UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE GUAYAQUIL

CARRERA DE COMPUTACIÓN

"ANÁLISIS SISTEMÁTICO DE MODELOS DE SEGURIDAD Y CONTROL DE ACCESO EN ARQUITECTURA SDN PARA LA DETENCIÓN DE ANOMALÍAS"

Trabajo de titulación previo a la obtención del

Título de Ingeniero en Ciencias de la Computación

AUTORES: ACOSTA GONZÁLEZ OTTO SEBASTIÁN

ORTEGA ÁVILA ELISA ABIGAIL

TUTOR: HUILCAPI SUBIA DARÍO, MSIG.

Guayaquil – Ecuador

2023

CERTIFICADO DE RESPONSABILIDAD Y AUTORIA DEL TRABAJO DE TITULACIÓN

Nosotros, Acosta González Otto Sebastián con documento de identificación N° 0941717878 y Ortega Avila Elisa Abigail con documento de identificación N° 0953496098; manifestamos que:

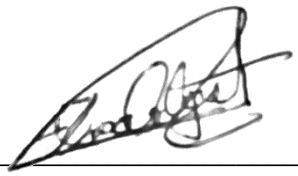
Somos los autores y responsables del presente trabajo y autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Guayaquil, x de agosto del año 2023

Atentamente,

Acosta González Otto Sebastián

0941717878



Ortega Avila Elisa Abigail

0953496098

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE

TITULACIÓN A LA UNIVERSIDAD POLITECNICA SALESIANA

Nosotros, Acosta González Otto Sebastián con documento de identificación N° 0941717878 y Ortega Avila Elisa Abigail con documento de identificación N° 0953496098, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Articulo Académico: "ANÁLISIS SISTEMÁTICO DE MODELOS DE SEGURIDAD Y CONTROL DE ACCESO EN ARQUITECTURA SDN PARA LA DETENCIÓN DE ACCESOS NO AUTORIZADOS", el cual ha sido desarrollado para optar por el título de: Ingeniero en Computación, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

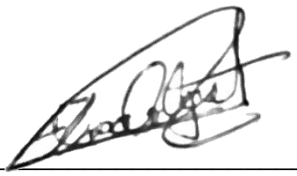
En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Guayaquil, x de agosto del año 2023

Atentamente,

Acosta González Otto Sebastián

0941717878



Ortega Avila Elisa Abigail

0953496098

CERTIFICADO DE DIRECCION DEL TRABAJO DE TITULACION

Yo, Dario Fernando Huilcapi Subia con documento de identificación N° 0920375177, docente de la Universidad Politécnica Salesiana, declaro que bajo mi tutoría fue desarrollado el trabajo de titulación: ANÁLISIS SISTEMÁTICO DE MODELOS DE SEGURIDAD Y CONTROL DE ACCESO EN ARQUITECTURA SDN PARA LA DETENCIÓN DE ACCESOS NO AUTORIZADOS, realizado por Acosta González Otto Sebastián con documento de identificación N° 0941717878 y Ortega Avila Elisa Abigail con documento de identificación N° 0953496098, obteniendo como resultado final el trabajo de titulación bajo la opción Articulo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Guayaquil, x de agosto del año 2023

Atentamente,

Huilcapi Subia Dario Fernando

0920375177

DEDICATORIA

Dedico este trabajo a mis padres Otto Hans que gracias a él me impulsó a seguir estudiando y poder crecer continuamente, mostrándome que siempre en la vida se está aprendiendo sobre todo si lo intentas en todo momento, ya que él quien me ha mostro el gusto por la computación y que me mostró el significado de no ahogarme en la orilla.

Acosta González Otto Sebastián

Dedico este trabajo a Dios quien por el estoy aquí y me ha dado fuerza desde el primer día que inicie esta aventura que ha marcado un crecimiento en mi vida. También a mis padres y mi abuelito que por ellos han tenido fe y me han enseñado a esforzarme en todo lo que haga en mi vida ya que han invertido tanto tiempo en mí y no puedo estar más agradecida con ellos ya que me han ayudado en todo. Por otro lado, quiero dedicar este trabajo a mi amiga Rebeca ya que ella ha sido mi ancla, me ha visto en los días que no he estado bien y ella ha tenido unos sabios consejos que el día de hoy lo he puesto en práctica. Así que este trabajo con todo mi esfuerzo, dedicación se lo dedico a estas personas que son importante de mi vida.

Ortega Avila Elisa Abigail

AGRADECIMIENTO

Quiero dar gracias a mi padre Otto y a mi madre Sofia que durante toda mi carrera profesional me apoyaron para seguir estudiando, así mismo agradecer a mis tías Carmen, Nadia y María que me dieron esa alegría de saber qué en algún momento podría lograrlo. Y un especial agradecimiento a mi abuelo Otto "Papoto" Acosta que fue un gran pilar en mi vida, dándome ese empujón cada que lo necesitaba, acompañándome durante casi toda mi carrera y mostrándome el significado de que toda la familia está llena de mucho "cacumen".

Acosta González Otto Sebastián

Quiero dar gracias a Dios por haberme puesto en este lugar, por darme y enseñando el sentido de las palabras sabiduría, fe y fuerza que sin él no estaría aquí, así como no podía estar agradecida con él. Dar las gracias a mis padres y mi abuelito por haber invertido en mi vida estudiantil en la forma económica y sentimental que nunca me falto ese refugio para aprender cómo enfrentar la vida y sus problemas. Doy gracias a mi amiga Rebeca que desde que empecé le contaba como siempre me iba y ella tan solo escucharme me impartía sus consejos de cómo sobrevivir y que todo esto nos enseña a ser buenos profesionales para ayudar a las demás generaciones. Por último, gracias a mi compañero de trabajo que siento respeto y admiración que cada día aprendo más me siento orgullosa haber trabajado contigo. No puedo estar más agradecida con ellos solo puedo decir gracias.

Ortega Avila Elisa Abigail

RESUMEN

Actualmente gracias al desarrollo continuo de redes definidas por software (Software-Defined Network) la industria de redes ha tenido una mayor demanda, así como un cambio en la estructura y arquitectura de las redes tradicionales. Sin embargo, junto con estos avances se ha producido un aumento de los problemas de seguridad y las preocupaciones sobre el acceso en el SDN, donde el control de la red se centraliza a través de un controlador lógico y la infraestructura de la red se hace programable.

Este estudio académico ofrece un análisis sistémico de los modelos de seguridad y control de acceso de la arquitectura SDN, con un enfoque analítico en el cual se identifican anomalías y accesos no autorizados. Teniendo como objetivo general realizar un análisis sistemático de los modelos de seguridad y control de acceso en la arquitectura SDN con en el fin de evaluar su efectividad en detección de anomalías, así mismo como objetivos específicos, identificar limitaciones y desafíos actuales de estos modelos, proponer pautas para el diseño e implementación para modelos de seguridad.

Tomando en cuenta que las redes SDN están hechas para dar soluciones a la flexibilidad y escalabilidad de las redes tradicionales, por ello la red SDN se transforma en una gran alternativa para los problemas de administración. En la propuesta se realizó un análisis exploratorio implementando una metodología de organización PRISMA que nos permitan conocer los modelos de seguridad implementados en redes SDN. Proponiendo como resultado implementación autenticación en dos pasos y cambio de credenciales en sistemas de accesos, para así evitar ingresos no autorizados y aumentar su resistencia a las nuevas amenazas.

Palabra Clave: Control de acceso, modelos de seguridad, Redes definidas por software (SDN), accesos no autorizados, revisión sistemática, malware, nodos, PRISMA.

ABSTRACT

Currently, thanks to the continuous development of software-defined networks (Software-Defined Network), the network industry has had a greater demand, as well as a change in the structure and architecture of traditional networks. However, along with these advances has come an increase in security issues and access concerns in SDN, where control of the network is centralized through a logic controller and the network infrastructure is made programmable.

This academic study offers a systemic analysis of the security and access control models of the SDN architecture, with an approach in which to identify anomalies or unauthorized access. Having as a general objective to carry out a systematic analysis of the security and access control models in the SDN architecture to evaluate their effectiveness in detecting anomalies, as well as specific objectives, to identify limitations and current challenges of these models, to propose Guidelines for the design and implementation of security models.

Considering that SDN networks are made to provide solutions to the flexibility and scalability of traditional networks, therefore the SDN network becomes a great alternative for administration problems. In the proposal, an exploratory analysis was carried out implementing a PRISMA organization methodology that will allow us to know the security models implemented in SDN networks. Proposing as a result the implementation of two-step authentication and change of credentials in access systems, to avoid unauthorized entry and increase their resistance to new threats.

Keywords: Access control, security models, Software Defined Networking (SDN), unauthorized access, systematic review, malware, node, PRISMA.

ÍNDICE

Listado de Acrónimos.

Tabla 1. Listado de Acrónimos.

SDN	Software Defined Networking
API	Application Programming Interface
DDoS	Distributed Denia of Service
DoS	Denial of Service
NFV	Virtualization of Network Functions
NAC	Network Acces Control
IoT	Internet of Things
SDP	Session Description Protocol

Fuente: creado por los autores.

1. Introducción

La importancia de la seguridad en las redes está aumentando debido al rápido avance y expansión de estas plataformas. Las redes SDN (Redes Definidas por Software) están ganando popularidad debido a que brindan un enfoque centralizado y programable para controlar de forma remota el comportamiento de los paquetes que ingresan, lo que resulta en una mejora en el rendimiento, control, gestión y flexibilidad de la red. A pesar de contar con múltiples técnicas disponibles para detectar anomalías y controlar el tráfico, es imprescindible continuar investigando y proponiendo mejoras más afectivas con el fin de identificar irregularidades de manera más eficiente.

En este estudio científico se analizan las restricciones y retos actuales de estos modelos, al mismo tiempo que se sugieren mejoras y métodos más efecticos para detectar anomalías en redes SDN en las etapas iniciales. Adicionalmente, se ofrecen sugerencias y directrices para desarrollar e integrar sistemas de seguridad y restricción de acceso más sólidos y eficientes en entornos SDN, lo cual ayuda a salvaguardar y mantener la integridad de las redes. Además, se están examinando y sugiriendo técnicas y metodologías más avanzadas para detectar anomalías en redes SDN en etapas tempranas. Se están considerando enfoques que se basan en el aprendizaje automático, la minería de datos y el monitoreo constante de la red para mejorar la efectividad y la eficiencia en la detección y reducción de riesgos. El propósito principal del articulo consiste en llevar a cabo un análisis sistemático de los patrones de seguridad y mecanismos de control de acceso en la estructura SDN para evaluar cuan efectivos son en la detección de irregularidades, por ello es necesario contestar las siguientes preguntas:

- ¿Cuál es el estado actual de la seguridad y control de acceso en la arquitectura SDN para mitigar un acceso no autorizado?
- ¿Existen modelos de seguridad para identificar posibles amenazas de acceso no autorizado en las redes SDN y que limitaciones tienen?
- ¿Qué propuestas de mejoras se pueden recomendar en la adaptación y aplicación de un modelo de seguridad que nos permita proponer técnicas y metodologías de detección temprana de acceso no autorizado en las redes SDN?

2.1 Revisión de Literatura

2.1.1 SDN

La implementación de la Red Definida por Software (SDN) ofrece una mayor flexibilidad y adaptabilidad en la administración de redes, permitiendo a las organizaciones optimizar las operaciones de red de acuerdo con las necesidades cambiantes. La tecnología SDN se refiere a la división programable de las funciones de control y transferencia en una red, lo que facilita la administración del enrutamiento mediante software, separando de manera lógica o física la gestión de los dispositivos físicos, como conmutadores y enrutadores. Existen distintas redes definidas por software(Ángel Segovia Fernández, 2020)

- **SDN abierta:** Los gestores emplean un protocolo para llevar a cabo la dirección y supervisión en la transferencia de datos dentro de la red. El protocolo ampliamente reconocido y normalizado es el OpenFlow.
- **SDN por API:** Sustituye la utilización de protocolos públicos con interfaces de programación de aplicaciones, las cuales posibilitan la regulación del flujo de datos a lo largo de la red de dispositivos.

Tanto las SDN abiertas como las API, controlan redes virtuales o de hardware tradicional.

- **SDN hibrida:** Integra a los protocolos de red tradicional con la innovación de las SDN en un solo entorno. SDN permite la integración gradual de SDN en un entorno heredado bajo administración de red mientras los protocolos de red estándar continúan administrando un segmento de tráfico.

2.1.2 OpenFlow

El protocolo OpenFlow, es un componente fundamental de SDN, supuso una revolución en la gestión y el control de redes. OpenFlow, en esencia, divide el plano de control del plano de datos, lo que permite que los controladores de red decidan de forma centralizada sobre el enrutamiento y el flujo de tráfico en lugar de depender de la lógica distribuida en dispositivos de red individuales.(Alsaeedi et al., 2019)

La gestión y la programación dinámicas de la red son posibles al protocolo OpenFlow, que funciona facilitando la comunicación entre los conmutadores y los controladores. OpenFlow simplifica la implementación de políticas de red únicas y se ajusta rápidamente a los patrones de tráfico cambiantes al hacer visibles las tablas de flujo de conmutación y permitir la manipulación directa. En comparación con las estrategias de enrutamiento convencionales, esta abstracción del control de la red ofrece más flexibilidad y una gestión eficaz.(Distrital Francisco José de Caldas et al., 2022)

OpenFlow crea una interfaz que permite la programación directa de dispositivos de red, tanto físicos como virtuales, a través de un controlador centralizado. Su característica única es el uso de flujos, que son reglas predeterminadas que se pueden configurar de forma estática o dinámica a través del controlador SDN(Leandro & Mejía, 2018a)

OpenFlow ayuda a que la red sea más dinámica y este bajo su control, mejorando así las cualidades adaptables y manejables de la arquitectura SDN.(Ángel Segovia Fernández, 2020)

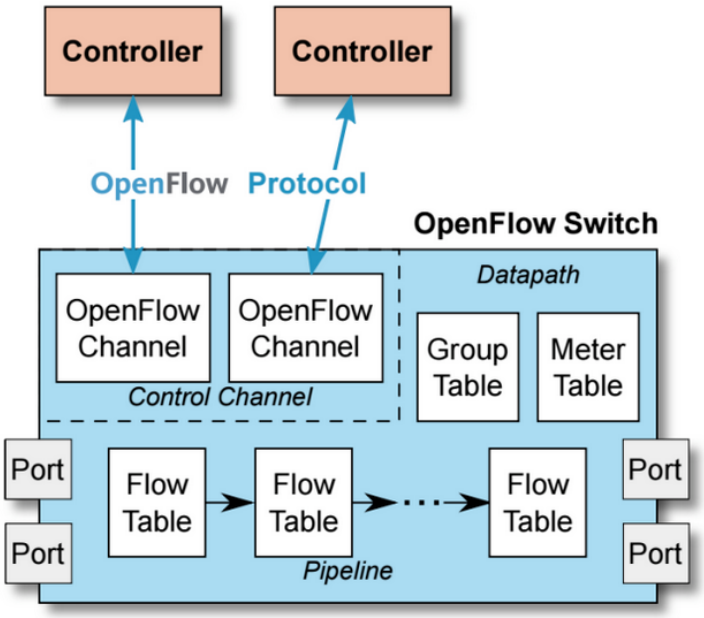


Figura 1.Arquitectura OpenFlow(Distrital Francisco Jose de Caldas et al., 2022)

2.1.3 Composición de la administración de la red

Debemos señalar que la rede definida por software SDN es el enfoque de la arquitectura de red esto permite que los administradores de red puedan gestionar de forma eficaz de los recursos de red a través de la centralización de software. Esto hace que la gestión de red sea más flexible y controlada para separar los planos de control y de datos en una arquitectura SDN.

El controlador SDN es el elemento central de la arquitectura, está a cargo de supervisar la gestión de dispositivos de red y la organización de flujo de datos. La arquitectura SDN abstrae varias capas de red, lo que permite que la red sea ajustable y hábil. La arquitectura SDN tiene como objetivo aumentar la flexibilidad de la red, la simplicidad de administración y la eficacia.(Ciena, 2023)

2.1.4 Vista de la topología de la red

En la arquitectura SDN (Software-Defined Networking), La entidad central es el controlador SDN. El controlador tiene varias funciones en SDN, como:

- Proporcionar una visión global de la topología de la red.
- Mantener las políticas de red y aplicar las medidas de seguridad de la red.
- Proporcionar una interfaz programable a los componentes de la red.
- Orquestar tareas como la configuración, gestión y optimización de la red.
- Proporcionar API de acceso norte a aplicaciones externas para acceder a servicios e información de red.

La arquitectura SDN suele incluir tres capas: la capa de aplicación, la capa de control y la capa de infraestructura. La capa de infraestructura contiene los dispositivos de red, como

conmutadores y enrutadores, mientras que la capa de control contiene el controlador SDN, y la capa de aplicación contiene las aplicaciones o funciones de red que utilizan las organizaciones.

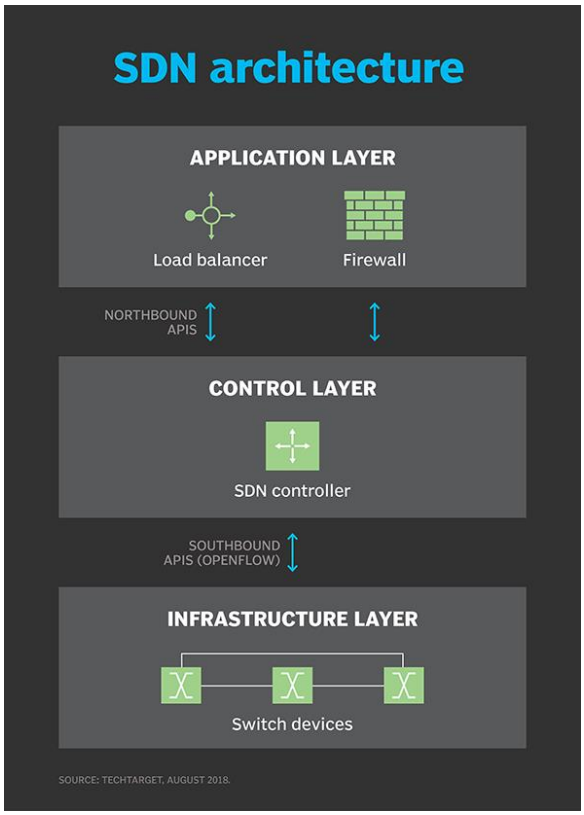


Figura 2. Arquitectura SDN (TechTarget, 2023)

La arquitectura SDN está diseñada principalmente para proporcionar una infraestructura de red centralizada, programable y flexible que pueda satisfacer mejor las demandas cambiantes de las aplicaciones y servicios modernos.(TechTarget, 2023)

Existen dos categorías las funciones del plano de control y las funciones del plano de datos de la arquitectura SDN. Los componentes físicos son administrados por operaciones del plano de control, incluido el establecimiento de políticas, la configuración de dispositivos de red y el control de patrones de tráfico. El controlador SDN, quien supervisa la administración de la red. Actúa como el elemento central de una SDN al controlar el flujo de datos a través de la red. Entre las operaciones cruciales del plano de control de una arquitectura SDN se encuentran la política de red, la configuración de red y la ingeniera de tráfico.

El procesamiento y la gestión del tráfico de red es responsable de las tareas del plano de datos. Se instala en hardware de red como conmutadores y enrutadores. El plano de datos de la arquitectura SDN. El controlador SDN programa el plano de datos. Enruta el tráfico de acuerdo con las políticas comerciales establecidas.

El enrutamiento, el procesamiento de paquetes y la clasificación de flujos son ejemplos de operaciones. La arquitectura SDN permite que sea flexible, ágil y escalable.

Las funciones de red del hardware propietario e implementarías en el software, la virtualización de funciones de red (NFV) es una arquitectura de red que tiene el objetivo de aumentar la agilidad y eficiencia de la red. La escalabilidad, la flexibilidad y capacidad de administración de la red están destinadas a facilitar a los operadores de red la implementación de nuevos servicios de manera más rápida y económica. NFV y SDN, ofrecen un marco para automatizar el control programático del tráfico de red, el uso de la virtualización de funciones de red como firewalls, balanceadores de carga y enrutadores, está creciendo en el campo de las telecomunicaciones ya que se implementan el NFV y SDN esto permite que las organizaciones ser más adaptables y responder mejor a las necesidades comerciales(ETSI, 2023).

2.1.5 NFV

Es un paradigma disruptivo en el campo de las redes de comunicación que tiene como objetivo alterar la forma en que se diseñan, implementan y gestionan las funciones de red que se han basado en hardware especializado. Las funciones de red como enrutadores, firewalls, balanceadores de carga y más se virtualizan y ejecutan como software en servidores de hardware normales a través de NFV. Para facilitar una implementación y una gestión más rápidas y eficaces de las funciones y los servicios de la red, el principal objetivo de NFV es aumentar la flexibilidad, la agilidad y la eficiencia de las redes. (Alenezi et al., 2019)

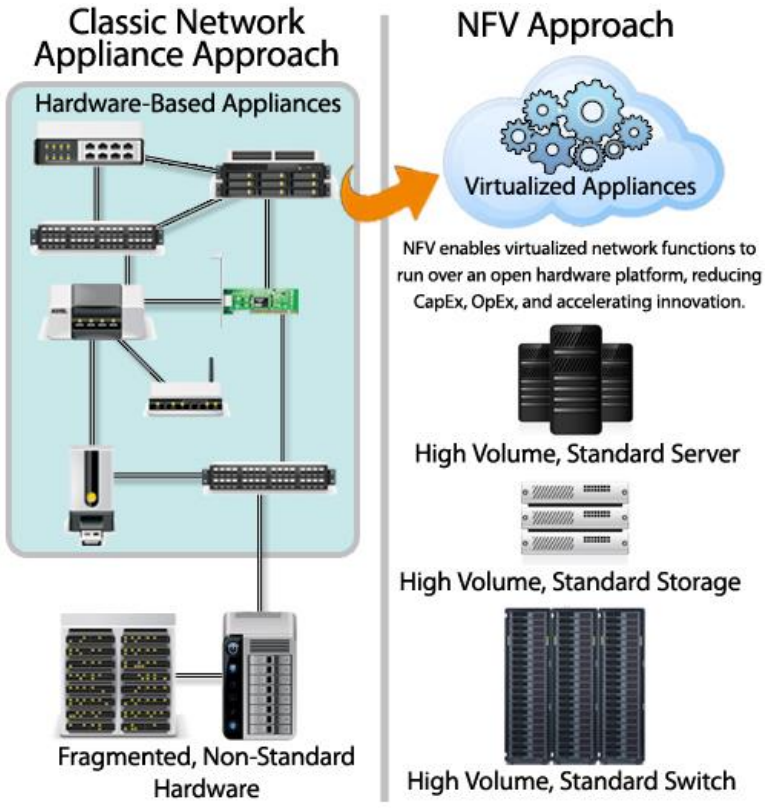


Figura 3. Función NFV (Mijumbi et al., 2016)

2.1.6 Ventajas / Desventajas de SDN

A continuación, se presenta una serie de ventajas y desventajas de la estructura SDN.

VENTAJAS.

- **Flexibilidad:** la capacidad de reconfigurar y adaptar la red de manera rápida y centralizada en respuesta a los resultados cambiantes.(Benzekki et al., 2016)
- **Agilidad:** La capacidad de introducir de forma rápida y eficaz nuevos programas y servicios, sin alterar la infraestructura subyacente.
- **Eficiencia:** Los costos operativos reducidos y la mayor utilización de la red son los resultados de la administración y optimización de recursos centralizados.
- **Automatización:** Las tareas se pueden automatizar gracias a la capacidad de programación de la red, lo que requiere menos intervención humana.
- **Reducción de Costos:** Al agilizar la gestión de la red y facilitar una utilización más eficaz de los recursos, SDN puede reducir los costos operativos.
- **Centralización del Control:** La red se puede administrar y monitorear fácilmente con la administración centralizada, lo que mejora la optimización y la seguridad de la red.(Shubbar, Alhisnawi, Abdulhassan, & Ahamdi, 2021)

DESVENTAJAS

- **Dependencia de la Infraestructura de Red:** la infraestructura subyacente tiene un impacto significativo en la efectividad de SDN, lo que puede causar problemas si no es lo suficiente confiable.(Yassine et al., 2022)
- **Seguridad:** el controlador SDN debe protegerse con medidas de seguridad adicionales porque la centralización del control puede ser un punto de vulnerabilidad.
- **Implementación Compleja:** Una arquitectura SDN requiere una importante reconfiguración de la infraestructura. SDN agrega una nueva capa de complejidad a la administración de redes porque requiere conocimientos y habilidades especializados para configurar y programar. (Saraswat et al., 2019a)

2.1.7 Acceso no autorizado

El acceso no autorizado describe los intentos o las acciones realizadas para obtener acceso a la red, los dispositivos o los recursos sin la autorización adecuada. Esto podría implicar la manipulación del flujo de datos, cambios de configuración de red, accesos no autorizados y otras actividades maliciosas que ponen en peligro la seguridad y la integridad de la infraestructura SDN.(Correa Chica et al., 2020)

2.1.8 Control de acceso

El proceso de localizar patrones o comportamientos inusuales en el tráfico de la red que podría apuntar a una amenaza de seguridad se conoce como detención de anomalías en la red. Las anomalías pueden incluir patrones de tráfico, grandes cantidades de datos. Los sistemas de detención de anomalías en la red pueden detectar amenazas potenciales al monitorear continuamente la actividad de la red y compararla con patrones conocidos de actividad típica.

Todo esto permite tener alerta los equipos de seguridad para que así tener medidas adecuadas para reducir el daño causado por los ataques y evitar los ataques cibernéticos por completo(Ahmed et al., 2016).

2.1.9 Disponibilidad de equipos autorizados

Solo los dispositivos autorizados y compatibles pueden acceder a una red gracias a Network Access Control (NAC), una herramienta de seguridad que aplica políticas. Esto se logra médiate la autenticación y confirmación de los dispositivos antes de permitirles el acceso a la red. NAC es una parte crucial de la seguridad de la red ya que protege contra los ataques de malware y acceso no autorizado a información privada.

2.1.10 Autorización de acceso

Una herramienta de seguridad NAC regula el acceso a los recursos de la red según la identidad del usuario, el estado del dispositivo y la ubicación. Las tres funciones del NAC son autenticación, autorización, y contabilidad. La autorización confirma que el usuario tiene derechos de acceso a os recursos que ha solicitado, mientras que la autenticación y la contabilidad realizan un seguimiento de la actividad del usuario para las necesidades de auditoría y cumplimiento.

NAC realiza tareas como la evaluación de la seguridad de los terminales, la aplicación de políticas según el libro (Stallings, 2016) la aplicación de políticas garantiza que los usuarios y los dispositivos cumplan con las políticas de seguridad de la red, mientras que la evaluación de la seguridad de los terminales ve las vulnerabilidades de seguridad.

En el artículo de (Al-Shaboti et al., 2018)enfatiza la importancia de NAC en la defensa contra amenazas internas y acceso no autorizado. Lo que resalta la función del NAC de hacer cumplir las normas de seguridad y asegurarse de que se cumplan.

2.2.11 Mapeo de control de acceso de la red

Para proteger la infraestructura de red programable de SDN, se desarrollaron modelos de seguridad de SDN. El modelo de seguridad OpenFlow, que se cetra en salvaguardar el protocolo OpenFlow, es uno de los modelos más empleados. En un entorno de red distribuida, el modelo de perímetro definido por software SDP ofrece acceso seguro a aplicaciones y recursos.(Goransson et al., 2016) (Scott-Hayward et al., 2015)

En la arquitectura SDN, los modelos de seguridad y el control de acceso se pueden examinar sistemáticamente para encontrar anomalías y asegurarse de que se implemente los controles de seguridad adecuados(Roberto & Sandoval, 2020).

La implementación de modelos de seguridad basados en el acceso y el control de usuarios es parte de la arquitectura de redes definidas por software (SDN)(Roberto & Sandoval, 2020). Las preocupaciones sobre la seguridad y la privacidad han recibido mucha más atención como resultado del crecimiento explosivo de internet de las cosas (IoT).la línea de investigación descrita en(Ing. Norma Beatriz Pérez et al., 2018) se centra en analizar la seguridad en varias

capas de la arquitectura IoT y ofrece soluciones para disminuir las amenazas en los dispositivos IoT. El objetivo del artículo es analizar la seguridad de la red SDN utilizando el modelo OpenFlow y proporcionar una explicación detallada del mismo(Leandro & Mejía, 2018b).

La detección sistemática de anomalías y la implementación adecuada de las medidas de seguridad apropiadas pueden ser asistidas por el análisis de los modelos de control de acceso y seguridad en la arquitectura SDN. El impacto de las limitaciones se puede reducir al diseñar e implementar un sistema de detección de DDoS en redes SDN mediante la implementación de un entorno colaborativo entre el plano de datos programable y el plano de control(Diana Carolina Álvarez Paredes, 2019).

SDN y NFV utilizan una plataforma de administración de nube que es OpenStack. Podemos integrar SDN y NFV en la plataforma en la nube basada en OpenStack para extraer conocimiento práctico de su interacción. OpenStack integra SDN, pero tiene importantes limitaciones prácticas en cuanto a escalabilidad, seguridad y estabilidad. Algunos problemas cruciales y la seguridad general de la nube, sostenemos una arquitectura SDN especifica que puede distribuir sus propios agentes funcionales de red en el plano de datos e implementar aplicaciones en el plano de control para así centralizar las orquestas de red(Krishna et al., 2023).

2.2.12 Orquestación del plano de control

La orquestación se refiere al proceso de coordinar y gestionar los diferentes componentes y servicios de seguridad para asegurar un funcionamiento coherente y eficiente del sistema en su conjunto. La orquestación en este contexto implica la automatización de tareas relacionadas con la configuración, implementación, gestión y supervisión de políticas de seguridad en una red SDN.

Algunos puntos clave para centralizar la orquestación de la red pueden ser:

- Coordinación de políticas de seguridad: La orquestación permite definir y coordinar las políticas de seguridad en la red SDN de manera centralizada. Esto implica la creación y gestión de reglas de acceso, políticas de encriptación, políticas de detección y mitigación de amenazas, entre otros aspectos de seguridad.
- Aprovisionamiento de servicios de seguridad: La orquestación facilita el aprovisionamiento y despliegue automatizado de servicios de seguridad en la red SDN. Esto puede incluir la instalación de firewalls, sistemas de prevención de intrusiones (IPS), sistemas de detección de anomalías y otros dispositivos o servicios de seguridad.
- Coherencia y consistencia en la configuración: La orquestación garantiza la coherencia y consistencia en la configuración de los componentes de seguridad en la red SDN. Esto evita inconsistencias y conflictos que podrían afectar la eficacia y eficiencia de la seguridad en la red.
- Supervisión y gestión centralizada: La orquestación permite supervisar y gestionar de manera centralizada el estado y el rendimiento de los componentes de seguridad en la red SDN. Esto incluye la detección y respuesta a eventos de seguridad, la generación de alertas, y la gestión de políticas en tiempo real.

El controlador SDN, los componentes de red y las políticas de seguridad son los componentes que forman esta orquestación.(Guan et al., 2018) Al automatizar los procesos y optimizar la

programación, la orquestación del plano de control aumentan la eficiencia operativa.(Hasan et al., 2020) Se mejora el rendimiento, reduce la carga administrativa y fomentan la investigación destinada a crear métodos de orquestación rápidos y eficientes. Esta orquestación también le da a la red flexibilidad y adaptabilidad. También mejorado por esta orquestación es la seguridad.(Bannour et al., 2020)

3. Metodología

Se realizará una búsqueda de fuentes relevantes de información a través de una revisión sistemática para analizar diferentes fuentes bibliográficas. Dado que en la revisión bibliográfica permite conocer diferentes metodologías y métodos usados en los temas de investigación, en donde podemos conocer limitaciones y fortalezas de diversas técnicas existentes en los artículos revisados, siendo una herramienta esencial para la sinterización de información, permitiendo nuevos conceptos de una ciencia que puede ser utilizada para la comunidad científica u otros conceptos. (Barquero Morales, 2022)

En este articulo la metodología que vamos a emplear fue el método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) conecta con la metodología de revisión sistemática con la revisión de la literatura, ofrece un método riguroso y estructurado para sintetizar y analizar los datos disponibles de manera minuciosa y objetiva.(Cumpston et al., 2019)

La organización y tabulación de los resultados se la realizará mediante el uso del método PRISMA, lo que permite una evaluación critica de la calidad metodológica y la aplicabilidad de cada estudio. Se realiza una búsqueda exhaustiva en bases de datos científicas y se seleccionan los estudios que cumplen estos criterios mediante el método PRISMA.(Urrútia & Bonfill, 2010).

Con el método PRISMA, la extracción y análisis de datos de los estudios seleccionados forma parte del proceso de revisión bibliográfica. Este paso permite una evaluación critica de la calidad metodológica y la aplicabilidad de cada estudio. De manera similar a una revisión sistemática convencional, la metodología PRISMA pone un fuerte énfasis en la transparencia en cada etapa del procedimiento para garantizar que se minimicen los sesgos y que las decisiones tomadas durante la revisión se documenten adecuadamente.(Agustín Ciapponi, 2020)

3.1 Materiales y métodos

Para la selección de documentos que presentan información de accesos no autorizados en redes SDN, herramientas, procedimientos y controladores se tomaron 30 artículos mediante la realización de búsqueda exhaustiva de fuentes bibliográficas en las bases de datos determinando a las preguntas de forma clara y precisa que los estudios puedan responder a las consultas planteadas.(Sobrido Prieto & Rumbo-Prieto, 2018)

Para asegurar la inclusión de estudios pertinentes y relevantes, el proceso de búsqueda y selección de literatura realizamos una búsqueda exhaustiva de varias bases de datos científicas Scopus, WoS (Web of Science), Google Scholar, IEEE, Springer Link. Estas bases de datos

fueron seleccionadas por su cobertura y calidad científica en el medio. Se utilizaron términos de búsqueda específicos relacionados con nuestro tema. En su mayoría, los artículos cumplen con el criterio de fecha de publicación limite dentro del rango de los último cinco años para ser tomados en cuenta (2018 A 2023)

4. Resultados

4.1 Selección de los Estudios

Se filtro la búsqueda es las siguientes bases de datos científicas como Scopus, WoS (Web of Science), Google Scholar, IEEE, Springer Link. Realizaremos la revisión sistemática usando método PRISMA que nos dará la pauta para llevar a cabo cada paso de la revisión sistemática, desde la formulación de la pregunta de investigación hasta la presentación de los hallazgos, de manera estructurada y detallada. La búsqueda se basó en los siguientes criterios (CyberSecurity OR Security) AND (Security Models OR Architecture) AND (Access Control OR Unauthorized Access)

Las bases de datos utilizadas para la búsqueda inicial arrojaron un total de 23.351 resultados. Los documentos de IEEE, Google Scholar, Springer Link, Scopus y WoS se evaluarán de acuerdo con nuestros estándares tanto de inclusión como de exclusión. Primero, se eliminan resúmenes, libros, reseñas y otros documentos que no sean artículos científicos. Luego se eliminan los artículos duplicados, no elegible y otros entre las bases de datos que nos deja un total de 22.887 artículos, luego examinamos los títulos y resúmenes de los artículos restantes.

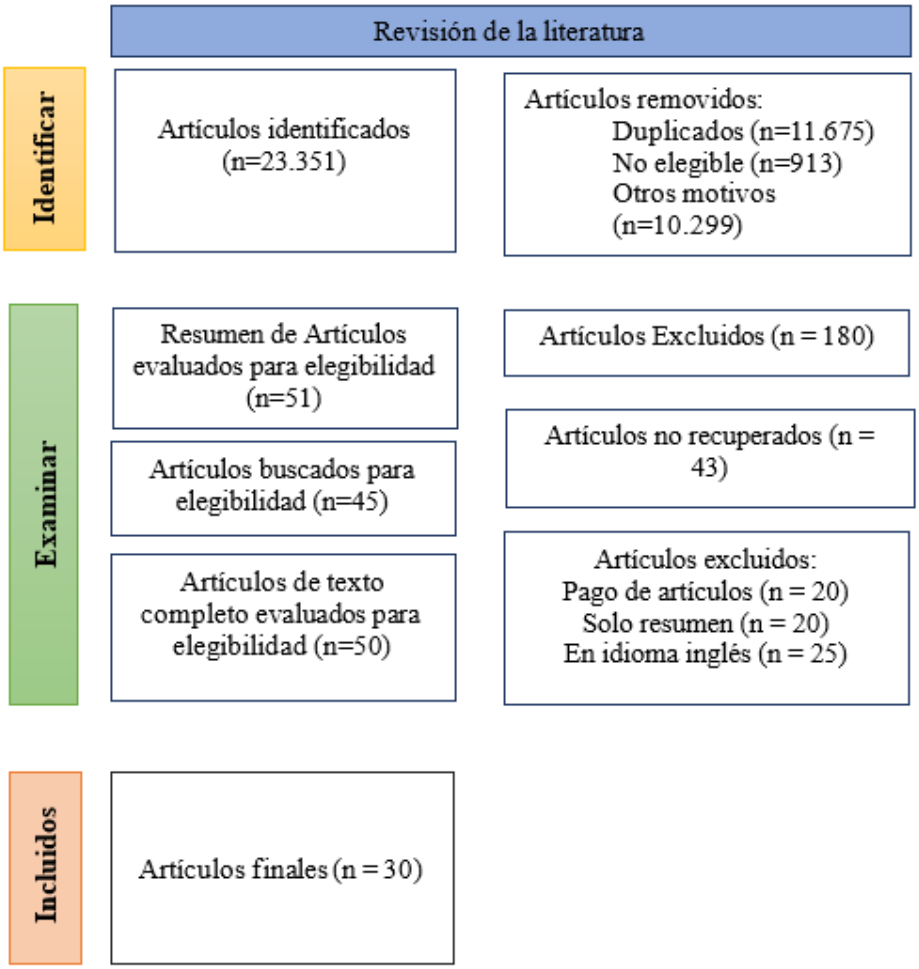


Figura 4. Revisión de la Literatura en PRISMA

4.2 Análisis y verificación de los resultados de la investigación

Tabla 2. Resumen de las Propuestas científicas con relación a la problemática.

Literatura verificada	Temática						Modelo	
	SDN	Security	Access Control	OpenFlow	Attack detection DDoS	Otros	Teórico	Práctico
Challenges and solutions in Software Defined Networking: A survey.(Saraswat et al., 2019b)	X	X	X			X	X	X
Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions.(Singh & Behal, 2020)	X	X	X		X	X	X	
Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions.(Valdovinos et al., 2021)	X	X	X	X	X		X	
A survey on Dos/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. (Alhijawi et al., 2022)	X	X	X		X		X	X
Hybrid SDN evolution: A comprehensive survey of the state-of-the-art. (Khorsandroo et al., 2021)	X	X	X			X	X	X
A comprehensive study of DDoS attacks over IoT network and their countermeasures.(Kumari & Jain, 2023)	X	X	X		X	X	X	
Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. (Golightly et al., 2023)	X	X	X			X	X	
DACAS: integration of attribute-based access control for northbound interface security in SDN. (Liu et al., 2023)	X	X	X			X	X	X
Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges(Sultana et al., 2021)	X	X				X		X

a) ¿Cuál es el estado actual de la seguridad y control de acceso en la arquitectura para mitigar un acceso no autorizado?

La gestión de acceso dentro de la estructura SDN abarca la habilidad de permitir o restringir la entrada a los recursos de la red conforme a las políticas predefinidas.(Palacio Rafael David & Puello Beltrán Juan José, 2020a) La seguridad en SDN conlleva salvaguardar tanto la infraestructura de la red como los datos de posibles peligros y acceso en la arquitectura SDN se puede sintetizar en los siguientes aspectos fundamentales:

- **Autenticación y autorización:** En SDN se han propuesto varios mecanismos de autenticación y autorización en SDN para garantizar que sólo los usuarios autorizados tengan acceso a los recursos de la red.(López G. Alexander et al., 2021) Algunos ejemplos son el uso de certificados digitales, la autenticación basada en roles y los controles de acceso granular.
- **Seguridad de la comunicación:** Para evitar los ataques de intercepción y la manipulación de datos, los componentes de la arquitectura SDN deben poder comunicarse de forma segura. Para garantizar la confidencialidad e integridad de las comunicaciones, se han propuesto protocolos de seguridad como TLS (Transport Layer Security) y SSH (Secure Shell).
- **Detección y prevención de intrusiones:** Estas dos características de seguridad de SDN son esenciales. Para identificar y mitigar amenazas potenciales, se han desarrollado firmas de ataque específicas y métodos de detección de anomalías. Para restringir o bloquear aún más el acceso de los atacantes, se han propuesto mecanismos de respuesta automática.
- **Seguridad de la capa de control:** dado que la capa de control en SDN gobierna la configuración y el comportamiento de la red, se convierte en un objetivo atractivo para los atacantes. La segmentación de la red, la autenticación del controlador y la detección de ataques de inundación son algunas de las medidas de seguridad que se han propuesto para proteger la capa del controlador.
- **Gestión de políticas de seguridad**: en SDN, la gestión de políticas de seguridad se ocupa de crear y hacer cumplir políticas de seguridad y acceso en toda la red. Para permitir la gestión centralizada de políticas, garantizar la coherencia de las políticas y hacerlas cumplir las políticas en toda la infraestructura, se han propuesto marcos y herramientas.

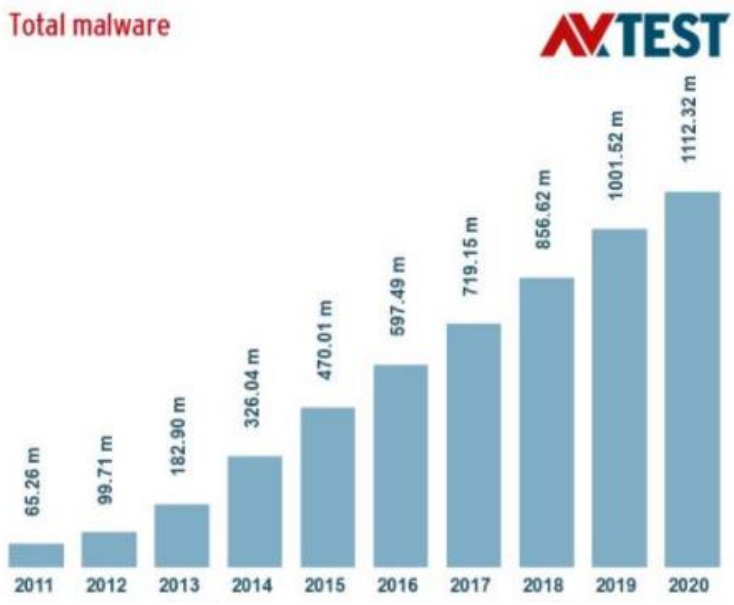


Figura 5. Malware total detectado de estos últimos 10 años (Ruipérez et al., 2021a)

El estado actual de los modelos de control de acceso y seguridad de la arquitectura SDN demuestra avances significativos en la detección de acceso no autorizado y la protección de la red ya que poseen de una seguridad robusta a su vez con dispositivos confiables.(Scott-Hayward et al., 2016)

Tabla 3. Enfoques y Estrategias de seguridad en SDN para accesos no autorizados.

Enfoques y Estrategias de seguridad en SDN	
Diversidad de Enfoques	Refleja la adaptación a diferentes escenarios y niveles de amenaza.
Integración de Tecnologías Avanzadas	Integración de tecnologías avanzadas, para mejorar la detección temprana de accesos no autorizados y así dar respuestas automatizadas y eficaces.
Automatización y Orquestación	Lleva a cabo políticas de seguridad de manera más ágil en toda la infraestructura. Así puede agilizar las respuestas de las amenazas y minimiza la exposición.
Prevención y Detención	Desarrollando modelos proactivos que anticipan posibles amenazas y reaccionan antes de que se materialicen.
Colaboración e Investigación	Comparten mejoras de prácticas, descubrimiento y soluciones a través de investigaciones, conferencias y publicaciones.

b) ¿Existen modelos de seguridad para identificar posibles amenazas de acceso no autorizado en las redes SDN y que limitaciones tienen?

Dado en los 30 artículos revisados en donde se muestran una serie de dificultades y limitaciones con la aplicación de modelos de seguridad y control de acceso en la arquitectura SDN para la detección de acceso no autorizado, lo que exige una cuidadosa consideración y soluciones creativas.

Las amenazas de acceso no autorizado se pueden encontrar en las redes definidas por software (SDN) gracias a los modelos y técnicas de seguridad. Estos modelos tienen como objetivo detectar actividad de red sospechosa o anormal y tomar medidas para detener o disminuir el acceso no autorizado.

- **Detección de anomalías:** La base de este método es la observación continua de la actividad de la red y el comportamiento del usuario. Las desviaciones de tráfico significativas se detectan mediante algoritmos de detección de anomalías, que también envían alertas en caso de que ocurra algo sospechoso.
  (Anet Fernández Bezanilla et al., 2018) Este trabajo propone un conjunto mínimo de controles de seguridad que deben ser implementados en nubes privadas y centros de datos virtualizados. Si bien no se enfoca específicamente en SDN, algunos de los controles propuestos, como la autenticación y la autorización, podrían ser aplicables a SDN. Una limitación de este modelo es que se enfoca en nubes privadas y centros de datos virtualizados, por lo que puede no ser directamente aplicable a otros entornos de red.

- **Modelos basados en el comportamiento:** Para usuarios y dispositivos en la red, se crean perfiles de comportamiento típicos. Cualquier desviación notable de estos perfiles podría ser una señal de acceso no autorizado.
  (Palacio Rafael David & Puello Beltrán Juan José, 2020)Este modelo utiliza técnicas de inteligencia artificial para detectar amenazas en una red de datos. Si bien no se enfoca específicamente en SDN, algunas de las técnicas de detección de amenazas, como la normalización y la clasificación basada en redes neuronales, podrían ser aplicables a SDN. Una limitación de este modelo es que se enfoca en la detección de amenazas, pero no proporciona soluciones específicas para mitigarlas.

- **Modelos basados en firmas:** Estos modelos, al igual que los programas antivirus tradicionales, utilizan firmas o patrones reconocidos de comportamiento malicioso para detectar amenazas en tiempo real. Se pueden analizar grandes conjuntos de datos utilizando técnicas de aprendizaje automático para encontrar patrones intrincados en el comportamiento humano y el flujo de tráfico. Se les puede enseñar a detectar amenazas nuevas o inusuales.
  (DANIELA TOAINGA URRUTIA et al., 2019) Si bien no se enfoca específicamente en SDN, algunas de las medidas de seguridad propuestas, como la identificación de vulnerabilidades y la aplicación de medidas de seguridad, podrían ser aplicables a SDN. Una limitación de este modelo es que se enfoca en redes de VoIP, por lo que puede no ser directamente aplicable a otros entornos de red.

- **Modelos basados en reglas:** Se establecen reglas específicas que especifican el comportamiento de red aceptable e inaceptable. Las amenazas pueden atribuirse a cualquier comportamiento que contravenga estas leyes.

(Carrión-Barco et al., 2021) Este modelo propone medidas de seguridad informática para garantizar el intercambio de información académica en un medio de conexión pública. Si bien no se enfoca específicamente en SDN, algunas de las medidas de seguridad propuestas, como la conexión segura y la autenticación, podrían ser aplicables a SDN. Una limitación de este modelo es que se enfoca en un medio de conexión pública específico, por lo que puede no ser directamente aplicable a otros entornos de red.

- **Monitoreo del Estado de los Dispositivos:** Para identificar cualquier actividad no autorizada o inusual, se observa el estado y comportamiento de los dispositivos conectados a la red.

A pesar de ser útiles, estos modelos de seguridad tienen los siguientes inconvenientes.

Tabla 4. Desafíos en los modelos de seguridad en SDN.

Inconvenientes de los Modelos de Seguridad en SDN	Descripción
Falsos positivos y falsos negativos	Los modelos tienen el potencial de generar alertas falsas (falsos positivos) o pasar por alto amenazas reales (falsos negativos), lo que puede afectar la efectividad de la detección.
Nuevas amenazas	Es posible que los modelos basados en patrones no puedan identificar amenazas que son completamente nuevas o no identificadas y que no se ajustan a ningún patrón existente.
Complejidad de la red SDN	Debido a la complejidad de las redes SDN, es un desafío desarrollar modelos de seguridad que tengan en cuenta todos los escenarios y configuraciones imaginables.
Sobrecarga asociada con el rendimiento	Algunos modelos introducen una sobrecarga asociada con el análisis de tráfico en curso, que puede tener un impacto en el rendimiento de la red.
Amenazas que cambian constantemente	Los modelos pueden tener dificultades para mantenerse al tanto de las nuevas amenazas y estrategias de ataque.

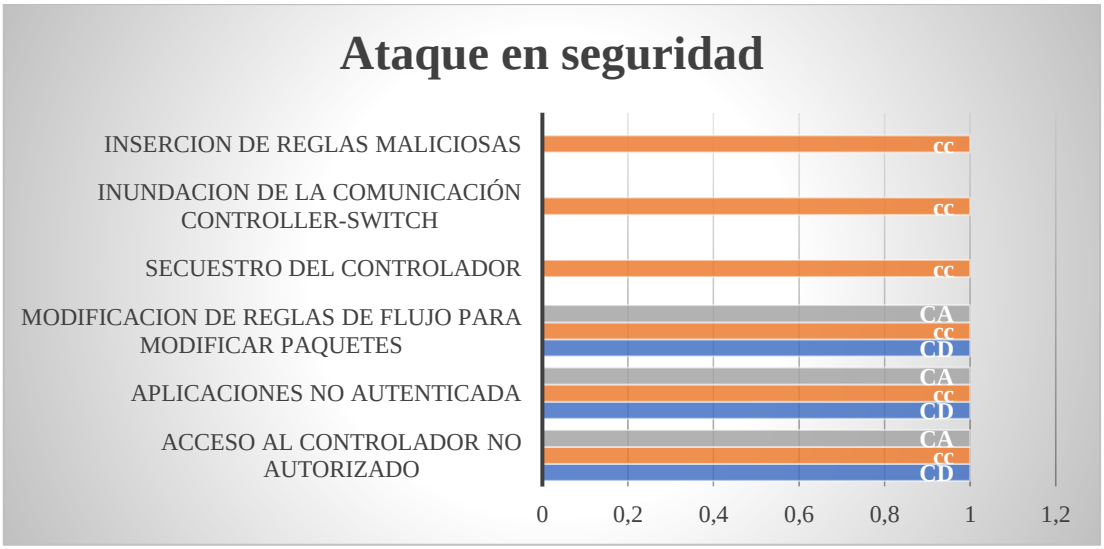


Figura 6. Ataques en seguridad

c) ¿Qué propuesta de mejora se pueden recomendar en la adaptación y aplicación de un modelo de seguridad que nos permita proponer técnicas y metodologías de detección temprana de acceso no autorizado en redes SDN?

Se pueden utilizar varias sugerencias y métodos de mejora para adaptar y aplicar un modelo de seguridad eficiente para la detección temprana de accesos no autorizados en redes SDN.

- **Integración de inteligencia artificial y aprendizaje automático:** Para mejorar las capacidades de detección, integre técnicas de inteligencia artificial y aprendizaje automático de vanguardia.(Vera, 2023) Para detectar nuevas amenazas de manera más precisa y adaptativa, los algoritmos de aprendizaje automático pueden reconocer patrones complejos de actividad y tráfico.

- **Considere el contexto:** En el que tienen lugar las actividades en lugar de simplemente analizar el comportamiento de los dispositivos individuales. Esto hace que sea más fácil distinguir entre el mal comportamiento y el comportamiento adecuado en diversas circunstancias.

- **Modelos de detección híbridos:** Combina varios modelos y métodos de detección para aumentar la precisión y disminuir los falsos positivos y negativos. Por ejemplo, podría combinar el análisis de comportamiento con la detección de anomalías para obtener una imagen más completa.

- **Actualización periódica de firmas y patrones:** Si utiliza modelos basados en firmas o patrones, asegúrese de mantenerlos actualizados para abordar nuevas amenazas y estrategias de ataque.

- **Integración de mecanismos de respuesta automatizados:** Como el bloqueo de tráfico o el aislamiento de dispositivos, que pueden actuar de forma inmediata frente a actividades sospechosas o maliciosas. La automatización puede reducir el tiempo de mitigación de un ataque en más del 50%(Toainga U. Daniela & Peña P. Daniel, 2019)

- **Monitoreo distribuido:** Use una estrategia de monitoreo distribuido en toda la red para recopilar datos de varios puntos y garantizar que ningún área quede desatendida.

- **Pruebas de penetración y validación:** Realice simulaciones de ataques y pruebas de penetración para medir la eficacia del modelo de seguridad. Esto facilita la detección de fallas y lagunas en el enfoque. Las pruebas de penetración han revelado vulnerabilidades no detectadas en más del 70% de los casos

- **Colaboración con la comunidad de investigación:** Para mantenerse actualizado sobre las amenazas de seguridad y los avances más recientes en las redes SDN, mantenga abiertas las líneas de comunicación con la comunidad de investigación y la industria. La colaboración con la comunidad de seguridad aumenta la detección temprana en un 30% en promedio

- **Consideración de la política de seguridad:** Garantizar que las políticas de seguridad y cumplimiento de la organización cumplan con el modelo de seguridad.

- **Establecer un proceso de auditoría y mejora continua:** Le permitirá evaluar la eficacia del modelo de seguridad y realizar las modificaciones necesarias. Los modelos que pasan por auditorías regulares mejoran su eficacia en más del 25% de seguridad.

- **Privacidad y cumplimiento normativo:** Asegúrese de que los métodos de monitoreo y detección cumplan con las leyes de privacidad y cumplimiento, como el RGPD. La no conformidad con regulaciones puede resultar en multas de hasta el 4% de los ingresos globales

- **Capacitación e Información:** Los usuarios y administradores reciben información sobre los riesgos del acceso no autorizado y las precauciones de seguridad. La formación en seguridad reduce los incidentes causados por errores humanos en un 45%

4.3 Controladores de Acceso en SDN para la detención de Accesos No Autorizados

- **Seguridad de Red:** Organizar la red en secciones lógicas para separar los flujos de tráfico y evitar que las amenazas se propaguen.(Farooq et al., 2023)
- **Control de Acceso Basado en Identidad:** Asegurar de que solo los usuarios autorizados puedan acceder a la red, use autenticación y autorización basadas en identidad.(Shubbar, Alhisnawi, Abdulhassan, & Ahmadi, 2021)

- **Análisis de Comportamiento:** Detectar patrones inusuales que pueden apuntar a un acceso no autorizado, vigilar el tráfico de la red y utilice el análisis de comportamiento.
- **Control de Flujo y Políticas de Acceso**: A través de la programación de tablas de flujo en hardware de red, SDN permite la implementación de políticas de acceso granular. Mediante el uso de criterios como una dirección IP, un puerto o un protocolo, los controladores pueden definir reglas que especifican como se debe manejar el tráfico.
- **Monitoreo Continuo y Respuesta Automatizada:** Los controladores SDN pueden implementar el monitoreo continuo de la red para identificar rápidamente los eventos de seguridad. Al redirigir o aislar automáticamente el tráfico malicioso si se descubre un acceso no autorizado, el controlador puede reducir la amenaza.(Gao & Xu, 2023)

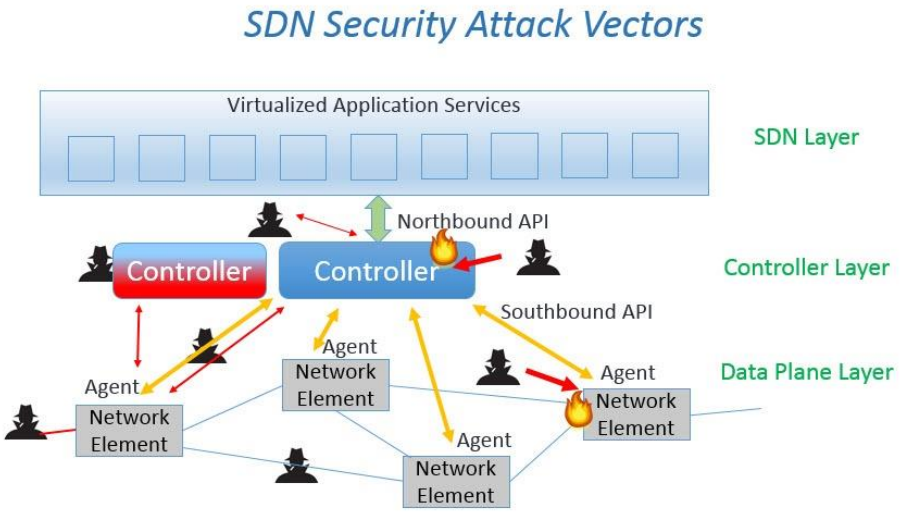


Figura 7. Arquitectura SDN y Atacantes.

De acuerdo con (Ruipérez et al., 2021b) el vector de ataque muestra cómo se puede hacer lanzamientos de ataques con las redes SDN, tomando en cuenta puntos de vulnerabilidad que tiene cada ataque teniendo como propósito una relación causa-efecto entre una fuente puntual de ataques y todos los componentes de una red SDN pueden ser los objetivos, siendo de utilidad para determinar niveles de daño como puede evidenciarse en la figura 7.

5. Discusión

En la actualidad las arquitecturas SDN ha evolucionado con el paso de los años y el paradigma de las redes definidas por software está contribuyendo a nuevos requerimientos de las redes, una arquitectura contando con un servidor en común puede ser utilizado para levantar la redundancia y disponibilidad dentro de una organización, en caso de existir un acceso sin autorización, la infraestructura virtualizada puede a ser gravemente vulnerada.

Por lo mencionando anteriormente, se vuelve importante identificar cualquier tipo de actividad no autorizada o inusual de manera preventiva para evitar que esto llegue a ocasionar un efecto mayor en la operación de las redes y para ello se incorporan métodos que tienen la capacidad de mejora de detección y aprendizaje de vanguardia. Por ello para poder identificar un comportamiento dentro de lo que aceptable, se estableces leyes o reglas que justifican un comportamiento adecuado para un acceso a la red, si bien es cierto no se enfoca completamente

a las redes SDN, muchas medidas como autenticación y conexión segura pueden ser aplicables a este modelo. Al hacer un enfoque de identificación de este tipo de amenazas se debe tomar en consideración que el tráfico en la red puede ser controlado con el aislamiento de dispositivos, actuando de manera inmediata sobre actividades sospechosas, garantizando equipos individuales cumplan con las políticas de seguridad y cumplimientos dentro de una organización.

Tomando en consideración que cada usuario cuenta con un perfil de comportamiento y asociado a un grupo de autorización de tareas, es más evidenciable una detección de anomalías permitiendo evaluar la eficacia de estos permisos, así nos aseguramos de recibir la información sobre los riegos e incidentes causados por errores humanos ya que estos comúnmente representan un 45% de los riesgos causados.

6. Conclusión

En cuanto a los expuesto a lo largo de este trabajo permite arribar, los temas críticos de seguridad y control de acceso en la arquitectura de SDN se han cubierto a fondo en este artículo, en donde se han investigado varios modelos y métodos para detectar y prevenir el acceso no autorizado en entornos SDN a través de un análisis sistemático.

El estudio ha destacado la importancia de implementar controles o medidas de seguridad solidas en las redes modernas, donde la flexibilidad y la eficiencia de SDN pueden ir de la mano con un posible aumento potencial de la vulnerabilidad. Así mismo, en esta investigación se enfatiza realizar previamente un análisis de los riesgos y nuevas amenazas para poder asegurar que las políticas e integridad de los datos en la red.

7. Referencias bibliográficas

Agustin Ciapponi. (2020). *La declaración PRISMA 2020: una guía actualizada para reportar revisiones sistemáticas*. http://www.prisma-state

Ahmed, M., Naser Mahmood, A., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications*, *60*, 19–31. https://doi.org/10.1016/J.JNCA.2015.11.016

Alenezi, M., Almustafa, K., & Meerja, K. A. (2019). Cloud based SDN and NFV architectures for IoT infrastructure. *Egyptian Informatics Journal*, *20*(1), 1–10. https://doi.org/10.1016/J.EIJ.2018.03.004

Alhijawi, B., Almajali, S., Elgala, H., Bany Salameh, H., & Ayyash, M. (2022). A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. *Computers and Electrical Engineering*, *99*, 107706. https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.107706

Alsaeedi, M., Mohamad, M. M., & Al-Roubaiey, A. A. (2019). Toward Adaptive and Scalable OpenFlow-SDN Flow Control: A Survey. *IEEE Access*, *7*, 107346–107379. https://doi.org/10.1109/ACCESS.2019.2932422

Al-Shaboti, M., Welch, I., Chen, A., & Mahmood, M. A. (2018). Towards Secure Smart Home IoT: Manufacturer and User Network Access Control Framework. *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, 892–899. https://doi.org/10.1109/AINA.2018.00131

Anet Fernández Bezanilla, I., Lilia García Perellada, M. R., Alain Garófalo Hernández, D. A., La Habana José Antonio Echeverría, de, Rotonda, C., & Habana, L. (2018). PROPUESTA DE CONTROLES DE SEGURIDAD PARA NUBES PRIVADAS Y CENTROS DE DATOS VIRTUALIZADOS. *Revista Telemática*, *17*(1), 56–72. http://revistatelematica.cujae.edu.cu/index.php/tele

Ángel Segovia Fernández. (2020). *Detección de vulnerabilidades y control de congestión a través de redes definidas por software (SDN)*.

Bannour, F., Souihi, S., & Mellouk, A. (2020). Adaptive distributed SDN controllers: Application to Content-Centric Delivery Networks. *Future Generation Computer Systems*, *113*, 78–93. https://doi.org/10.1016/J.FUTURE.2020.05.032

Barquero Morales, W. G. (2022). ANALISIS DE PRISMA COMO METODOLOGÍA PARA REVISIÓN SISTEMÁTICA: UNA APROXIMACIÓN GENERAL. *Saúde Em Redes*, *8*(sup1), 339–360. https://doi.org/10.18310/2446-4813.2022v8nsup1p339-360

Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). Software-defined networking (SDN): a survey. *Security and Communication Networks*, *9*(18), 5803–5833.

Carrión-Barco, G., Sánchez-Chero, M.-J., Del, C. I., Castro, C., William, F., Flores, C., & Timaná Alvarez, M. (2021). Modelo de seguridad informática para un medio de conexión pública. *Año*, *12*. https://doi.org/10.46925//rdluz

Ciena. (2023). *What is SDN?* Https://Www.Ciena.Com/Insights/What-Is/What-Is-SDN.Html.

Correa Chica, J. C., Imbachi, J. C., & Botero Vega, J. F. (2020). Security in SDN: A comprehensive survey. *Journal of Network and Computer Applications*, *159*, 102595. https://doi.org/10.1016/J.JNCA.2020.102595

Cumpston, M., Li, T., Page, M. J., Chandler, J., Welch, V. A., Higgins, J. P., & Thomas, J. (2019). Updated guidance for trusted systematic reviews: a new edition of the Cochrane Handbook for Systematic Reviews of Interventions. In *The Cochrane database of systematic reviews* (Vol. 10, p. ED000142). NLM (Medline). https://doi.org/10.1002/14651858.ED000142

DANIELA TOAINGA URRUTIA, DANIEL PEÑA PÉREZ, De Ingeniería En, E., Telecomunicaciones, E., Redes, Y., & Por, D. (2019). *"ANÁLISIS DE VULNERABILIDADES INSIDER CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (DoS) EN REDES."*

Toainga U. Daniela, & Peña P. Daniel. (2019). *"ANÁLISIS DE VULNERABILIDADES INSIDER CONTRA ATAQUES DE DENEGACIÓN DE SERVICIO (DoS) EN REDES*.

Diana Carolina Alvarez Paredes. (2019). *FRAMEWORK DE DETECCIÓN Y DIAGNÓSTICO AUTOMÁTICO DE ANOMALÍAS PARA REDES MÓVILES UTILIZANDO KPIS DE TRANSMISIÓN*.

Distrital Francisco Jose de Caldas, U., Eduardo Cáceres Guevara, J., & Alexis Casilimas Fajardo, C. (2022). *Arquitectura y funcionamiento de redes definidas por software (SDN)*.

Eom, T., Hong, J. B., Park, J. S., & Kim, D. S. (2015). Security Modeling and Analysis of a SDN Based Web Service. In G. Wang, A. Zomaya, G. Martinez, & K. Li (Eds.), *Algorithms and Architectures for Parallel Processing* (pp. 746–756). Springer International Publishing.

ETSI. (2023, March 12). *Network Functions Virtualisation (NFV)*. Https://Www.Etsi.Org/Technologies/Nfv.

Farooq, M. S., Riaz, S., & Alvi, A. (2023). Security and Privacy Issues in Software-Defined Networking (SDN): A Systematic Literature Review. In *Electronics (Switzerland)* (Vol. 12, Issue 14). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics12143077

Gao, Y., & Xu, M. (2023). *Defense Against Software-Defined Network Topology Poisoning Attacks* (Vol. 28, Issue 1).

Golightly, L., Modesti, P., Garcia, R., & Chang, V. (2023). Securing distributed systems: A survey on access control techniques for cloud, blockchain, IoT and SDN. *Cyber Security and Applications*, *1*, 100015. https://doi.org/10.1016/J.CSA.2023.100015

Goransson, P., Black, C., & Culver, T. (2016). *Software defined networks: a comprehensive approach*. Morgan Kaufmann.

Guan, Y., Lei, W., Zhang, W., Liu, S., & Li, H. (2018). Scalable orchestration of software defined service overlay network for multipath transmission. *Computer Networks*, *137*, 132–146. https://doi.org/10.1016/J.COMNET.2018.03.005

Hasan, T., Akhunzada, A., Giannetsos, T., & Malik, J. (2020). Orchestrating SDN Control Plane towards Enhanced IoT Security. *2020 6th IEEE Conference on Network Softwarization (NetSoft)*, 457–464. https://doi.org/10.1109/NetSoft48620.2020.9165424

Hrsg, V. (2022). *Kommunikation und Bildverarbeitung in der Automation Technologien für die intelligente Automation Technologies for Intelligent Automation*.

Ing Norma Beatriz Perez, M., Alfredo Bustos, M., Berón, M. M., & Rangel Henriques, P. (2018). *ANÁLISIS SISTEMÁTICO DE LA SEGURIDAD EN INTERNET OF THINGS*.

Khorsandroo, S., Sánchez, A. G., Tosun, A. S., Arco, J. M., & Doriguzzi-Corin, R. (2021). Hybrid SDN evolution: A comprehensive survey of the state-of-the-art. *Computer Networks*, *192*. https://doi.org/10.1016/j.comnet.2021.107981

Krishnan, P., Jain, K., Aldweesh, A., Prabu, P., & Buyya, R. (2023). OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. *Journal of Cloud Computing*, *12*(1). https://doi.org/10.1186/s13677-023-00406-w

Kumari, P., & Jain, A. K. (2023). A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Computers & Security*, *127*, 103096. https://doi.org/10.1016/J.COSE.2023.103096

Leandro, C., & Mejia, V. (2018a). *ANÁLISIS DE SEGURIDAD EN REDES SDN (REDES DEFINIDAS POR SOFTWARE)*.

Leandro, C., & Mejia, V. (2018b). *ANÁLISIS DE SEGURIDAD EN REDES SDN (REDES DEFINIDAS POR SOFTWARE)*.

Liu, Y., Zhao, B., An, Y., & Guo, J. (2023). DACAS: integration of attribute-based access control for northbound interface security in SDN. *World Wide Web*, *26*(4), 2143–2173. https://doi.org/10.1007/s11280-022-01130-2

López G. Alexander, González B. Henry, & Gainza Dainys. (2021). *PropuestaDeMetodologiaParaElAnalisisDeSeguridadEn...*

Mijumbi, R., Serrat, J., Gorricho, J.-L., Bouten, N., De Turck, F., & Boutaba, R. (2016). Network Function Virtualization: State-of-the-Art and Research Challenges. *IEEE Communications Surveys & Tutorials*, *18*(1), 236–262. https://doi.org/10.1109/COMST.2015.2477041

Palacio Rafael David, A., & Puello Beltran Juan José, A. (2020a). *ESTUDIO DE LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS AL PROTOCOLO DHCP EN UNA RED DE COMPUTADORAS MEDIANTE TÉCNICAS DE INTELIGENCIA ARTIFICIAL*.

Palacio Rafael David, A., & Puello Beltran Juan José, A. (2020b). *ESTUDIO DE LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIOS AL PROTOCOLO DHCP EN UNA RED DE COMPUTADORAS MEDIANTE TÉCNICAS DE INTELIGENCIA ARTIFICIAL*.

Roberto, J., & Sandoval, S. (2020). *Artículos científicos T La gestión en redes definidas por software (SDN) desde la perspectiva de FCAPS* (Vol. 23).

Ruipérez, J., Tutor, C., Óscar, J., & Martínez, R. (2021a). *Seguridad en Redes definidas por software (SDN)*. www.etsit.upv.es

Ruipérez, J., Tutor, C., Óscar, J., & Martínez, R. (2021b). *Seguridad en Redes definidas por software (SDN)*. www.etsit.upv.es

Saraswat, S., Agarwal, V., Gupta, H., Mishra, R., Gupta, A., & Dutta, T. (2019a). Challenges and Solutions in Software Defined Networking: A Survey. *Journal of Network and Computer Applications*, *141*. https://doi.org/10.1016/j.jnca.2019.04.020

Saraswat, S., Agarwal, V., Gupta, H. P., Mishra, R., Gupta, A., & Dutta, T. (2019b). Challenges and solutions in Software Defined Networking: A survey. *Journal of Network and Computer Applications*, *141*, 23–58. https://doi.org/10.1016/J.JNCA.2019.04.020

Scott-Hayward, S., Natarajan, S., & Sezer, S. (2015). A survey of security in software defined networks. *IEEE Communications Surveys & Tutorials*, *18*(1), 623–654.

Scott-Hayward, S., Natarajan, S., & Sezer, S. (2016). A survey of security in software defined networks. In *IEEE Communications Surveys and Tutorials* (Vol. 18, Issue 1, pp. 623–654). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/COMST.2015.2453114

Shubbar, R., Alhisnawi, M., Abdulhassan, A., & Ahamdi, M. (2021). A Comprehensive Survey on Software-Defined Network Controllers. *Lecture Notes in Networks and Systems*, *201*, 199–231. https://doi.org/10.1007/978-981-16-0666-3_18

Shubbar, R., Alhisnawi, M., Abdulhassan, A., & Ahmadi, M. (2021). *A Comprehensive Survey on Software-Defined Network Controllers* (pp. 199–231). https://doi.org/10.1007/978-981-16-0666-3_18

Singh, J., & Behal, S. (2020). Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. *Computer Science Review*, *37*, 100279. https://doi.org/https://doi.org/10.1016/j.cosrev.2020.100279

Sobrido Prieto, M., & Rumbo-Prieto, J. M. (2018). La revisión sistemática: pluralidad de enfoques y metodologías. *Enfermería Clínica*, *28*(6), 387–393. https://doi.org/10.1016/J.ENFCLI.2018.08.008

Stallings, W. (2016). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.

Sultana, R., Grover, J., & Tripathi, M. (2021). Security of SDN-based vehicular ad hoc networks: State-of-the-art and challenges. *Vehicular Communications*, *27*, 100284. https://doi.org/10.1016/J.VEHCOM.2020.100284

TechTarget. (2023, July 24). *software-defined networking (SDN)*. Www.Techtarget.Com/Searchnetworking/Definition/Software-Defined-Networking-SDN.

Urrútia, G., & Bonfill, X. (2010). PRISMA declaration: A proposal to improve the publication of systematic reviews and meta-analyses. *Medicina Clinica*, *135*(11), 507–511. https://doi.org/10.1016/j.medcli.2010.01.015

Valdovinos, I. A., Pérez-Díaz, J. A., Choo, K.-K. R., & Botero, J. F. (2021). Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. *Journal of Network and Computer Applications*, *187*, 103093. https://doi.org/https://doi.org/10.1016/j.jnca.2021.103093

Vera, F. (2023). *Integración de la Inteligencia Artificial en la Educación superior: Desafíos y oportunidades*. https://orcid.org/0000-0002-4326-1660

Yassine, M., Youssef, Q., EL GHOLAMI, K., Sadqi, Y., & Mounir, S. (2022). A comprehensive survey on SDN security: threats, mitigations, and future directions. *Journal of Reliable Intelligent Environments*, *9*. https://doi.org/10.1007/s40860-022-00171-8