, F. R. Yu, and Q. Yan, "When big data meets software-defined networking: SDN for big data and big data for SDN," IEEE Netw., vol. 30, junio 2016. p. 58–65.
[23] H. Jang and J. Lin, "SDN Based QoS Aware Bandwidth Management Framework of ISP for Smart Homes," 2017 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Cloud Big Data Comput. Internet People Smart City Innov. 2017. pp. 1– 6.
[24] A. Mckeown, H. Rashvand, T. Wilcox, and P. Thomas, "Priority SDN Controlled Integrated Wireless and Powerline Wired for Smart-Home Internet of Things", in 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015. p. 1825–1830.
[25] T. Theodorou and L. Mamatas, "CORAL-SDN: A software-defined networking solution for the Internet of Things", 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 2017, p. 1–2.
[26] P. Bosshart, D. Daly, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker, "Programming Protocol- Independent Packet

Processors", ACM DIGITAL LIBRARY. 2013. vol. 44, p. 88–95
[27] "Open Source Mano – ETSI", OSM, noviembre 2019, [En línea]. Disponible en: https://osm.etsi.org/.
[28] R. Bifulco and R. Canonico, "Analysis of the handover procedure in Follow-Me Cloud," 2012 1st IEEE Int. Conf. Cloud Networking, CLOUDNET 2012, 2012. PP 185–187.
[29] M. B. Al-Somaidai, "Survey of Software Components to Emulate OpenFlow Protocol as an SDN Implementation," Am. J. Softw. Eng. Appl, 2014, vol. 3, no. 6, p. 74.
[30] S. Ali and M. Ghazal, "Real-time Heart Attack Mobile Detection Service (RHAMDS): An IoT use case for Software Defined Networks" in 2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE), 2017, p. 1–6.
[31] P. Demestichas, A. Georgakopoulos, D. Karvounas, K. Tsagkaris, V. Stavroulaki, J. Lu, C. Xiong, and J. Yao, "5G on the Horizon: Key Challenges for the Radio-Access Network" IEEE Veh Technol Mag, 2013. vol. 8, p. 47–53.
[32] A. De La Oliva, X. C. Perez, A. Azcorra, A. Di Giglio, F. Cavaliere, D. Tiegelbekkers, J. Lessmann, T. Haustein, A. Mourad, and P. Iovanna, "Xhaul: toward an integrated fronthaul/backhaul architecture in 5G networks" IEEE Wirel. Commun, 2015, vol. 22, PP 32–40.
[33] A. Sutton, "5G network architecture," J. Inst. Telecommun. Prof, 2018, vol. 12, pp. 8–15, 2018.
[34] X. Costa Perez, A. Garcia Saavedra, L. XI, T. Deiss, and O. De La Antonio, "5G- Rosshaul: an Sdn / Nfv Integrated Fronthaul / Backhaul Transport Network Architecture" vol. 24, no. February,2017, pp. 38–45.
[35] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper - Cisco", Cisco, noviembre 2019, [En línea]. Disponible en: https://www.cisco.com/c/dam/m/en_in/innovation/enterprise/assets/mobile-white-paper-c11-520862.pdf.
[36] "P4 Language Consortium", Git Hub, noviembre 2019, [En línea]. Disponible en: https://p4.org/.
[37] G. Bianchi, E. Biton, N. Blefari-Melazzi, I. Borges, L. Chiaraviglio, P. de la Cruz Ramos, P. Eardley, F. Fontes, M. J. McGrath, L. Natarianni, D. Niculescu, C. Parada, M. Popovici, V. Riccobene, S. Salsano, B. Sayadi, J. Thomson, C. Tselios, and G. Tsolis, "Superfluidity: a flexible functional architecture for 5G networks," Trans. Emerg. Telecommun. Technol. 2016, vol. 27, p. 1178–1186.
[38] Open Networking Lab (ON. Lab), "ON. Lab Delivers Software for New Open Source SDN Network Operating System - ONOS", 2017. [En línea]. Disponible en: https://www.prnewswire.com/news-releases/onlab-delivers-software-for-new- open-source-sdn-network-operating-system--onos-300004797.html.
[39] J. Teixeira, G. Antichi, A. Del Chiaro, S. Giordano, and A. Santos, "Datacenter in a Box: Test Your SDN Cloud-Datacenter Controller at Home" in 2013 Second European Workshop on Software Defined Networks, 2013, p. 99–104.
[40] A. Asensio, L. Gifre, M. Ruiz, and L. Velasco, "Carrier SDN for flexgrid-based inter-datacenter connectivity" in 2014 16th International Conference on Transparent Optical Networks (ICTON), 2014, PP 1– 4.
[41] P. Varga, G. Kathareios, A. Mate, R. Clauberg, A. Anghel, P. Orosz, B. Nagy, T. Tothfalusi, L. Kovacs, and M. Gusat, "Real-time security services for SDN- based datacenters," in 2017 13th International Conference on Network and Service Management (CNSM), 2017, PP 1–9.
[42] W. Hong, K. Wang, and Y H. Hsu, "Application-Aware Resource Allocation for SDN-based Cloud Datacenters," in 2013 International Conference on Cloud Computing and Big Data, 2013, p. 106–110.
[43] P. Samadi, D. Calhoun, H. Wang, and K. Bergman, "Accelerating Cast Traffic Delivery in Data Centers Leveraging Physical Layer Optics and SDN" IFIP Int. Conf. Opt. Netw. Des. Model, 2014, PP 73–77.
[44] Y. Han, S. Seo, J. Li, J. Hyun, J. Yoo, and J. Hong, "Software defined networking-based traffic engineering for data center networks" Netw. Oper. Manag. Symp. (APNOMS), 2014 16th Asia-Pacific, 2014, p. 1–6.
[45] I. Elgendi, K Munasinghe, and A. Jamalipour, "A three-tier SDN architecture for DenseNets" in 2015 9th International Conference on Signal Processing and Communication Systems (ICSPCS), 2015, vol. 1, p. 1–7.
[46] I. Monga, E. Pouyoul, and C. Guok, "Software-Defined Networking for Big- Data Science - Architectural Models from Campus to the WAN" in 2012 SC Companion: High Performance

Computing, Networking Storage and Analysis, 2012, p. 1629–1635.
[47] "ITU- Software-defined Networking (SDN)", ITU, noviembre 2019 [En línea]. Disponible en: https://www.itu.int/en/ITU-T/sdn/Pages/default.aspx.
[48] P. Qin, B. Dai, B. Huang, and G. Xu, "Bandwidth-Aware Scheduling With SDN in Hadoop: A New Trend for Big Data," IEEE Syst, diciembre 2017, vol. 11, PP. 2337– 2344.
[49] A. Khan and B. Ratha, "Time series prediction QoS routing in software defined vehicular ad-hoc network" in 2015 International Conference on Man and Machine Interfacing (MAMI), 2015, PP 1–6.
[50] P. Jayashree and F. Princy, "Leveraging SDN to Conserve Ener in WSN An Analysis" 2015 3rd Int. Conf. Signal Process. Commun. Netw, 2015. PP 6-15.
[51] S. Jain, M. Zhu, J. Zolla, U. Hölzle, S. Stuart, A. Vahdat, A. Kumar, S. Mandal,
J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer and J. Zhou, "B4," in Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM - SIGCOMM 13, 2013, PP 3.
[52] S. Lazar and C. Stefan, "Future vehicular networks: ¿what control technologies?" Commun. (COMM), 2016 Int. Conf, PP 337–340.
[53] E. Ali, M. Manel and Y. Habib, "An Efficient MPLS-Based Source Routing Scheme in Software-Defined Wide Area Networks (SD-WAN)" in 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), 2017, PP. 1205–1211.
[54] E. Rojas, "From Software-Defined to Human-Defined Networking: Challenges and Opportunities," IEEE Netw, enero 2018, vol. 32, p. 179–185.
[55] T. Ninikrishna, S. Sarkar, R. Tengshe, M. Jha, L. Sharma, V. Daliya and
S. Routray, "Software defined IoT: Issues and challenges" Proc. Int. Conf. Comput. Methodol. Commun. ICCMC 2017, vol. 2018, PP. 723–726.
[56] M. Ketel, "Enhancing BYOD Security through SDN" SoutheastCon 2018, pp. 1–2.
[57] "IRTF Software-Defined Networking Research Group (SDNRG)", IRTF, noviembre 2019, [En línea]. Disponible en: https://irtf.org/concluded/sdnrg.
[58] H. Jang, C. Huang and F. Yeh, "Design a bandwidth allocation framework for SDN based smart home" 7th IEEE Annu. Inf. Technol. Electron. Mob. Commun. Conf. IEEE IEMCON 2016, pp 6-12.
[59] Huawei Technologies Inc, "Huawei Agile Campus Network Solution Brochure" noviembre 2019. [En línea]. Disponible en: https://e.huawei.com/ru/related-page/solutions/technical/agile-networking/agile-campus-solutions/agile-campus/brochure/Solutions_Campus_network.
[60] SdxCentral LLC, "Network Virtualization Report" Ind. Rep. pp 1–44, 2017.
[61] J. Rodriguez, "Integración de redes IP utilizando SDN" Inst. Tecnológico Buenos Aires, 2017, PP 27-32.
[62] ON. LAB, "Introducing ONOS - a SDN network operating system for Service Providers", Technical report, 2014, vol. 1, p. 14.
[63] J. Medve, R. Varga and A. Tkacik, "OpenDaylight: Towards a model-driven SDN controller architecture," rock. IEEE 15th Int. Symp. World Wireless, Mob. Multimed. Netw,2014, pp. 1–6.
[64] M. Paliwal, D. Shrimankar, and O. Tembhurne, "Controllers in SDN: A Review Report" IEEE Access, vol. 6, p. 36256–36270.
[65] "ETSI - Network Functions Virtualization", ETSI, noviembre 2019, [En línea]. Disponible en: https://www.etsi.org/technologies-clusters/technologies/nfv.