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

Ariza Palacio Rafael David*
Asesor Puello Beltran Juan José
Universidad Del Sinú Elías Bechará Zainúm Seccional Cartagena
Escuela De Ingeniería De Sistemas
Cartagena-Colombia, 2020.

RESUMEN

El presente trabajo presenta una revisión sistemática de la literatura sobre la detección y prevención de ataques de denegación de servicios al protocolo DHCP en una red de computadoras mediante técnicas de inteligencia artificial. Para esto se toma como referencia 50 artículos y proyectos de los cuales por medio de los requisitos para seleccionar se tomaron 30 relacionados a la temática a los cuales se les realizo la revisión literaria que sirvió para la producción del artículo de revisión sistemática. Los trabajos fueron seleccionados y clasificados por año de publicación, fuente y país de producción. Posteriormente se construyó un estado del arte que describe los resultados de obtenidos al implementar prototipos relacionados con la temática en cada una de las investigaciones.

Los hallazgos de este documento contribuyen la comprensión de algunas debilidades de los sistemas informáticos y lo sencillo que es en ocasiones violar una de esas vulnerabilidades, logrando que cualquier usuario, el cual no requiere un mínimo conocimiento en la materia, pueda acercarse y entender la temática y dar cuenta la importancia de la detección, prevención y mitigación de ataques denegación de servicios al protocolo DHCP en una red de computadoras.

Palabras clave: DHCP, seguridad, inteligencia artificial, DDoS, machine learning, mitigación, vulnerabilidad.

ABSTRACT

The present work presents a systematic review of the literature on the detection and prevention of denial of service attacks to the DHCP protocol in a computer network using artificial intelligence techniques. For this, 50 articles and projects are taken as a reference, of which, through the requirements to select, 30 related to the topic were taken, to which the literary review was carried out, which was used to produce the systematic review article. The works were selected and classified by year of publication, source and country of production. Later, a state of the art was built that describes the results obtained by implementing prototypes related to the theme in each of the investigations.

The findings of this document contribute to understanding some weaknesses of computer systems and how easy it is sometimes to violate one of these vulnerabilities, making it possible

for any user, who does not require a minimum knowledge in the matter, to approach and understand the subject. and realize the importance of detection, prevention and mitigation of denial of service attacks to the DHCP protocol in a computer network.

Key words: DHCP, security, artificial intelligence, DDoS, machine learning, mitigation,

vulnerability.

INTRODUCCIÓN

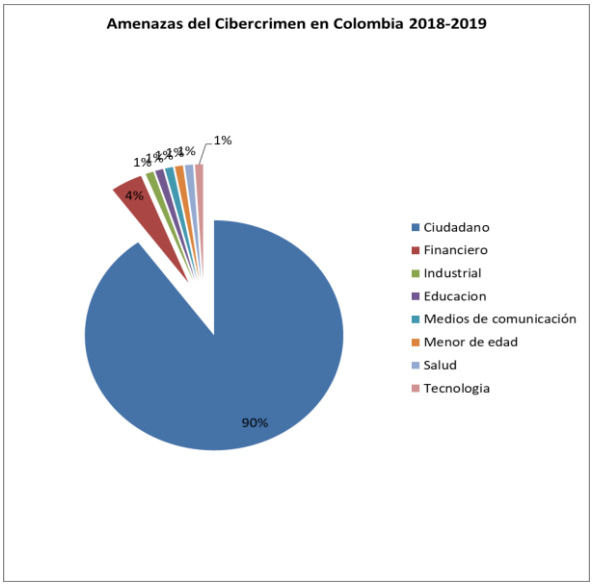
En un mundo cada vez más globalizado e interconectados, en el que las relaciones, negocios, interacciones e intercambios de información precisan de la eliminación, obstáculos impuestos por la distancia física, es fundamental la presencia de sistemas de comunicación eficientes en el transporte y difusión de la información, lo cual la seguridad está relacionada con la protección de los activos frente a amenazas y los riegos de ataque a una red de datos en cualquier organización son latentes, es decir, las amenazas pueden afectar al funcionamiento, operación, integridad o disponibilidad de una red o sistema. El avance de los medios tecnológicos y de comunicación ha provocado que el surgimiento de nuevos vectores de ataques mediante la red, cada día se descubran puntos débiles que comprometen los datos informáticos, existe la importancia de medir la seguridad y como se puede abordar el grave problema que hay detrás de vulnerabilidades que permitan a un atacante.

La seguridad es algo fundamental en el correcto movimiento de las redes de datos, pues con ella se garantiza la confiabilidad, la seguridad, y la correlación de datos sobre un mismo medio, sin mencionar otros. Una violación a dicha seguridad puede ocasionar severos daños a la integridad de las redes de datos, las cuales son de vital importancia en cualquier organización y pueden llegar a afectar datos relevantes para usuarios que hagan uso de diferentes sistemas de información.

Ahora bien, la conexión de dispositivos y la aparición de nuevas tecnologías como el internet de las cosas (IOT), hacen que las redes y dispositivos que en ella participan se conviertan en objetivos potencialmente vulnerables. Gracias a ese crecimiento tecnológico también crece la ciberdelincuencia, por lo que cada día se lucha en contrarrestar eso mecanismos que hoy día utilizan los llamados cibercriminales, con intereses diversos, ya que algunos lo hacen por dinero y otros por diversión. Red de cómputos, los cuales se transfieren la información a través de la red. Por tal motivo dichas empresas deben salvaguardar su sistema de información teniendo una gestión de seguridad informática para no estar expuestos a hacker (1).

Esta dinámica de los ciberdelincuentes ya es parte de la realidad de los usuarios en los últimos 3 años la policía ha detectado 15.565 incidentes informáticos (2), dentro de los ataques más frecuentes en Colombia observándose en la Ilustración 1.Incidentes Cibernético, se encuentra:

Ilustración 1.Incidentes Cibernético



Fuente: Amenazas del Cibercriminal en Colombia 2018-2019 (3).

Estos ataques no solo afectan al usuario, también afecta a un sistema financiero que cuesta alrededor de US 575.00 millones al año, representando a nivel global un 0.5%, solo en América Latina y del caribe cuesta alrededor de US 90.000 millones al año con el costo de 16% total de los delitos del mundo (1).

Por lo anterior, surge el siguiente interrogante; ¿Cómo se aplica la Inteligencia Artificial (IA) en la prevención y detección de ataques al protocolo DHCP?

La IA se ha organizado en varios campos de trabajo: como el pensamiento, conocimiento, aprendizaje, reconocimiento de lenguaje, la posibilidad de efectuar acciones, entre otras. El uso de la IA en la seguridad informática, enfatizado en los Sistemas Detectores de Intrusos, mediante el ataque de denegación de servicios al protocolo DHCP. A la hora de querer prevenir y detectar los ataques por denegación de servicios se encuentran diferentes métodos para ello, los cuales implican Inteligencia Artificial o AI, esta implementación ha ayudado y mejorado mucho la seguridad por medio del Machine learning ya que este crea una línea base de las actividades básicas y normales de la red, cuando hay un ataque el comportamiento de la red cambia notablemente, por lo tanto el Machine learning notará este cambio y se notificará como un posible ataque o una posible invasión a la red. Debido a esto se formula un objetivo general en el cual se busca construir un artículo de revisión sistemática sobre el aporte de la inteligencia artificial a la detección de ataque al protocolo DHCP.

Es por esto que se hace pertinente el estudio de la inteligencia artificial como herramienta para la prevención y detección de ataques al protocolo DHCP, lo que ayuda a la comprensión general de la temática y al desarrollo de estrategias y herramientas que permita gestionar la seguridad de la información dando aviso al administrador de sistema que está siendo atacado en la red mediante un correo electrónico.

En concordancia con lo anterior y en busca tener la mayor precaución posible que nos permita mantener una red funcional de manera constante; a sabiendas de que uno de los ataques más comunes y conocidos es el de denegación de servicio (DDoS), se desarrollar una revisión sistemática de las investigaciones y/o proyectos relacionados a la inteligencia artificial para prevención y detección de ataques al protocolo DHCP, por lo que el presente artículo se divide en tres fases fundamentales.

En primera instancia se ejecuta la recopilación de treinta referencias que funcionaran como fuente de información, seguidos de un estudio de contenido que posteriormente serviría como base para la construcción de un estado del arte. Por último, se establecen los hallazgos de la investigación y se enumeran las conclusiones.

MARCO TEÓRICO

En la actualidad toda empresa se basa en la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos. A continuación, se presenta los conceptos asociados a la seguridad informática y los usos de inteligencia artificial en la prevención de ataques:

Seguridad en sistemas informáticos y redes de comunicación

Las redes han tenido grandes cambios en los últimos años, lo que incrementa su uso y expone a los usuarios a ataques cibernéticos generando pérdidas a las organizaciones, es por tal que se debe priorizar la integridad de estos usuarios, su disponibilidad y la confiabilidad de poder dar sus datos personales. Este proceso es necesario poder acceder los sistemas informáticos que ayuda a organizar las tareas dentro de un sistema de información (4).

Se entiende por seguridad informática al conjunto de reglas y normas diseñadas para garantizar la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica abarcando hardware y software.

Ataques informáticos

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización. Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques. (5)

Vulnerabilidad y ataques

Hoy en día gran parte de la información del ser humano está procesado mediante los sistemas de red de informática computo, convirtiéndose en una operación esencial para mantenerse protegida generando confiabilidad, integridad y disponibilidad. Según la FBI los virus informáticos siguen siendo una de las mayores pérdidas financiera dentro del a empresa con una representación del 74% causando aseso no autorizado dentro del sistema. (6).

- **Ataques pasivos**: Son ataques sin permisos a la red para obtener más información del usuario mediante un mensaje, en este se modifica los mensajes de entrega o se retarde.

Ilustración 2.Ataques pasivos
Fuentes: Ana Mesa, Seguridad informática (7).

- **Ataques activos**: en este se analiza el tráfico y se libera los contenidos del mensaje produciendo cambios en la información dentro del mismo sistema.
- **Ataques Distribuidos:** son los ataques por degeneración de servicio (DDoS) presentado en la web.

Ilustración 3.Ataques DDoS
Fuentes: Ana Mesa, Seguridad informática (7).

Este tipo de ataques tiene como objetivo principal imposibilitar el uso dentro una red de sistema mediante una aplicación o un canal que se tramitan, este servidor web permite simultáneamente desconectar de la red.
DoS (Denial of Servicel) o DDoS (Destributed Denial of Service) sus ataques se dan por las IP que generan a una capacidad de respuesta de rechazo en el servicio.
Según Alejandro afirma que “Los ataques de denegación de servicio son un tipo de ataque informático a través del cual se reduce o anula la capacidad de servidores o recursos informáticos de ofrecer servicio” (8), es decir, los ataques se presentan en una fecha específica con la IP de las víctimas.

Tipos de atacantes

Existen dos tipos de atacantes en las redes que son:

- Insiders: se considera el personal que puede alterar los archivos interno de la compañía.

- Outsider: son el personal externo los cuales obtiene todos los usuarios y las claves por medio de programas en las cuales permite su fácil acceso a las compañías.

Entre estos métodos se encuentras:

Hacker *: "La palabra hacker deriva del vocablo inglés "hack" (cortar, golpear), el cual comenzó a adquirir su primera connotación tecnológica a principios del siglo XX, cuando pasó a formar parte de la jerga de los técnicos telefónicos de los EU, quienes en ocasiones lograban arreglar de inmediato las cajas defectuosas mediante un golpe seco, un hack"* (9).

Detector de intruso

Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles. (10)

Máquinas de soporte vectorial:

Es el soporte para dar soluciones a los problemas binario para desarrollo de multiclase (11).
Tiene como objetivo crear hiperplano para limita las redes neuronales, ayudando a las correcta decisión de las posibles clases como por ejemplo la Ilustración 4.Detencion de análisis cardiacas como aprendizaje como lo muestra la en esta muestra la función denominada Kernel , el cual emplear las máquinas de soporte vectorial que permite la clasificación no lineal utilizando la función gaussiana, también se puede usar en las siguientes formas:

- Clasificación binaria.
- Clasificación multiclase
- Regresión
- Selección de variables
- Clustering

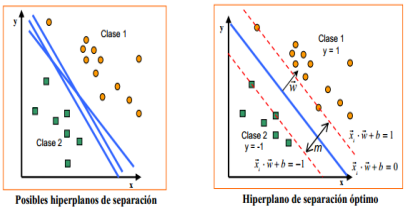


Ilustración 4.Detencion de análisis cardiacas como aprendizaje automático
Fuente: E. Carmona, « Dpto. de Inteligencia Artificial,» Universidad Nacional de Educación a Dsitansia, 2015. (11)

- Kernel Polinomial: Hace referencia al grado de polinomio característico de D.
- Kernel gaussiano: Se crea el hiperplano para depender de los parámetros.

Relación entre la inteligencia artificial y la ciberseguridad en Colombia

- En el 2017 los delitos informáticos afectaron cerca de 446 empresas en Colombia.
- Con una detección de 9.6% en 2017, Colombia se encontraba en el quinto lugar de países de Latinoamérica con mayor propagación del código malicioso Ransomware (una de las modalidades de Malware).
- 11.618 denuncias por delito digital recibieron en el Centro Cibernético de la Policía en 2017. El hurto por medios informáticos y semejantes (60%), seguido de la violación de datos personales (16%) y acceso abusivo a un sistema informático (15%) fueron los más denunciados.
- Una nueva organización será víctima de ransomware cada 14 segundos en 2019, y cada 11 segundos antes de 2021. (Fuente: Cyber Security Ventures).

Inteligencia artificial.

Es la parte de la información que permite que funcione de manera autónoma del sistema, es una de las creaciones poderosas creadas por

el ser humano, pero no se conoce los alcances si llega a caer en manos equivocadas (12).
Inteligencia Artificial en DDoS: esta inteligencia combinada permite ver los ataques DDoS basado AI como una infraestructura capaz de manejar de forma eficiente las aplicaciones web mejorando de forma automática, ya no hablando solo de ataques humanos si no DDoS por medio de máquinas.

Redes Neuronales Artificiales

Las redes neuronales artificiales (ANN) permite el aprendizaje de forma automática teniendo bases del sistema nervioso, donde se trate de interconectar las redes mediante las neuronas por un impulso de estímulo.
Las redes neuronales son técnicas matemáticas que intenta imitar los procesos de aprendizaje conociendo las primeras redes como Perceptrón y Adaline , las cuales fueron capaces de aprender y entender las imágenes u objetos que pueda presentar una problemática (13).Es importante reconocer que la utilización de esta herramienta permite conocer visualmente como un proceso paralelo.
De igual forma Lara (14), afirma que “RNAs, son un proceso natural como un sistema biológico llamado sistema de procesamiento de información”

Clasificaciones de redes neuronales

Las RNAs son nodos que se relaciona como las neuronas en las cuales puede llegar a ser un complejo neocognitron o perceptron.

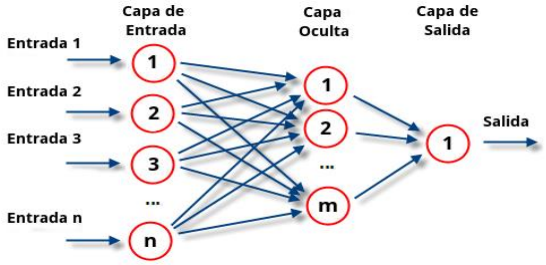


Ilustración 5.Niveles de Redes Neuronales
Fuente: Arredondo, T. (2012). Introducción a las Redes Neuronales (15).

Se puede observar en la ilustración N° 4, las redes neuronales tienen capas o niveles que permite el funcionamiento de los niveles de la red.

Trafico de la red de datos.

Permite dar a conocer los datos dentro de la red mediante el registro TCP/IP, datos de uso de la CPU o datos generado en intente, este sistema operativo permite detectar intruso en el sistema de prevención de Intrusos (IDS / IPS) (16).
Los datos TCP/IP son tomados por un sniffer que captura los paquetes que pasan por un punto modificados de la red, Componiéndose de los siguientes puntos:

- Dirección IP de destino.
- Dirección IP de origen.
- Tipo de servicio.
- Puerto de destino.
- Puerto de origen.
- El tipo de protocolo

El modelo TCP/IP tiene como objetivo servir como trasmisión los paquetes de los datos dentro de las redes, proviene de los protocolos de control de trasmisión y protocolo de internet

Protocolo de Internet (IP)

Es la parte fundamental en internet, permitiendo el flujo de trasporte de los datos en datagrama peo no garantiza la entrega (17).

Protocolo de Control de Transmisión (TCP)

Es un protocolo orientado a crear conexiones que permita trasmitir por medio de las redes.

Sus funcionamientos crean que cada paquete permita la validación y control de los datos en él envió de los paquetes por red TCP/IP, según Siles Raul en su análisis de sistema afirma que “los modelo permite fundamental para comenzar el análisis de los puntos defectuosos de la red” (18).

Ilustración 6.Modelo de Capas
Fuente: R. Siles, «Análisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados,» 2012. (18)

En esto se define un modelo de TCP/IP cuenta con:

- Capa de Red: aceptas los datagramas de IP y se trasmite a una red especifica utilizando un interfaz de red en un dispositivo que sirve como controlador.
- Capa de Internet: maneja las comunicaciones entre un cómputo con otro mediante paquetes en la entrada de datagrama mediante un software de capa de red el cual envía mensaje por ICMP (protocolo de control de mensajes de internet), esta capa permite los puntos de red
- Capa de Transporte: permite la comunicación entre las aplicaciones, esta capa permite llegar sin error el flujo de información, llegando de forma confiable en este se tiene una recepción y retrasmisión de algún dato extraviado dentro de la red mediante códigos de destino en los programas de la aplicación.
- Capa de Aplicación: es la que se utiliza para acceder a los servicios dentro de la red, se da por medio de los protocolos de los diferentes niveles de trasporte al enviar o recibir, este modelo TCP/IP permite la flexibilidad y soporte en la red entre capas de la comunicación y los distintos usuarios

La Familia de Protocolos Modelo TCP/IP permite operar de la siguiente manera como lo muestra en la Ilustración 7.Modelo TCP/IP, es importante reconocer para poder analizar la vulnerabilidad del sistema

Ilustración 7.Modelo TCP/IP
Fuente: R. Siles, «Análisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados,» 2012. (18)

El protocolo DHCP y su funcionamiento

DHCP es un protocolo cliente/servidor en el que normalmente el servidor tiene una lista de direcciones IP dinámicas y éstas van siendo asignadas a los clientes por dicho servicio, sabiendo en todo momento qué maquina está en posesión de esa IP. El DHCP permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Este protocolo también permite al administrador supervisar y distribuir las direcciones IP de forma centralizada, automática, o incluso reservar direcciones IP's para equipos específicos dentro de la red. DHCP tiene tres formas distintas de asignar direcciones IP:

- Asignación manual o estática: Distribuye una dirección IP a una máquina determinada. Esto suele ser usado cuando se quiere controlar la asignación de dirección IP a cada cliente y evita que se conecten clientes no autorizados a la red.
- Asignación automática: Esta forma de distribución de direcciones IP es utilizada cuando el número de clientes en la red no varía demasiado. Funciona asignando una dirección IP a una máquina cliente la primera vez que ésta hace la solicitud DHCP al servidor y la misma dirección es asignada cada vez que la máquina se conecta a la red.
- Asignación dinámica: Este método de asignación permite que la dirección asignada a un cliente varíe, ya que normalmente una

dirección IP es dada al cliente por un intervalo de tiempo. Una vez finalizado el cliente debe volver a hacer la petición para la obtención de una nueva o misma dirección IP. Esto es útil cuando el número de clientes en la red no es fijo. (19)

Funcionamiento de DHCP

DHCP funciona sobre un servidor central (servidor, estación de trabajo o incluso un PC) el cual asigna direcciones IP a otras máquinas de la red. Este protocolo puede entregar información IP en una LAN o entre varias VLAN. Esta tecnología reduce el trabajo de un administrador, que de otra manera tendría que visitar todos los ordenadores o estaciones de trabajo uno por uno. Para introducir la configuración IP consistente en IP, máscara, gateway, DNS, etc.

Un servidor DHSC (DHCP Server) es un equipo en una red que está corriendo un servicio DHCP. Dicho servicio se mantiene a la escucha de peticiones broadcast DHCP. Cuando una de estas peticiones es oída, el servidor responde con una dirección IP y opcionalmente con información adicional. (20)

Machine Learning

Machine learning es el conjunto de técnica de inteligencia artificial basada en algoritmos de predicción, según Carlos Gonzalez afirma que "*El aprendizaje automático ("machine learning", en inglés) hace referencia al subcampo dentro de las ciencias de la computación especializado en el reconocimiento de patrones complejos en conjuntos de datos"* (21). El aprendizaje automático se divide en:

- Supervisado: Los datos están relacionados con una variable o datos que permite la entada de etiquetas clasificada en sistema finitas y discretas
- Regresión: son las salidas continuas de los datos mediante las variables.
- No supervisada: Los datos no tiene o dispone de salida donde se hace necesario crea estructura de platones mediante la estructura de clustering) y la asociación de la misma.

Algoritmo

En el algoritmo el Machine Learning permite hallar patrones de la información que por medio de algoritmo puede realizar las diferentes tareas clasificándolo en supervisado, semi-supervisado, por refuerzo, multi-tarea y transducción, entre estos algoritmos existe un tipo de aprendizaje encontramos:

- Supervisado: Decision Tree, kNN, Random Forest, Logistic Regression.
- No supervisado Apriori Algorithm, k-Means, Hierarchical Clustering
- Refuerzo Markov Decision Process, Q Learning.

En esta permite la predicción de los algoritmos de Machine Learning para detectar las amenazas sospechosas dentro de la seguridad

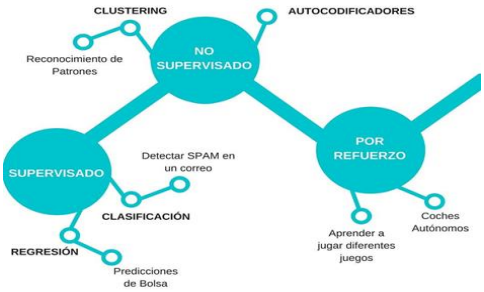


Ilustración 8.Tipos de Aprendizaje
Fuente: Joseph ,N. Conjunto de test ,2016. (22)

- Aprendizaje Supervisado: se utiliza información (dataset), reconocer imágenes (labels) o una nueva imagen (sin labels), dando predicciones continúas para generar nuevos patrones.
- Aprendizaje No Supervisado: no se cuenta con valor label teniendo como objetivo aprender los patrones de forma directa.
- Aprendizaje por Refuerzo: se da por medio de la experiencia se aprende de la prueba y el error para poder perfeccionarlo sin grandes cantidades de datos.

También ayuda como un conjunto de entrenamiento y conjunto de test

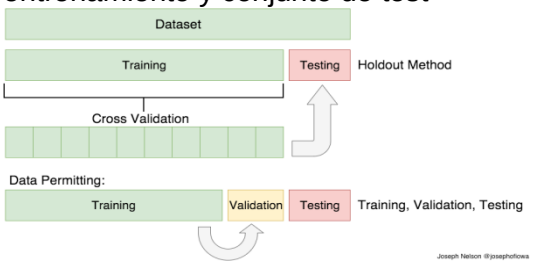


Ilustración 9.conjunto de entrenamiento y conjunto de test
Fuente : Joseph ,N. Conjunto de test ,2016. (22)

Árbol de decisiones

Los árboles de decisión o de clasificación son un modelo surgido en el ámbito del aprendizaje automático (Machine Learning) y de la Inteligencia Artificial que, partiendo de una base de datos, crea diagramas de construcciones lógicas que nos ayudan a resolver problemas. A esta técnica también se la denomina segmentación jerárquica. Es una técnica explicativa y descomposicional que utiliza un proceso de división secuencial, iterativo y descendente que, partiendo de una variable dependiente, forma grupos homogéneos definidos específicamente mediante combinaciones de variables independientes en las que se incluyen la totalidad de los casos recogidos en la muestra. (23)

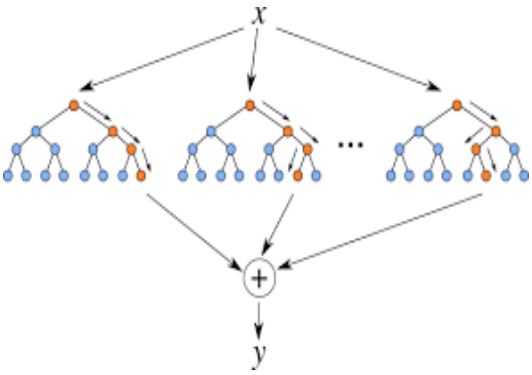


Ilustración 10.Arbol de decisiones
Fuente: Joseph ,N. Conjunto de test ,2016. (22)

MATERIALES Y MÉTODOS

El presente artículo se enfoca en una exploración bibliográfica descriptiva, que pretende explicar de manera sencilla diferentes características relacionadas a la inteligencia artificial para prevención y detección de ataques al protocolo DHCP.

Naturaleza de estudio:

Esta investigación es de naturaleza cualitativa, debido que su objetivo es mostrar los aportes relacionados la inteligencia artificial para prevención y detección de ataques al protocolo DHCP, en ella se conceptualiza sobre la realidad y se utiliza la recolección de información como medio principal para obtener una indagación más sólida y de fácil manejo que deje al descubierto las conclusiones y posibles inconvenientes en esta normativa (24).

Herramientas metodológicas:

Revisión literaria: como su nombre lo indica se procederá a la revisión bibliográfica y otros materiales que se relacionen con el asunto de estudio para así extraer, recopilar y organizar la información que atañe al problema de investigación. Para ello se tendrá en cuanta base de lectura crítica y su proceso de aplicación.

Para la revisión de la literatura Caro et al. lo resumieron en dos pasos:

1. Estudios preliminares o primarios: estudios individuales previos a la revisión sistemática.

2. Estudios secundarios: es la revisión sistemática en sí, planificación de la revisión, desarrollo de la revisión, publicación de los resultados de la revisión.

Fuentes de información

Fuentes primarias: Para identificar las principales fuentes que abordan la temática se buscaron artículos de investigación y tesis doctorales en las siguientes bases de datos: Scielo, Dialnet, Redalyc, ScienceDirect, proquest, MultiLegis, ieeexplore.

Fuentes secundarias: trabajos de grado y revistas de tipo científico no reconocidas citables y de referencia.

Sistematización de la información

Para el análisis de la información se incluye una base de datos de tipo discriminatoria con el propósito de eliminar fuentes no confiables y extraer la información útil para la investigación:

Tabla de sistematización:
Tipo de estudio:
Autor:
Año:
País:
Temática:
Metodología:
Conclusiones:
Palabras clave:
Fuente:

Muestra

Con el propósito de dar cumplimiento al objetivo planteado, la revisión del material bibliográfico se fundamenta en la identificación, selección y análisis de treinta (30) artículos, tesis e investigaciones, publicados en el periodo de (2000-2019), elaborados por estudiantes e investigadores y publicados en revistas reconocidas en el ámbito.

RESULTADOS

Después de la revisión sistematizada, en donde se tomaron como referencia 30 investigaciones, artículos y proyectos relacionados a la prevención de riesgos utilizando técnicas de inteligencia artificial, para desarrollar un análisis reflexivo sobre el desarrollo de sistemas de prevención y detección de ataques de denegación de servicio al protocolo al DHCP mediante la supervisión de la red.

Tabla SA 01

Autor	Auz Cadena Fabiola Cecilia
Temática	Implementación de controles en una LAN para mitigar los ataques del DHCP utilizando las mejores prácticas del diseño de redes.
Año	2019
Conclusiones	Se implementaron los controles dentro de la red de área local (LAN) reforzando la seguridad y privacidad de los clientes que establecen comunicación entre ellos y su navegación por internet. Se diseñó un escenario de red en la herramienta GNS3 que permitió la implementación del protocolo DHCP con su respectivo servidor y clientes.

Tabla SA 02

Autor	Jose León Henao Ríos
Temática	Definición de un modelo de seguridad en redes de cómputo, mediante el uso de técnicas de inteligencia artificial
Año	2012
Conclusiones	Como resultado de lo anterior se determinó que un muy alto porcentaje de las técnicas usadas por los atacantes para vulnerar una red se basan en protocolos tcp, de ahí que el trabajo se desarrolló exclusivamente sobre este tipo de tramas y específicamente sobre 8 (ocho) campos de esta.

Tabla SA 03

Autor	Eduardo Rodríguez
Temática	Defensa de un servidor público frente a ataques a través de red
Año	2019
Conclusiones	Como se ha visto a lo largo de este documento, un cortafuego no es infalible, pero es una herramienta de gran valor a la hora de detectar un sistema. IPtables provee una gran utilidad como cortafuegos para asegurar los sistemas en los cuales se instala, no solo por el hecho de poseer unas cadenas de reglas que controlan los paquetes de red, sino porque posee varios módulos que ayudan a controlar muchos comportamientos de los paquetes.

Tabla SA 04

Autor	Damián Matich
Temática	Redes neuronales: Conceptos básicos y aplicaciones
Año	2001
Conclusiones	El pensamiento tiene lugar en el cerebro, que consta de billones de neuronas interconectadas. Aprendizaje significa que aquellos problemas que inicialmente no pueden resolverse después de obtener más información acerca del problema. Por lo tanto, las redes neuronales consisten de unidades de procesamiento que intercambian datos o información.

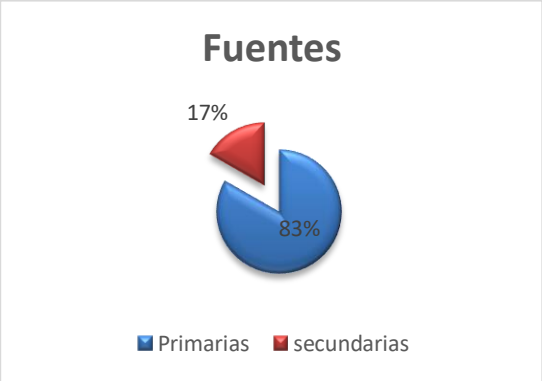
Tabla SA 05

Autor	Luis Orellana, Rafael Hernández
Temática	Seguridad en redes de datos
Año	2003
Conclusiones	Se dice insegura a una red en la cual la privacidad de los datos sea limitada y que se encuentre en riesgo de ser interceptados, alterados o robados, así mismo como propensas a transmitir información que dañe la red misma con virus, ya sea informáticos o de sistemas operativos, y por lo tanto la red se vuelva inestable, no brindando tranquilidad de un funcionamiento constante y optimo, y en la que no se pueda contar con un ancho de banda variable hasta de los límites de una velocidad en la que la transmisión de la información sea estable y aceptable, produciendo un debilitamiento en el rendimiento de la red, volviendo imposible la transmisión de datos, debido a que la red se ha vuelto sumamente lenta.

Análisis bibliométrico

Después de una revisión bibliométrica se determinó que de las fuentes revisadas 83% de las fuentes son consideradas primarias y solo un 17% son secundarias.

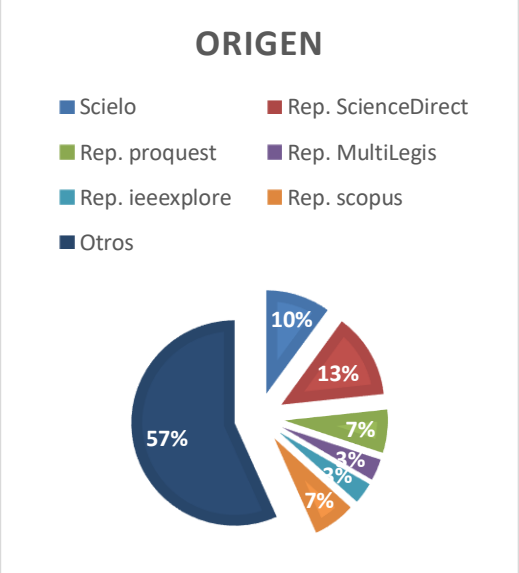
Caracterización de estudio



Fuentes	**Numero de publicaciones revisadas**	**%**
Primarias	*25*	*83%*
Secundarias	*5*	*17%*
Total fuentes	**30**	**100%**

Según los criterios de clasificación propuestos en el planteamiento metodológico, las fuentes primarias corresponden a revistas científicas y las secundarias a trabajos de otras fuentes.

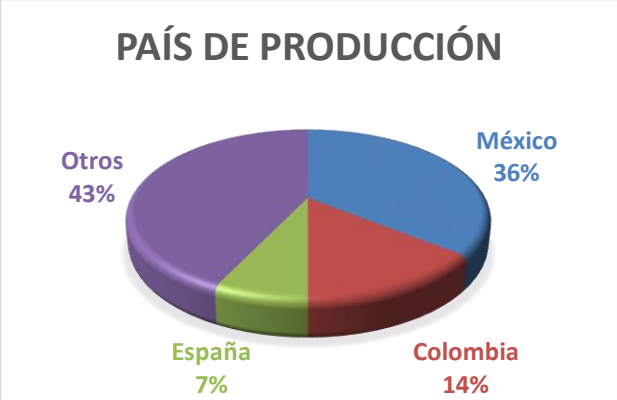
Tabla 1: Origen



Fuentes de publicación	Número de publicaciones revisadas	%
Otros	*17*	*57%*
Scielo	*3*	*10%*
Rep. ScienceDirect	*4*	*13%*
Rep. scopus	*2*	*7%*
Rep. proquest	*2*	*7%*
Rep. MultiLegis	*1*	*3%*
Rep. ieeexplore	*1*	*3%*
Total fuentes	**30**	**100%**

De las investigaciones revisadas, el 57% no corresponde a las fuentes planteadas anteriormente (Scielo, Dialnet, Redalyc, ScienceDirect, proquest, MultiLegis, ieeexplore), lo que indica que pertenecen a tesis universitarias publicadas en repositorios virtuales.
En la siguiente tabla se describe el país de producción. Según los criterios mencionados en la metodología solo se tomaron fuentes de origen Iberoamericano.

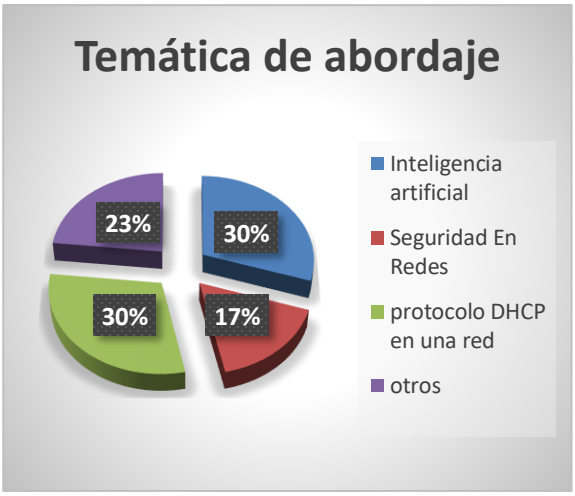
Tabla 2: Ciudad origen de la publicación



País de mayor producción literaria.	Número de publicaciones revisadas	%
México	*10*	*36%*
Colombia	*4*	*14%*
España	*2*	*7%*
Otros	*12*	*43%*
Total fuentes	**30**	**100%**

De las investigaciones que sirvieron como referencia, solo 7% son de origen español, mientras que el 14% son colombianas y en límites superiores un 36% son investigaciones mexicanas y el resto corresponden a investigaciones que no especifican el país de origen.

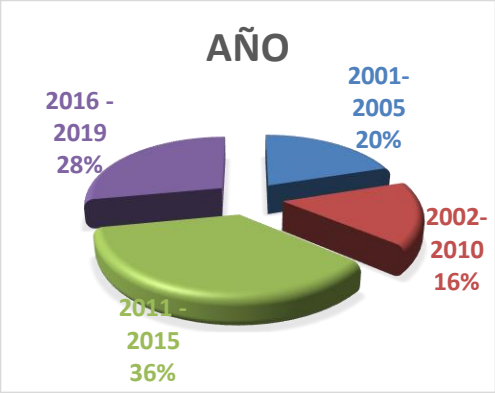
Tabla 3: temática de abordaje



Temática de abordaje Lit.	Número de publicaciones revisadas	%
Inteligencia artificial	*9*	*30%*
Seguridad En Redes	*5*	*17%*
protocolo DHCP en una red	*9*	*30%*
otros	*7*	*23%*
Total fuentes	**30**	**100%**

De las investigaciones revisadas las temáticas de mayor recurrencia son la inteligencia artificia (IA) y el protocolo DHCP en una red ambos con un 30%. Mientras la seguridad en redes y otras temáticas como el uso de la tecnología, normativas de seguridad entre otros, tuvieron una menor recurrencia.

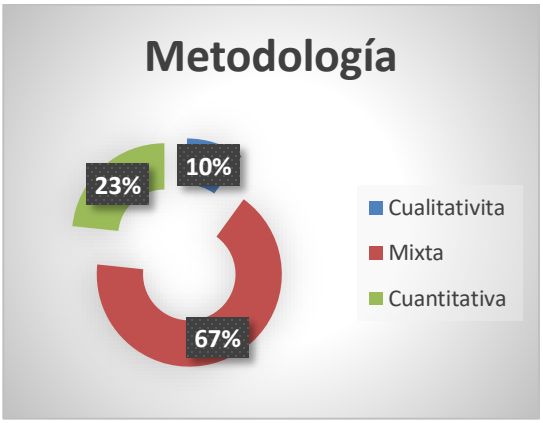
Tabla 8: Año de publicación



Año.	Número de publicaciones revisadas	%
2001- 2005	*5*	*30%*
2002- 2010	*4*	*17%*
2011 - 2015	*9*	*30%*
2016 -2019	*7*	*23%*
Total fuentes	**30**	**100%**

De las publicaciones revisadas, se encuentran con un porcentaje correspondiente al 30%, 17% y 30% las publicadas entre 2001 y 2015, y en los niveles inferiores con un porcentaje de 23% las publicadas entre el año 2016 y 2019.

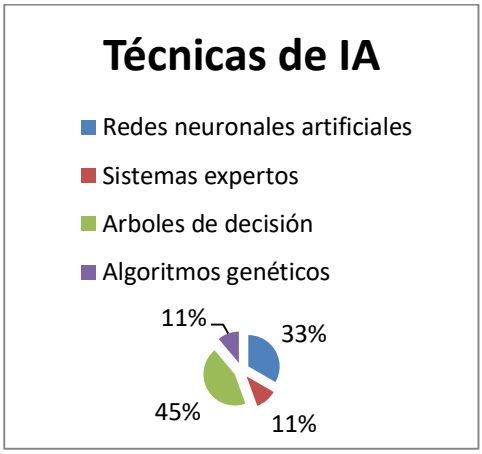
Tabla 9: metodología



Metodología	Número de publicaciones revisadas	%
Cualitativita	*3*	*10%*
Mixta	*20*	*67%*
Cuantitativa	*7*	*23%*
Total fuentes	**30**	**100%**

De las publicaciones revisadas se puede inferir que la metodología con mayor porcentaje de utilización es el mixto con un 67%, seguido por el cuantitativo con un 23% dejando por último el cualitativo con un 10%.

Tabla 10. Técnicas de IA

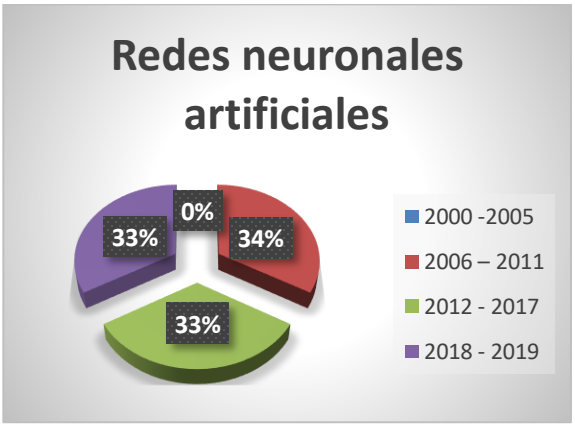


Técnicas de IA	Número de publicaciones revisadas	%
Redes neuronales artificiales	*3*	*10%*
Sistemas expertos	*1*	*67%*
Arboles de decisión	*4*	*23%*
Algoritmos genéticos	*1*	*23%*
Total fuentes	**30**	**100%**

La técnica de inteligencia artificial más utilizada en las publicaciones revisadas es el árbol de decisión con un 45%, seguida por las redes neuronales artificiales con un 33%, dejando los sistemas expertos y algoritmos

genéticos con un 11% como la técnica menos utilizada.

Tabla 11. Redes neuronales artificiales



	Años de publicación	N°	%
Redes neuronales artificiales	*2000 -2005*	*0*	*0%*
	2006 – 2011	*1*	*34%*
	2012 - 2017	*1*	*33%*
	2018 - 2019	*1*	*33%*
	Total	**3**	**100%**

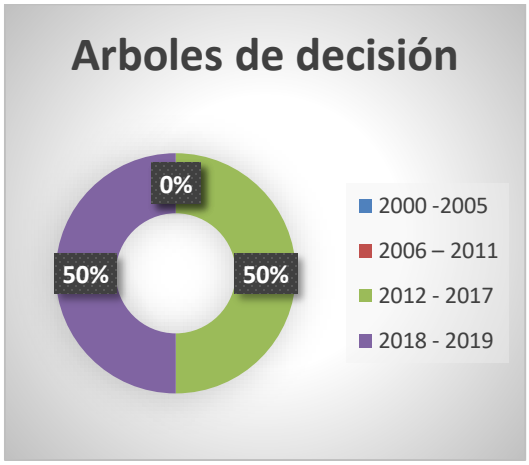
De las publicaciones revisadas se publicó del año 2006 al 2011 un solo artículo teniendo como porcentaje 34%, en el 2012 al 2017 con un 33%.

Tabla 12, Sistemas expertos

	Años de publicación	N°	%
Sistemas expertos	*2000 -2005*	*0*	*0%*
	2006 – 2011	*0*	*0%*
	2012 - 2017	*0*	*0%*
	2018 - 2019	*1*	*100%*
		1	*100%*

La técnica de sistemas expertos se utilizó en una de las publicaciones realizadas la cual se dio entre el 2018 y el 2019 con un porcentaje del 100%

Tabla 13. Arboles de decisión

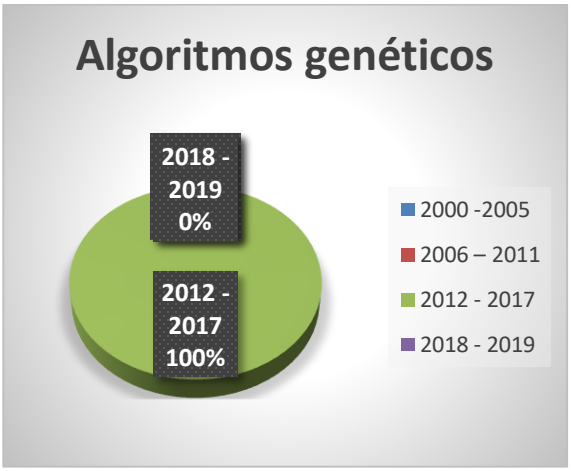


	Años de publicación	N°	%
Arboles de decisión	*2000 -2005*	*0*	*0%*
	2006 – 2011	*0*	*0%*
	2012 - 2017	*2*	*50%*
	2018 - 2019	*2*	*50%*
		4	**100%**

La técnica de árboles de decisión es la más utilizada en las publicaciones revisadas que se realizaron siendo cuatro los artículos que implementaron esta técnica teniendo como porcentaje un 50% entre los años 2012 y 2017, y por consiguiente entre el 2018 y 2019 con un 50%.

Tabla 14. Algoritmos genéticos.

	Años de publicación	**N°**	**%**
Algoritmos genéticos	*2000 -2005*	*0*	*0%*
	2006 – 2011	*0*	*0%*
	2012 - 2017	*1*	*100%*
	2018 - 2019	*0*	*0%*
		1	***100%***



Dentro de las publicaciones revisadas solo una utilizo la técnica de algoritmos genéticos publicada entre el 2012 y 2017 con un porcentaje del 200%.

Análisis de los resultados

Los resultados del análisis de producción, nos permite entrever que la inteligencia artificial y los protocolos de seguridad son una temática de mucho interés a nivel mundial y que son muchas las investigaciones que han surgido a lo largo de los años.

Esto se debe a la necesidad de intercambiar información y la necesidad de protegerla. Para la protección de estos datos, se deben establecer mecanismos que validen la información que se puede recibir y transmitir. Analizando las soluciones existentes, se encuentra que es viable la creación de un proceso de seguridad, el cual, tendrá como base el grado de certeza obtenido durante la fase de clasificación del flujo de datos de la red, logrando una correcta distinción de un flujo representativo de ataque y de un flujo normal (25).

Ahora bien, según la teoría revisada, el desconocimiento del funcionamiento de un sistema, así como de su uso y la violación de reglas establecidas para el mantenimiento de la seguridad en una red, son las principales causas de generar vulnerabilidad a una red y de que factores externos o internos puedan generar una incidencia en la red, ocasionando pérdida de información, pérdida de servicios o robo de la información que se maneja.

La aplicación de técnicas de minería de datos que emplean algoritmos pertenecientes a la inteligencia artificial ofrece una gran ventaja para entender el comportamiento de un fenómeno, en este caso reconocer cuando se produce un ataque de intrusión en una red, el cual, logra valerse del envío de paquetes permitidos por los protocolos de red, pero en un formato mayor, con lo cual, se consigue una saturación del servidor y dejarlo fuera al servicio (26).

DISCUSIÓN

Con los avances tecnológicos la seguridad informática se ha convertido en una de las operaciones que garantice a los usurarios la protección de sus datos dentro de la red de manera segura. Por eso la IA es desarrollada con tecnología como lenguajes de programación y bases de datos pero lo que dota a estos programas de habilidades comparables con las humanas es el uso del Machine Learning, esto permite garantizar la seguridad de un servicio y los datos que alberga es un punto primordial en la existencia de un servicio y en especial de la organización, puesto que una vulnerabilidad no controlada y explotada por algún atacante, puede llevar a la organización no solo a perder dinero por los daños al servicio, sino a ser sancionados por el incumplimiento de algunas de las leyes de regulación con respecto a la información en servicios informáticos.
La IA ha reinventado la protección de puntos finales al proporcionar seguridad predictiva y

preventiva que detiene los ataques de forma proactiva antes de que afecten a los sistemas críticos. El antivirus tradicional requiere capas de tecnología y una primera víctima, y no pueden evitar amenazas nunca antes vistas o desconocidas. La IA predice y protege en pre-ejecución a los sistemas, antes de que ocurra un ataque, y sin un paciente cero. Con menos capas de seguridad, tráfico de red y uso de memoria, puede alcanzar una efectividad superior al 99% frente a los ataques, a la vez que ahorra tiempo, dinero y recursos. (27).

Hernández Rodríguez en el proyecto "Defensa de un servidor público frente a ataques a través de red" Tecnologías de la información. 2019 este proyecto utiliza IPtables, cortafuego que implementan los equipos con las distribuciones de Linux, para detectar y contener los ataques más frecuentes a servidores expuestos por prestar servicios a todo el mundo. Para la realización del estudio de los ataques más importantes, utilización o/y desarrollo de herramientas que implementen estos ataques y implementación de un cortafuego implementado con IPtables para la protección contra diferentes ataques. Estas herramientas de ataques garantizarán el correcto funcionamiento del sistema creado y así crear un entorno seguro en el que el servidor podría ofrecer un servicio sin miedo a verse afectado por los diferentes ataques que se estudiarán (28).

Por otra parte el documento "Definición De Un Modelo De Seguridad En Redes De Cómputo, Mediante El Uso De Técnicas De Inteligencia Artificial" por José León Henao Ríos en el año 2012 de la Facultad De Ingeniería y Arquitectura, Departamento de Ingeniería Eléctrica y Electrónica de la universidad Nacional de Colombia, tuvo como objetivo principal general conocimiento de versatilidad que permita el acceso de la informaciones pero con los problemas que se presenta en las redes es necesario identificar las técnicas que permitan mitigar las amenazas aportando a nuestro trabajo conocer las especificaciones de la normalización (Z-Score), reducción de dimensional dad (PCA) y clasificación basada en redes neuronales (ANN1) con el fin de proponer un sistema de detección de intrusiones (IDS) En el caso de AI combina tres modos de aprendizaje que realiza sin la necesidad de ser supervisado por un programador, luego señala los intentos de ciberataque para que los analistas hagan observaciones y en base a los errores y aciertos en su identificación de ciberataques, añade patrones a sus análisis, esto ha sido llamado por los especialistas: "sistema de aprendizaje activo continuo". (6)

En otro aporte encontramos la tesis titulada "Sistema de Detección de Ataques EDoS en Entornos Cloud" por Julio Javier Lopez Gimenez, Jose Angel Madrona Martini, Lorenzo Susarte Trujillano en el año 2015 tiene como aporte la tecnología de la existencia en la nube y la flexibilidad de usar las IP para las demandas de los usuarios, en esta investigación se sostuvo que los algoritmos de aprendizaje automático (Algoritmos de regresión, Algoritmos bayesianos, Algoritmos de agrupación, Algoritmos de árbol de decisión, Algoritmos de redes neuronales, Algoritmos de Aprendizaje Profundo) representan uno de los máximos exponentes de la inteligencia artificial en la actualidad. Capaces de detectar los errores que cometieron y de corregirlos, los sistemas basados en estándares de aprendizaje automático ayudan a combatir la incertidumbre y permiten tomar las decisiones adecuadas en base a datos rigurosos. Dos habilidades muy valoradas en la ciberseguridad, especialmente porque los ataques modernos se basan en incógnitas. (29).

En cuanto a los sistemas para la detención de intruso que no son más que pautas para el cuidado del sistema, implementados desde 1980. Hemos revisado el artículo titulado: *"Implementación de un sistema de detección de intrusos para la red local de la ferretería corintios en santa marta*", de Hugo Alberto Payares Becerra en el año el 2016 por la UNAD , tiene como objetivo Implementar un Sistema de Detección de Intrusos IDS en la red de datos de la ferretería corintio apoyado en medidas de ciberseguridad para disminuir la intrusiones internas y externas de usuarios que comprometen la seguridad de la información, nos permite dar apoyo los

procesos de vulnerabilidad de las organizaciones mediante software o multiplataforma configurada en el Snort, en este proyecto se sostiene que el uso de sistemas de aprendizaje automático permite detectar y analizar ciberamenazas de forma rápida para prevenir o detener incidentes de manera efectiva. Por eso representa uno de las principales perspectivas en términos de ciberseguridad corporativa.

La decisión de la elaboración del trabajo de grado con Snort, es que este es un sistema IDS basado en red (NIDS). El cual, tiene como característica analizar y capturar paquetes en busca de alertas, registro y cualquier anomalía que presente la red, con la finalidad de evitar las vulnerabilidades que presente dicha información de la organización. Por esta razón se hizo necesario implementar un IDS ya que con el desarrollo de este se pretende utilizar los mecanismos necesarios que justifiquen su validez y ejecución beneficiando el manejo de la información en cuanto a seguridad e integridad de la información y así dar pautas o recomendaciones para implementar un IDS en la Ferretería Corintios, implementando la herramienta de detección de intrusos para la red que permita proteger los activos reales de la información digitalizada. (29).

En el trabajo "*Comparación de algoritmos para detección de intrusos en entornos estacionarios y de flujo de datos".* Realizado por Rivero, Ribeiro y kadir en el 2016, tuvo como objetivo analizar un conjunto de datos que cuentan con 41 atributos distintos, de los cuales, se seleccionaron 23 para su clasificación. El entrenamiento se realizó con el 10 % de los 51 millones de instancias Preliminares contenidas en la base de datos, aplicándoles tres variantes de preprocesamiento, para después hacer una comparación basada en el uso de algoritmos representativos del aprendizaje automático. Entre estos algoritmos se encuentran, una Red Neuronal Perceptron Multicapa (MLP), SMO que es una variante empleada en WEKA del algoritmo de Máquinas de Soporte Vectorial (SVM), el algoritmo J48, Naive Bayes y el algoritmo basado en instancias K con valores 3, 5 y 7.

En este artículo se describen y proponen tres variantes de pre procesamiento sobre el conjunto de datos KDD99, incluye selección de atributos. Luego la experimentación se realiza primeramente a partir de evaluar algoritmos representativos en entornos estacionarios sobre las variantes obtenidas a partir de pre procesar KDD99. Por último, dado que el tráfico de red es un flujo constante de datos, en el cual pueden existir variaciones de conceptos relacionadas con las tasas de falsos positivos, unido al hecho de que no se encuentran muchas investigaciones que aborden la detección de intrusos en entornos de flujos de datos nos conduce a realizar una comparación de varios algoritmos también representativos de flujos de datos. Como resultado se obtiene cuáles son los algoritmos que mejores resultados ofrecen en la detección de intrusos sobre las variantes de pre procesamiento propuestas, tanto para entornos estacionarios como de flujos de datos (30).

En el trabajo "*Implementación de controles en una LAN para*

Mitigar los ataques del DHCP utilizando las mejores prácticas del diseño de redes" por Cadena Auz, La implementación de un servidor DHCP es importante dentro de una red, ya que proporciona direcciones IP automáticamente a los clientes que se conectan asignándoles todos los parámetros de la red necesarios, sin embargo, sin la configuración adecuada se encuentra vulnerable a ataques de suplantación e incumplimiento de DHCP.

Considerando los ataques posibles al servidor DHCP se implementarán los controles para mitigar las vulnerabilidades como la seguridad de puertos y activar la indagación de DHCP en el switch para identificar al servidor de confianza.

Uno de los proyectos encontrado acerca de la temática que se está tratando en esta tesis, el cual lleva como nombre "*Vulnerabilidad, tipos de ataques y formas de mitigarlos en las capas del modelo OSI en las redes de datos de las organizaciones*" tiene como objetivo relacionar las diferentes formas de

prevención a los diversos ataques a las infraestructuras de red, durante el proceso se pudo identificar que uno de los mejores métodos para hacerle frente a los ataques informáticos es anticipar su presencia, una de las estrategias de mitigación a ataques específicos son el footpriting, fingerprinting, escaneo de puertos, entre otros que permiten mitigar todo proceso de detección de intrusos

Queda claro que existen situaciones en las cuales es necesario implementar otras medidas de seguridad complementarias de forma que, el cortafuego sea solo una primera instancia en la defensa de una máquina y detrás de él existan sistemas encargados de ayudar a mitigar posibles ataques.
Dentro de los trabajos revisados implementan técnicas de minería de datos. Cuantos más complejos son los conjuntos de datos recopilados, mayor es el potencial que hay para descubrir insights relevantes. Los comerciantes detallistas, bancos, fabricantes, proveedores de telecomunicaciones y aseguradoras, entre otros, utilizan la minería de datos para descubrir relaciones entre todas las cosas, desde precios, promociones y demografía hasta la forma en que la economía, el riesgo, la competencia y los medios sociales afectan sus modelos de negocios, ingresos, operaciones y relaciones con clientes.
En síntesis, el aprendizaje automático está ayudando a perfeccionar las soluciones de ciberseguridad. Sin embargo, A medida que las empresas adoptan nuevos sistemas de protección de su entorno digital, los ciberdelincuentes también desarrollan habilidades más sofisticadas. Por ello, la única opción para avalar la seguridad es situarse un paso adelante en el uso de sistemas automatizados basados en IA.

CONCLUSIONES

Con el desarrollo de este artículo se puede concluir que los objetivos establecidos al comienzo han sido cumplidos, las redes de datos hoy en día funcionan bajo un modelo basado en capas de protocolos. Debido a esto se ha desarrollado mucha literatura enfocada al funcionamiento de dichos modelos, buscando demostrar sus aspectos más importantes de funcionamiento, entre los cuales se encuentra la seguridad.

Así mismo como se ha realizado estudios sobre la seguridad en dichos modelos, también se han desarrollado nuevas amenazas y vulnerabilidades que se han enfocado estrictamente a atacar los protocolos de cada capa y buscar la manera de hacer el mayor daño posible a las redes de las empresas u organizaciones que no estén preparadas para prevenirlos, detectarlos y mitigarlos.

A la hora de querer prevenir y detectar los ataques por denegación de servicios se encuentran diferentes métodos para ello, los cuales implican Inteligencia Artificial o IA, esta implementación ha ayudado y mejorado mucho la seguridad por medio del Machine learning ya que este crea una línea base de las actividades básicas y normales de la red, cuando hay un ataque el comportamiento de la red cambia notablemente, por lo tanto el Machine learning notará este cambio y se notificará como un posible ataque o una posible invasión a la red.

El punto débil del Machine Learning es que también está al alcance de los ciber delincuentes por lo tanto es una batalla no tan fácil de ganar. Sin embargo, a esto se le pueden sumar otros métodos de prevención; para ello se puede configurar de manera adecuada los Firewalls para poder filtrar de forma más efectiva las IP inválidas, incluso algunos routers y firewalls traen consigo la opción para prevenir floods (Inundaciones), es decir que la seguridad no solo depende del usuario en sí, sino que también de los equipos físicos que se empleen en su estructura de red. Por otra parte, la prevención depende en gran manera directamente del proveedor de servicios de red ya que ellos pueden ayudar a bloquear el tráfico inusual de datos más cercano a su origen.

El machine learning y la inteligencia artificial hoy juegan un papel crucial en la detección de posibles ciberataques y cada vez más

sociedades de ciberseguridad disponen ocuparse con estas tecnologías para enfrentar a los cibercriminales.

Entre las habilidades más frecuentes se encuentran la de poder recolectar y almacenar información para luego analizarla a partir de un Motor de Machine Learning. Al final, se busca predecir posibles comportamientos o vulnerabilidades en los equipos y servidores y de esta forma lograr reaccionar de manera anticipada.

Primero hay que deducir que no hay una forma única. Las organizaciones deben poseer una estrategia que cubra los diferentes aspectos apoyada en los riesgos. Tienen que invertir recursos, pero en esa estrategia se debe incluir sensibilización. Hay que emplear una serie de inspecciones para que se monitoree su ambiente digital. No simplemente los servidores donde está la información, sino saber qué se está ocurriendo con los datos, quién los está utilizando y si verdaderamente están autorizados.

Aunque las tecnologías en redes siguen avanzado permitiendo en gran medida controlar el acceso no autorizado de usuarios o personas en una red de una organización, aun muchas de ellas siguen siendo vulnerables a las intrusiones de hackers, sin importar el tipo de ataque que se haga, ya sea por la falta de conocimiento del valor de su información, por el desconocimiento de los mismos ataques o por la falta de políticas de seguridad claras que sean estrictamente impuestas por parte de los administradores de los sistemas de información de tal manera que sirva de blindaje ante posibles modelos de ataques.

Es importante entonces tener en cuenta los aspectos mencionados sobre los tipos de ataques, vulnerabilidades y forma de mitigación, para tener una visión más clara del impacto operacional en los procesos de una organización y así poder dimensionar la verdadera importancia de que la red de datos del sistema de información se encuentre completamente segura.

BIBLIOGRAFÍA

1. **Banco Interamericano del Desarrollo.** *Ciberseguridad.¿Estamos preparados en America Latina y el Caribe?* 2016. Organizacion de las americas unida.

2. **Nacioanal, Plataforma de Informacion de la Policia.** *Estadistica Centro Cibernetico de la policia nacional.* [En línea] Octubre de 2017. caivirtual.gov.co.

3. **Centro Cibernetico Policia Nacional.** *Amenazas de Cibercrimen en Colombia 2016-2017.* [En línea] 2018. caivirtual.com.

4. *Configuración de una Red Local.* **Rubén, Balirac Seijas.** madrid : Instalación y Configuración de Computadores y Periféricos, mayo 2016.

5. **Mieres, Jorge.** Ataques Informaticos. *Debilidades de seguridad comunmente explotadas.* [En línea] 2009. http://proton. ucting. udg. mx/tutorial/hackers/hacking. pdf.

6. **Lopez, J.** *Sistema de deteccion de ataques EDoS en entorno cloud.* Cundinamaca : s.n., 2015.

7. **Mesa, A.** Sistema Informatico . [En línea] Octubre de 2016. http://nichimm3.blogspot.com/2016/10/amenazas-humanas.html.

8. **Castrillo, A.** Medidas de protección frente ataques de denegación de servicio (DoS). [En línea] Eneo de 2018. https://www.incibe-cert.es/blog/medidas-proteccion-frente-ataques-denegacion-servicio-dos..

9. **Lizamar, J.** *Hackers en el contexto de la sociedad de la informacion.* Mexico : s.n., 2005.

10. **Lopez, Oscar Andres, Parra, Misael Leonardo y Manzur, Beatriz.** Arquitectura y comunicaciones en sun sistema de deteccion de intrusos. *Primer congreso Iberoamericano de seguridad informatica CIBSI.* [En línea] 2002.

11. **Carmona, E.** *Dpto. de Inteligencia Artificial.* s.l. : Universidad Nacional de Educación a Dsitancia , 2015.

12. *Definición De Un Modelo De Seguridad En Redes De Cómputo, Mediante El Uso De Técnicas De Inteligencia Artificial.* **León, Henao Ríos José.** Pág. 2 -126 , Manizales – Colombia. : Universidad nacional. , 2012.

13. **Freeman , J y Skapura.** *Neural networks: algorithms, applications and programming techniques.* s.l. : Computation and Neural Systems Series, 1991.

14. **Lara, J.** *Aplicacion de las redes neuronales artificiales al campo de la valoracion inmobiliaria.* Mapping : s.n., 2015.

15. **Arredondo, T.** Introducción a las Redes Neuronales. [En línea] 2012. http://profesores.elo.utfsm.cl/~tarredondo/info/soft-comp/Introduccion%20a%20las%20redes%20neuronales.pdf. .

16. *desarrollo de un proceso de seguridad para la prevención de intrusiones en una red privada.* **Laura, Alcántara Ramírez Ana.** Valle De Chalco Solidaridad, México : s.n., 2017.

17. *arquitectura de servicios tecnológicos que soportan los sistemas de información y entrega de servicios informáticos, relacionados con los procesos misionales y de apoyo de la superintendencia nacional de salud.* **Andrés, arrado Velásquez Fabio.** bogota : Estudios En Ambientes Virtuales., 2018.

18. **Siles, R.** *Análisis de la seguridad de la familia de protocolos TCP/IP y sus servicios asociados.* 2012.

19. **Cerdan Lopez, Juan Francisco.** Administracion de sistemas corporativos basados en windows 2012. *Server. Protocolos de red.* [En línea] 2015.

20. **Barrios, Fernanda.** El protocolo DHCP y su funcionamiento. [En línea] 2017. https://www.ugr.es/~fernanla/Untitled.pdf.

21. **González, C.** *En qué consiste el aprendizaje automático (machine learning) y qué está aportando a la neurociencia cognitiva.* Belgica : Dept. of Experimental Psychology, 2018.

22. **Joseph, N.** Conjunto de test. [En línea] 2016. https://bookdown.org/content/2031/arboles-de-decision-parte-ii.html.

23. **Parra, Francisco.** Estadistica y Machine Learning. [En línea] 2019. https://bookdown.org/content/2274/portada.html.

24. *metodologia de la investigacion .* **Sampieri, Hernandez.** Buenos aires : Free libros, 2000, Vol. 5.

25. *Defensa de un servidor público frente a ataques a través de red.* **Eduardo, Hernández Rodríguez.** 12, Las Palmas de Gran Canaria : Tecnologías de la información., 2019, Vol. 1.

26. *Una propuesta de IDS, basado en Redes Neuronales Recurrentes.* **Pinacho, P., Valenzuela T.** Grupo de Investigación en Tópicos de Seguridad de Chile (GITS), : Universidad Santiago De Chile (USACH),, octubre de 2003.

27. *implementación de controles en una LAN para mitigar los ataques del DHCP utilizando las mejores prácticas del diseño de redes.* **Cecilia, Auz Cadena Fabiola.** 29, manchala : Unidad Académica De Ingeniería Civil, 2019, Vol. 1.

28. *Defensa de un servidor público frente a ataques a través de red.* **Eduardo, Hernández Rodríguez.** las palmas gran canarias : Rev. ciencias e ingenieria, 2019, Vol. 94.

29. **Paxson, V.** V. Paxson, «feuture,» 2017. [En línea]. Available: WWW.bro-ids.org. [Último acceso: Agosto 2019]. *feuture.* [En línea] 2017. www.bro-ids.org..

30. *Comparación de algoritmos para detección de intrusos en entornos estacionarios y de flujo de datos.* **Rivero, J. Ribeiro, B. Kadir H.** Revista Universidad y Sociedad, págs. 32-42.

31. **Cesar Mejia, Nini Ramirez, Juan Rivera.** *VULNERABILIDAD, TIPOS DE ATAQUES Y FORMAS DE MITIGARLOS EN LAS CAPAS DEL MODELO OSI EN LAS REDES DE DATOS DE LAS ORGANIZACIONES.* PEREIRA : UTP, 2012.

32. **Valencia, A ,» Madrid, 2016.** *Códigos de la buena práctica seguridad.* Madrid : s.n., 2016.

33. **Martin, C.** Blog de carmennmartin. [En línea] Noviembe de 2015. http://diarium.usal.es/carmennmartin/2015/11/06/red-de-area-local/.

34. **Montañama, R.** Arquitectua LAN conmutada. [En línea] 2015. https://angell2017.wordpress.com/2017/02/01/primera-entrada-del-blog/.

35. **Fuentes, C.** Redes inalámbricas. [En línea] 2015. https://slideplayer.es/slide/5473520/.

36. **breiman.** *Classification and Regression Trees.* Taylor & Francis : Francia, 1984.

37. **Profesorado, I. d.** Instituto de Tecnologías Educativas y de Formación del Profesorado. [En línea] 2010. [Citado el: 27 de febrero de 2020.] http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dhcp.html.

38. **Muñoz, José Domingo.** [En línea] 2017. [Citado el: 06 de 03 de 2020.] https://serviciosgs.readthedocs.io/es/latest/dhcp/dhcp.html.

39. **Henao, J.** *Definición De Un Modelo De Seguridad En Redes De Cómputo, Mediante El Uso De Técnicas De Inteligencia Artificial.* bogota : Universidad Nacional de Colombia, 2012.

40. **Ramiro, A.** *Inteligencia artificial utilizada en ataques DDOS.* Madrid : s.n., 2018.

41. **Revista Dinero.** *La seguridad informática mueve US$34.000 millones .* [En línea] Abril de 2015. https://www.dinero.com/empresas/articulo/seguridad-informatica-colombia-mundo/202796..

42. **Optical News,.** *«Ataques informáticos con inteligencia artificial.* [En línea] 2010 de Julio . https://www.optical.pe/ataques-informaticos-con-inteligencia-artificial/.

43. **Union, I.** *Open System Interconnection OSI.* [ed.] Comunication Networks. 1996.

44. **Armando, D.** Centro de Estudio de Desarrollo Agrario y Rural. [En línea] 2015. http://www.econlink.com.ar/sistemas-informacion/definicion.

45. **ISO2007.** Sistema de Gestión de la Seguridad de la informatica. [En línea] 2005. http://www.iso27000.es/.

46. **Carlos Higuera.** Tecnología. [En línea] 9 de 06 de 2012. [Citado el: 06 de 03 de 2020.] https://es.slideshare.net/CarlosHiguera3/dhcp-presentacin?from_action=save.

47. *Sistema de Deteccion de Ataques EDoS en Entornos Cloud.* **Lucila, arcıa Villalba Luis Javier y Sandoval Orozco Ana.** Madrid : Universidad Complutense de Madrid, Junio de 2015., Vols. Pag 1- 88 .

48. *Redes Neuronales: Conceptos Básicos y Aplicaciones.* **Jorge, Matich Damián.** Regonal Rosario : Universidad Tecnológica Nacional, Marzo de 2001.