Análisis de las Vulnerabilidades del Protocolo de Comunicación TCP/IP en redes de telecomunicaciones inalámbricas corporativas

Franci Elena Joaqui Anacona

Mayerly Meneses Muñoz

Asesora

Paulita Flor Salazar

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2024

Nota de Aceptación

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Popayán, 3 de junio de 2024

Dedicatoria

Con profunda gratitud, dedicamos este logro a nuestros queridos padres y a nuestras familias. Su amor incondicional y apoyo constante han sido la luz que ha guiado nuestro camino profesional. Agradecemos de corazón cada sacrificio y cada palabra de aliento. Queremos hacer una mención especial al padre de Mayerly, que, aunque ya no está con nosotros, su espíritu y enseñanzas siguen inspirándonos cada día. Este éxito es tanto suyo como nuestro

Agradecimientos

Agradecemos en primera instancia a Dios, por la sabiduría y fortaleza brindadas durante este arduo pero gratificante camino. A nuestra familia, por su cariño, oraciones y apoyo incondicional, fundamentales para este triunfo. A nuestros amigos, quienes nos han ayudado con sus consejos, risas y compañía, siendo nuestro soporte emocional. A nuestros compañeros de vida, gracias por recorrer este sendero a nuestro lado. A los docentes que nos enseñaron a soñar en grande y el sentido de la perseverancia. A nuestra asesora de trabajo de grado, por acompañarnos con compromiso, e invaluable experiencia. A todos ustedes, nuestro más sincero y eterno agradecimiento, pues son los verdaderos autores de este logro.

Resumen

A lo largo de la evolución de la tecnología y con la llegada del internet, se han ido conociendo diferentes términos que resultan importantes de entender y tener en cuenta cuando del estudio de las redes de comunicación se trata, dentro de estos términos se encuentra la seguridad informática o ciberseguridad, la cual se puede definir e interpretar como las prácticas, técnicas y herramientas diseñadas para proteger los sistemas informáticos, redes, datos y programas contra accesos no autorizados, o cualquier otra forma de amenaza que pueda comprometer la confidencialidad, integridad o disponibilidad de la información.

Se ha evidenciado que, así como avanza la tecnología y los sistemas de información y comunicación, avanzan también los diferentes métodos y herramientas utilizados contra la seguridad de estos mismos. Como resultado de estas prácticas han surgido varias investigaciones en las que se han ido documentando los antecedentes existentes en la seguridad de los protocolos de comunicación utilizados en las redes de comunicación inalámbricas corporativas, uno de ellos es el protocolo de comunicación TCP/IP, estas investigaciones han dejado expuestas ciertas falencias existentes en el protocolo que se hacen necesarias abordar para poder garantizar la seguridad de una red en la que se vea involucrada información confidencial, como es el caso de las redes corporativas.

De este modo, a lo largo del desarrollo de esta monografía se verán expuestas diferentes fuentes, que evidencian dichas falencias, las cuales han sido abordadas con el propósito de proponer estrategias que ayuden a la prevención y contención de las vulnerabilidades existentes en el protocolo de comunicación TCP/IP en redes inalámbricas corporativas.

Palabras Clave: Seguridad Informática, Ciberseguridad, Vulnerabilidades, Redes.

Abstrac

Throughout the evolution of technology and with the advent of the Internet, different terms have become known that are important to understand and take into account when it comes to the study of communication networks, among these terms is computer security or cybersecurity, which can be defined and interpreted as the practices, techniques and tools designed to protect computer systems, networks, data and programs against unauthorized access, or any other form of threat that may compromise the confidentiality, integrity or availability of information.

It has become evident that as technology and information and communication systems advance, so do the different methods and tools used against their security. As a result of these practices, several investigations have been carried out documenting the existing background in the security of communication protocols used in corporate wireless communication networks, one of them being the TCP/IP communication protocol. These investigations have exposed certain shortcomings in the protocol that need to be addressed in order to guarantee the security of a network in which confidential information is involved, as in the case of corporate networks. In this way, throughout the development of this monograph, different sources will be exposed, which will avoid the need to address the security of the network in which confidential information is involved, such as corporate networks.

Key words: Computer Security, Cybersecurity, Vulnerabilities, Networks.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Introducción

En el marco del auge del crecimiento empresarial y tecnológico, las redes de telecomunicaciones inalámbricas corporativas desempeñan un papel fundamental en la facilitación de la comunicación y el intercambio de datos. Sin embargo, esta dependencia creciente también expone estas redes a diversos riesgos de seguridad.

Entre los protocolos de comunicación encargados de que este intercambio de datos sea posible se encuentra el protocolo de comunicación TCP/IP, un componente esencial que, aunque robusto, no está exento de vulnerabilidades potenciales. El análisis de las vulnerabilidades del protocolo de comunicación TCP/IP en entornos de redes de telecomunicaciones inalámbricas corporativas se convierte, por lo tanto, en una fuente esencial para salvaguardar la integridad, confidencialidad y disponibilidad de la información empresarial. La Monografía presentada, busca analizar las vulnerabilidades específicas asociadas con el protocolo de comunicación TCP/IP, para identificar amenazas emergentes que permitan proponer estrategias para fortalecer la seguridad en el entorno presentado.

Planteamiento del Problema

Antecedentes del Problema

Los protocolos de comunicación en redes de telecomunicaciones, son objeto de diversos estudios que han permitido la evolución tecnológica en aspectos de seguridad informática, pues de ellos depende la identificación de vulnerabilidades o fallas que una vez expuestas son clave tanto para el fortalecimiento de la infraestructura de estos protocolos a nivel hardware y software, como para la detección de fallas comunes en el diseño e implementación de técnicas de seguridad implementadas en las redes de telecomunicaciones inalámbricas; El enfoque principal dado en esta investigación es el estudio de las vulnerabilidades presentes en el protocolo de comunicación TCP/IP en redes de telecomunicaciones inalámbricas corporativas sin embargo; los estudios realizados y documentados sobre el tema se han centrado principalmente en el estudio de las vulnerabilidades existentes en la capa de aplicación de este protocolo, se ha considerado que esta es una de las capas del protocolo de comunicación TCP/IP que mayor vulnerabilidades presenta y la falta de documentación y fortalecimiento de estas, puede tener repercusiones significativas en la confidencialidad y disponibilidad de la información transmitida. Al respecto en su tesis de investigación; "vulnerabilidades de las redes TCP/IP Y principales mecanismos de seguridad" Gutiérrez. A. (2009), concluyó "Los principales desafíos en el protocolo de comunicación TCP/IP surgen en la capa de Aplicación. Esta capa, debido al volumen significativo de datos que maneja y a las deficiencias inherentes a la programación, facilita que terceros operen de manera anónima, desarrollando software malicioso sofisticado (virus) destinado a manipular servicios específicos".

Dada la creciente amenaza de ataques cibernéticos, especialmente aquellos dirigidos a entidades corporativas, se ha identificado que una de las vulnerabilidades comúnmente explotadas es la conexión no autorizada a equipos y servidores. Este tipo de ataques abarca diversas técnicas, incluyendo la violación de sistemas de control de acceso, la explotación de vulnerabilidades (exploits) y otros métodos que, en última instancia, pueden resultar en el acceso no autorizado a información confidencial almacenada en servidores.

Entre las vulnerabilidades que podrían ser aprovechadas se encuentran aquellas relacionadas con el protocolo de comunicación TCP/IP, el cual sirve como el pilar fundamental para la interconexión de dispositivos en una red, (Silva & López, 2018). Este protocolo, organizado en capas, ha sido la base de Internet y ha demostrado ser esencial para la comunicación entre diferentes tipos de computadoras y redes.

La conexión no autorizada a sistemas y servidores, impulsada por vulnerabilidades en el protocolo TCP/IP, puede tener consecuencias significativas (Martínez, 2019). Los atacantes podrían comprometer la seguridad y confidencialidad de la información almacenada en servidores corporativos. Incluso, en algunos casos, podría acceder a datos y archivos que aparentemente habían sido eliminados del sistema, lo cual representa una amenaza grave para la integridad de la información. (Rodríguez, 2020)

En este contexto, es fundamental adoptar un enfoque proactivo hacia la seguridad de las redes corporativas, especialmente en entornos inalámbricos donde las vulnerabilidades pueden ser más explotables. La metodología cualitativa propuesta en este trabajo se centra en el análisis de las vulnerabilidades del protocolo de comunicación TCP/IP, proporcionando una base sólida

para comprender y abordar las posibles amenazas a la seguridad de la información en entornos empresariales (López & Gómez, 2019).

Este análisis no solo contribuye a la identificación de posibles vulnerabilidades, sino que también sienta las bases para la implementación de medidas de seguridad y la gestión efectiva de riesgos. En un panorama donde la información corporativa es un activo invaluable, la comprensión detallada de las vulnerabilidades en el protocolo de comunicación TCP/IP se vuelve esencial para garantizar la integridad, confidencialidad y disponibilidad de los datos en entornos empresariales conectados.

Descripción del Problema

TCP/IP es conocido como uno de los protocolos de comunicación con mayor utilidad en el medio de las comunicaciones, su funcionamiento se basa en una arquitectura dividida en cuatro capas dónde cada una tiene una función diferente y la comunicación entre estas se realiza por medio de interfaces definidas como protocolos de servicio, entre las funciones de las capas se tiene el encapsulamiento y enrutamiento de datos. La modularidad inherente al enfoque del protocolo TCP/IP ha permitido que sus capas operen de manera independiente, facilitando la interoperabilidad y la sustitución de tecnologías sin afectar otras capas del sistema. Este protocolo ha implementado medidas de seguridad robustas, basadas en auditoría de seguridad, detección de intrusiones, actualización y parches, control de acceso, autenticación, cifrado de datos y firewalls. A pesar de estas bases sólidas, a lo largo del tiempo, se han identificado vulnerabilidades que representan amenazas a la seguridad de las redes de telecomunicaciones. Una de las vulnerabilidades persistentes en el protocolo de comunicación TCP/IP es la "Predicción de números de secuencia". Esta vulnerabilidad implica la capacidad de un atacante

para prever el número de secuencia utilizado para identificar paquetes en una conexión TCP. Si un atacante logra identificar este número, puede falsificar paquetes hacia el host de destino desde una dirección IP con el mismo origen, lo que técnicamente se conoce como inyección en una conexión TCP. Este tipo de ataque puede resultar en el cierre de una conexión TCP existente y en la desviación y pérdida de información sensible. La gravedad de esta vulnerabilidad se refleja en numerosos informes de ataques dirigidos a diversas entidades gubernamentales y estatales, donde el objetivo principal es el robo de información sensible que fluye a través de los servidores de comunicación. A pesar de los esfuerzos para abordar estas vulnerabilidades, la predicción de números de secuencia sigue siendo una amenaza significativa. En este contexto, la pregunta de investigación planteada se vuelve crucial:

¿Cuáles son las Vulnerabilidades existentes en el protocolo de comunicación TCP/IP, que pueden afectar la seguridad de una red de telecomunicaciones Inalámbrica Corporativa?

Justificación

Las redes de telecomunicaciones inalámbricas han ido evolucionando día a día, y juegan un papel fundamental en el funcionamiento de la comunicación, conexión y flujo de datos en pequeños y grandes entes corporativos, y es por los beneficios que pueden ofrecer y el gran volumen de datos que se transportan sobre ellas, que se encuentran expuestas a diversas amenazas de seguridad, siendo el protocolo de comunicación TCP/IP un elemento central y crítico en la transmisión de datos. El análisis detallado de las vulnerabilidades asociadas Al protocolo de comunicación TCP/IP en el contexto de redes de telecomunicaciones inalámbricas corporativas se presenta como un área de investigación indispensable puesto que; las vulnerabilidades en el protocolo TCP/IP pueden dar lugar a consecuencias graves, como la interceptación no autorizada de datos, la manipulación de información crítica y la interrupción de servicios vitales para la operación empresarial. Un caso similar y no ajeno al problema planteado; se conoció el doce de septiembre de 2023 en Colombia, dónde un ataque tipo Ransomware ('secuestro' digital de información y aplicaciones) que fue dirigido a IFX Network afectó más de 700 máquinas con el cifrado o ataque realizado, en una entrevista dada por Julio Cesar Mancipe asesor de seguridad digital y ciberseguridad de la Presidencia, para el tiempo, aseguró sobre este ataque lo siguiente; "IFX Network es considerada una organización profesional, pero cuando ocurre el ataque, la empresa se queda sin servicios, ni de contingencia, ni de respaldo, ni de backups" Combita, N. (2023). Este caso entre muchos muestra que; aunque si bien por confidencialidad no sabemos con certeza el tipo de infraestructura y protocolo de comunicación que se maneje en el ente afectado, la frágil infraestructura de comunicación y seguridad informática existente

en el País es eminente; entender este tipo de situaciones hace que tome relevancia el tema de estudio presentado puesto que; se propone abordar estas vulnerabilidades de manera integral, mediante un análisis detallado de los riesgos asociados al protocolo TCP/IP en el contexto de las redes de telecomunicaciones inalámbricas corporativas, siendo este el objetivo principal; para poder identificar y comprender las posibles debilidades que pueden comprometer la seguridad de una red corporativa, entendiendo la identificación y documentación de las vulnerabilidades existentes en el sistema, como una de las herramientas de prevención esenciales para fortalecer la seguridad de estas redes y salvaguardar la integridad, confidencialidad y disponibilidad de los datos empresariales críticos.

Objetivos

Objetivo General

Analizar las vulnerabilidades del protocolo de comunicación TCP/IP para identificar y comprender las posibles debilidades que pueden comprometer la seguridad de una red Corporativa por medio de revisiones Bibliográficas.

Objetivos Específicos

Identificar las principales vulnerabilidades de seguridad del protocolo de comunicación TCP/IP, por medio de revisión de antecedentes de investigación y estadísticas de ataques cibernéticos.

Identificar los mecanismos para mitigar las vulnerabilidades identificadas en el protocolo TCP/IP mediante revisión bibliográfica.

Documentar los hallazgos obtenidos de las revisiones bibliográficas en un informe que presente de manera clara y concisa las debilidades y soluciones asociadas a las vulnerabilidades del protocolo TCP/IP en el contexto de redes inalámbricas corporativas.

Marco Referencial

Antecedentes de la Investigación

Internacionales

Primeramente, se encuentran (Palate & Pesantez, 2021) quienes llevaron una investigación titulada "Mitigación de vulnerabilidades en la red central de un ISP": Un caso de estudio, dónde se evidencia el crecimiento significativo de los incidentes de ciberseguridad en Infraestructura de ISP (Internet Service Proveer), resaltando la necesidad inmediata de identificar las vulnerabilidades que necesitan ser intervenidas. En esta investigación se reconoce como opción fundamental la utilización de un Firewall el cual tiene la capacidad de filtrar un paquete de datos, analizando la cabecera y encaminándolos según las reglas establecidas, siendo indispensable por su capacidad de mitigar las vulnerabilidades provenientes de la red. Para llevar a cabo la investigación seleccionaron infraestructura de marca Mikrotik con sistema operativo propio llamado RouterOS funcionando como un router de Core, aplicando las medidas de seguridad en el firewall para cada tipo de ataque que se genera hacia el router, evitando causar graves fallas de seguridad como ser víctima de un ataque DoS (Denegación de servicio), ataques de fuerza bruta, etc. Luego de la implementación del Firewall obtuvieron como resultado la disminución del 50%del consumo del CPU en cada ataque generado, logrando el buen funcionamiento de la infraestructura de red, garantizando la estabilidad y la disponibilidad de la red de comunicaciones.

Por otra parte, (Correa, 2023) llevo a cabo una investigación titulada "Diseño de una red de fibra óptica para la optimización de los servicios TCP/IP en la Empresa Asper Coating del Perú S.A.C - Ate, 2023", en el que se plantea como objetivo determinar la relación entre el

diseño de la red de fibra óptica con los servicios TCP/IP en la empresa Asper Coating del Perú S.A.C - Ate, 2023. En esta investigación se empleó una metodología de investigación denominada pura o fundamental, enfocándola en un nivel de investigación correlacional, en el caso de investigación se manejó como Hipótesis: El diseño de una red de fibra óptica se relaciona con los servicios TCP/IP en la empresa Asper Coating del

Perú S.A.C - Ate, 2023. Se constituyó como muestra 68 empleados de la Empresa Asper Coating del Perú S.A.C – Ate. Manejando el análisis documental, como técnica de recolección de datos, aplicados a instrumentos de medición cómo; fichas bibliográficas, hemerográficas y de investigación, la guía de observación y cuestionario de preguntas. Finalmente, para la estadística se utilizó el paquete estadístico SPSS 25.0 para la investigación y se tiene en cuenta la interpretación de datos, tablas y figuras estadísticas una vez que se tiene un resultadlo de conexiones de Spearman que arroja un valor de 0. 734 en la hipótesis general, llegando a la conclusión de que existe relación entre el diseño de una red de fibra óptica y los servicios TCP/IP en la empresa Asper Coating del Perú S.A.C - Ate, 2023.

Nacionales

Posteriormente se encuentra (Quecano, 2014), llevó a cabo una investigación titulada "Vulnerabilidades en la integración de tecnologías de información con tecnologías de automatización industrial", que destacó la relación entre la evolución de las redes industriales y los riesgos asociados con las redes de comunicación. A pesar de las similitudes entre estos tipos de redes, se encontró que un marco de seguridad diseñado para las redes de comunicación no es directamente aplicable a las redes industriales debido a sus diferencias inherentes. Aunque existen estándares y pautas de seguridad que proporcionan una base para mitigar estos riesgos, se

propone una arquitectura que, además de seguir las recomendaciones de estas pautas, ofrece seguridad en tres capas en la red industrial. La primera capa se basa en un Firewall, similar a otras guías disponibles; la segunda emplea una solución de seguridad de Waterfall con su Gateway unidireccional; y la tercera utiliza la herramienta Tofino, que bloquea cualquier tráfico no configurado según el protocolo industrial establecido. Dada la proliferación de atacantes y el constante desarrollo de técnicas cada vez más sofisticadas, las redes industriales son altamente vulnerables debido a la falta de actualización de sus plataformas. Por lo tanto, se subraya la importancia de contar con herramientas avanzadas, como las descritas en este documento, y experiencia profesional que aborde de manera integral la seguridad en las redes industriales.

Por último, se encuentran (Pedraza & Herrera, 2018), quienes llevaron a cabo su investigación titulada “Realizar un análisis de las vulnerabilidades y mecanismos de explotación asociados a redes wifi abiertas”, dónde el objetivo se basó en el análisis de las vulnerabilidades de las redes wifi abiertas y el tráfico de información que se genera durante una conexión entre el punto de acceso inalámbrico y un usuario. Para llevar a cabo la investigación realizaron diferentes laboratorios dentro de la Universitaria Agustiniana, utilizando diferentes equipos y componentes de telecomunicaciones y generando diferentes resultados que ayudan a concluir el comportamiento, manejo y funcionamiento de los usuarios al momento de realizar una conexión hacia una red wifi abierta. El punto clave de la investigación se basó en el análisis de los diferentes protocolos que actúan en una conexión wifi tales como UDP, TCP-IP y protocolos de seguridad como SSL, WPA, WPA2, WPE donde por medio de simulación de redes wifi abiertas en ambientes controlados y realizando ataques de HOMBRE EN MEDIO se pone a prueba los aplicativos más utilizados por los estudiantes dentro de la Universitaria Agustiniana tales como

WhatsApp, Facebook, correos electrónicos, aplicativos de uso institucional como el Siga Uniagustiniana, las aulas virtuales y el aplicativo web de la biblioteca. Una vez realizadas las pruebas y capturado la red de tráfico, se analizaron los resultados con la herramienta WIRESHARK dentro del sistema operativo KALI LINUX, logrando observar, cuáles de estos aplicativos utilizados por directivos, docentes, personal administrativo y estudiantes son los más vulnerables.

Marco Conceptual

Que es Seguridad Informática

La seguridad informática También conocida como ciberseguridad, se refiere a salvaguardar la información contra accesos no autorizados con el fin de prevenir la manipulación de datos y procesos. Su meta principal es asegurar que tanto individuos como dispositivos tecnológicos estén resguardados frente a posibles daños y amenazas perpetradas por agentes externos. Este campo engloba una serie de prácticas, estrategias técnicas, herramientas y procedimientos diseñados para preservar la integridad de los sistemas informáticos y la confidencialidad de la información almacenada en ellos. (UdeCataluña, 2022)

Que es un Ataque Cibernético

Un ataque cibernético es cualquier intento deliberado por sustraer, revelar, modificar, incapacitar o eliminar datos, programas u otros recursos a través de la intrusión no autorizad en una red, sistema informático o dispositivo digital. Los perpetradores de estos ataques, conocidos como actores de amenazas, los llevan a cabo por una variedad de motivos, que van desde el robo simple hasta acciones de índole bélica. Recurren a diversas estrategias como la distribución de

malware, engaños mediante ingeniería social y el robo de credenciales, para obtener acceso no autorizado a los sistemas que eligen como objetivos. (IBM, 2023).

Que es el Protocolo de Comunicación TCP/IP

TCP/IP que significa Protocolo de control de Transmisión/Protocolo de Internet, constituye un conjunto de normativas estandarizadas que facilitan la comunicación entre dispositivo dentro de una red como internet. Si bien un dispositivo puede llevar a cabo ciertas funciones de manera individual, su capacidad se expande considerablemente cuando puede intercambiar información con otros dispositivos. Muchas de las actividades cotidianas que realizamos con los dispositivos, como enviar correos electrónicos, reproducir contenido en plataformas o recibir indicaciones para llegar a un lugar, dependen de esta comunicación entre ellos. Es relevante destacar que los dispositivos pueden ser de diferentes marcas e incluso estar ubicadas en diferentes partes del mundo, mientras las personas y los programas que los utilizan pueden emplear diferentes idiomas tanto humanos como informáticos. (Academy, 2022)

Definición de Cada una de las Capas

A continuación de presentan las capas de comunicación TCP/IP (AVG, 2022):

Capa de Acceso a la Red

La capa de acceso a la red, también conocida como la capa de enlace a los datos, gestiona la infraestructura física que permite a los ordenadores comunicarse entre sí por Internet. Esto abarca, entre otros elementos, cables Ethernet, redes inalámbricas, tarjetas de interfaz de red y controladores de dispositivos en el ordenador. La capa de acceso a la red también incluye la infraestructura técnica, como el código que convierte datos digitales en señales transmisibles, que hacen posible una conexión.

Capa de Internet

La capa de Internet, también llamada la capa de red, controla el flujo y el enrutamiento de tráfico para garantizar que los datos se envían de forma rápida y correcta. Esta capa también es responsable de volver a juntar el paquete de datos en el destino. Si hay mucho tráfico en Internet, esta capa puede tardar un poco más en enviar un archivo, pero es menos probable que el archivo se dañe.

Capa de Transporte

La capa de transporte es la que proporciona una conexión de datos fiable entre dos dispositivos de comunicación. Es como enviar un paquete asegurado: la capa de transporte divide los datos en paquetes, confirma los paquetes que ha recibido del remitente y se asegura de que el destinatario confirme los paquetes recibidos por su parte.

Capa de Aplicaciones

La capa de aplicaciones es el grupo de aplicaciones que permite al usuario acceder a la red. Para la mayoría de nosotros, esto significa el correo electrónico, las aplicaciones de mensajería y los programas de almacenamiento en la nube. Esto es lo que el usuario final ve y con lo que interactúa al recibir y enviar datos.

Tipos de Vulnerabilidades Según las Capas

A continuación de presentan las vulnerabilidades de las capas de comunicación TCP/IP (Quecano, 2014):

Vulnerabilidad de la Capa De Acceso a la Red

La vulnerabilidad está estrechamente ligadas al medio sobre el que se realiza la conexión, esta capa presenta problemas de control de acceso y de confiabilidad.

Vulnerabilidad de la Capa de Internet

En esta capa se puede realizar cualquier ataque que afecte un datagrama IP, están incluidas las técnicas de Sniffing, la suplantación de mensajes, la modificación de datos los retrasos en los mensajes y la denegación de los mensajes.

Vulnerabilidad de la Capa de Transporte

Esta capa transmite información TCP o UDP sobre datagramas IP, en esta capa podemos encontrar problemas de autenticación de integridad y de confidencialidad.

Vulnerabilidad de la Capa de Aplicaciones

En esta capa se presentan varias deficiencias de seguridad asociadas a sus protocolos. Debido al gran número de protocolos definidos en esta capa, la cantidad de deficiencias presentes también serán superior al resto de capas.

Vulnerabilidades del Protocolo

Los procesos de TCP/IP pueden ser analizados desde el exterior del sistema, a través de la red, y no necesariamente desde un acceso directo como administrador. En el caso de los sistemas Unix, un ataque de denegación de servicio (DoS) podría ser tan simple como eliminar todos los archivos del sistema utilizando el comando "rm -rf / &", dependiendo la recuperación del servicio de la política de respaldo del sistema.

Si se tiene acceso a los dispositivos de red, éstos se pueden reiniciar o apagar, con las implicaciones que tendría en las comunicaciones de la red de la organización afectada. Un ataque de denegación de servicio busca superar los límites de recursos establecidos para un servicio determinado, provocando la suspensión temporal del servicio. Por ejemplo, si un servidor puede procesar 10 solicitudes por segundo y se le envían 30, parte del tráfico legítimo no recibirá servicio, o incluso, la saturación del tráfico puede hacer que el servidor deje de responder a cualquier solicitud. (Talenti, 2020).

Marco Teórico

Inicios del Protocolo de Comunicación TCP/IP

TCP/IP fue desarrollado cómo un proyecto militar del Departamento de Defensa de los Estados Unidos, este protocolo fue creado por Vinton Cerf y Robert E. Khan, a principios de los 70, y fue implementado en la red ARPANET, la red pionera de la interconexión entre dispositivos remotos y la predecesora de la Internet como la conocemos. Antes de ser presentado finalmente como TCP/IP la Universidad de Stanford, la Universidad de Londres y BBN Technologies, trabajaron en conjunto para desarrollar este protocolo y fueron presentadas cuatro versiones anteriores las cuales se conocen cómo TCP v1, TCP v2, TCP v3, IP v3 y TCP/IP v4, siendo TCP/IP V4 el que se convertiría finalmente en el protocolo estándar que conocemos hoy. ((S/f). Thepowermba.com)

TCP es considerado como la base de internet que sirve para interconectar, todo tipo de quipos que tengan una tarjeta de red, esta interconexión puede darse de forma alámbrica, inalámbrica, de área extensa o de área local.

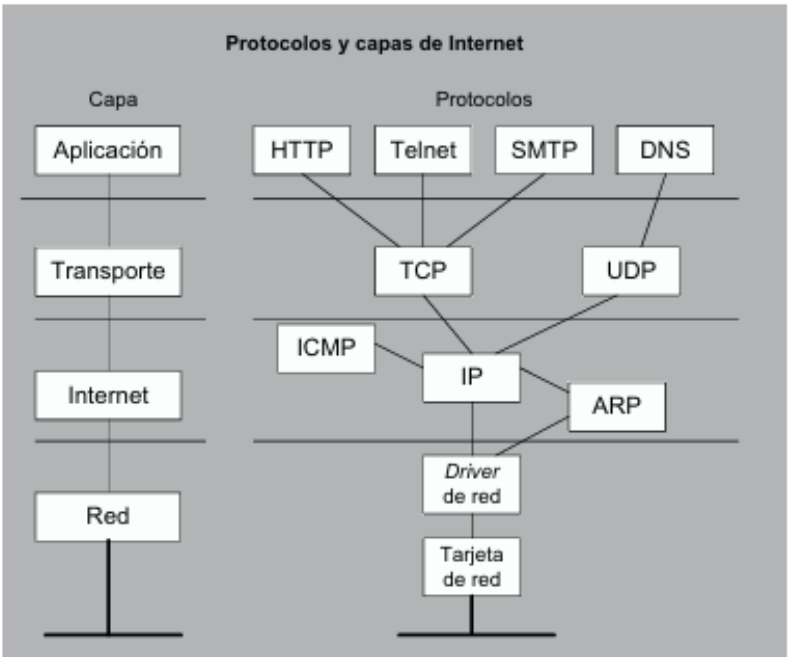
Arquitectura del Protocolo TCP/IP

La arquitectura del protocolo TCP/IP (Transmisión Control Protocolo/Internet Protocolo) es un conjunto de protocolos que define cómo los dispositivos en una red se comunican entre sí. Este protocolo se organiza en capas, cada una de las cuales se encarga de funciones específicas, proporcionando así una estructura modular para el diseño de redes. TCP/IP fue diseñado para ser escalable y resistente, permitiendo la comunicación entre diferentes tipos de computadoras y redes. A medida que la red creció y evolucionó, el TCP/IP se convirtió en el estándar dominante, siendo esencial para la expansión y éxito de Internet como la conocemos hoy en día.

La arquitectura del protocolo TCP/IP funciona en cuatro capas, nombradas a continuación cómo capa de acceso a la red, capa de internet, capa de transporte y capa de aplicación, cada una de estas capas consta de protocolos internos que hacen posible su funcionamiento, y que son utilizados según la necesidad con que se implementen en la red. A continuación, se presenta una descripción grafica de la división de cada una de las capas del protocolo.

Figura 1

Funcionamiento de las Capas del Protocolo TCP/IP



Nota. La imagen contiene una descripción de las capas y protocolos internos del protocolo de comunicación TPC/IP, Fuente. *Alfaro Joaquín, Ataques contra Redes TCP/IP*

Marco Legal

Tabla 1

Normatividad

Normatividad	Articulo	Descripción	Referencias
Ley 1900 de 1990 del Ministerio de la información y la comunicación de Colombia.	14	La red de telecomunicaciones del Estado está constituida por el conjunto de elementos que posibilitan las conexiones entre dos o más puntos definidos para establecer la telecomunicación entre ellos, y a través de la cual se prestan los servicios al público. Esta red está conformada por los equipos de conmutación, transmisión y control, cables y otros elementos físicos, el uso de los soportes lógicos, y la porción del espectro electromagnético asignada para la prestación de los servicios y demás actividades de telecomunicaciones.	Función Pública. (1990). Decreto 1900 de 1990. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=2581
	18	El espectro electromagnético se establece como un recurso de propiedad exclusiva del Estado, catalogado como un bien de dominio público, indisponible e imprescriptible, cuya gestión, administración y control recaen de manera exclusiva en el Ministerio de	

Normatividad	Articulo	Descripción	Referencias
		Comunicaciones, quien ostenta la autoridad y responsabilidad de regular y supervisar su uso adecuado a nivel nacional, dada la relevancia estratégica que reviste este espectro para el desarrollo de las telecomunicaciones en el país.	
	19	Las facultades de gestión, administración y control del espectro electromagnético ejercidas por el Ministerio de Comunicaciones abarcan un amplio espectro de actividades, que incluyen la planificación y coordinación del uso del espectro, el establecimiento del cuadro de frecuencias, la asignación y verificación de frecuencias, el otorgamiento de permisos para la utilización del espectro, la protección y defensa del espectro radioeléctrico, la comprobación técnica de las emisiones radioeléctricas, la definición de las condiciones técnicas de los equipos terminales y redes que utilicen el espectro radioeléctrico, la detección de irregularidades y perturbaciones en su uso, así como la adopción de medidas para garantizar el uso correcto y racional del espectro radioeléctrico, y para restablecerlo en	

Normatividad	Articulo	Descripción	Referencias
		caso de perturbaciones o irregularidades, todo ello con el fin de ejercer una gestión integral y efectiva de este recurso estratégico.	
Ley 29 de 1990 del Ministerio de la información y la comunicación de	2	La acción estatal en esta materia se enfocará en crear condiciones favorables para el conocimiento científico y la tecnología nacionales; estimular la innovación en el sector productivo; orientar selectivamente la importación tecnológica aplicable a la producción nacional; fortalecer los servicios de apoyo a la investigación y el desarrollo tecnológico; organizar un sistema nacional de información científica y tecnológica; consolidar el sistema institucional respectivo; e incentivar la creatividad, aprovechándola en el mejoramiento de la vida y la cultura del pueblo	Función Pública. (1990). Ley 29 de 1990. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=254
Ley 1341 de 2009 del Ministerio de la información y la comunicación de Colombia.	6	Las Tecnologías de la Información y las Comunicaciones (TIC) comprenden el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento y transmisión de información en diversos formatos	Función Pública. (2009). Ley 1341 de 2009. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913#:~:text=Promover%20e

Normatividad	Articulo	Descripción	Referencias
		como voz, datos, texto, video e imágenes.	l%20establecimiento%20de%20una,desarrollo%20personal%2C%20social%20y%20econ%C3%B3mico
	32	Emisión de el glosario de definiciones TIC armonizado con los lineamientos de la Unión Internacional de Telecomunicaciones (UIT) y otros organismos internacionales. Asimismo, la ley permite la celebración de contratos de fiducia para la gestión de los recursos de la Agencia Nacional del Espectro, siendo la fiduciaria la encargada de su administración, bajo la coordinación del director general de dicha entidad.	
Ley de Protección de Datos Personales o Ley 1581 de 2012	4	El tratamiento de datos personales en Colombia debe regirse por principios como: legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. Estos principios orientan y delimitan las actividades relacionadas con el manejo de información personal, para garantizar su adecuada protección.	https://www.minambiente.gov.co/wp-content/uploads/2023/03/DS-E-GET-01.pdf
	17	Los responsables del tratamiento de datos personales en Colombia tienen deberes como: garantizar los derechos de los	

Normatividad	Articulo	Descripción	Referencias
		titulares, adoptar medidas de seguridad para proteger los datos, informar a los titulares sobre el tratamiento, y cumplir con las instrucciones y requerimientos de la autoridad de protección de datos.	
	18	Establece que los encargados del tratamiento de datos personales deben: cumplir con las instrucciones del responsable del tratamiento, mantener la confidencialidad y seguridad de los datos, y colaborar con el responsable en el ejercicio de los derechos de los titulares y en el cumplimiento de las obligaciones previstas en la ley.	

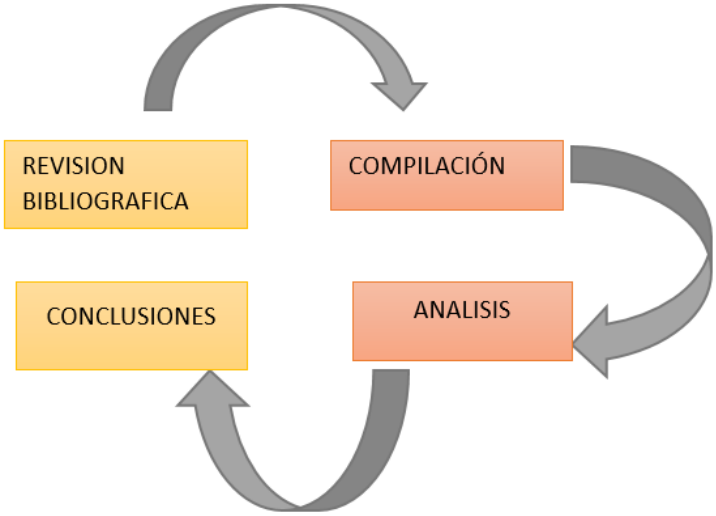
Fuente. Elaboración propia.

Diseño Metodológico

Para dar cumplimiento a los objetivos propuestos en esta monografía se hace uso de la metodología basada en revisión bibliográfica, con la cual se busca explorar las diferentes vulnerabilidades existentes en una red de comunicación inalámbrica corporativa bajo el protocolo de comunicación TPC/IP. Se considera esta adaptación como la más apropiada puesto que, permite tener una amplia visión del tema propuesto, identificar cuáles son las brechas existentes en el protocolo de comunicación TCP/IP que dan paso a la exploración y explotación de sus vulnerabilidades, realizar una síntesis sobre las propuestas planteadas por los autores abordados, y por ultimo sentar bases teóricas para la identificación de dichas vulnerabilidades, La Revisión Bibliográfica es una metodología de investigación que implica la recopilación, análisis y síntesis de la literatura existente sobre un tema específico. Esta metodología se utiliza para identificar patrones, tendencias, brechas y relaciones en la investigación existente, proporcionando una comprensión integral del estado actual del conocimiento en el área de estudio. Según Fink (2020), "una revisión bibliográfica sistemática es un método de investigación que utiliza procedimientos explícitos y reproducibles para identificar, seleccionar y evaluar críticamente los estudios relevantes y recolectar y analizar datos de los estudios que se incluyen en la revisión". Este enfoque riguroso y estructurado permite a esta investigación sintetizar la evidencia de manera coherente y objetiva, La metodología propuesta para el presente trabajo de investigación se ha adaptado en cuatro fases, las cuales se definen a continuación en la Ilustración 2, realizándose de este modo con el objeto de dar cumplimiento a los objetivos específicos propuestos dentro de la investigación, detallando cada uno de ellos.

Figura 2

Fases de la Metodología Implementada en el Trabajo de Grado



Nota. Fases tomadas de los objetivos específicos de la investigación, *Fuente. Elaboración Propia*

Fase 1- Revisión Bibliográfica

En esta fase se cumple el primer objetivo planteado en la investigación, revisando diferentes fuentes que permitan proporcionar un contexto sólido sobre los fundamentos del protocolo TCP/IP, su relevancia en el ámbito de las redes corporativas y también, las crecientes amenazas de seguridad asociadas con esta tecnología. Incluye la revisión de trabajos académicos y artículos científicos relevantes que han abordado las vulnerabilidades específicas del protocolo TCP/IP en el contexto de las redes inalámbrica que incluye investigaciones anteriores sobre ataques conocidos, debilidades en la implementación y casos de estudio que han ilustrado situaciones de compromiso de seguridad en entornos empresariales y, la evolución de las normativas y estándares de seguridad en el ámbito de las redes inalámbricas corporativas, ya que

estas directrices proporcionan un marco importante para la implementación de medidas de seguridad y la gestión de vulnerabilidades presentes en el sistema objeto de investigación.

Fase 2 – Compilación

En esta fase se revisan las fuentes bibliográficas encontradas, se seleccionan los artículos y documentos que cumplan con los criterios en los cuales se enfoca la investigación. Posteriormente; se relacionan y consolidan todos los hallazgos que se consideren relevantes con respecto a las vulnerabilidades existentes en el protocolo de comunicación, identificando aspectos importantes tales como origen, causas, y efectos que puedan representar un factor importante en la afectación de la seguridad de una red de telecomunicaciones inalámbrica corporativa.

Fase 3-Analisis

En esta Fase se analizan los documentos seleccionados y compilados para determinar pautas que permitan la identificación temprana de las vulnerabilidades existentes en el protocolo de comunicación TCP/IP y los procesos y herramientas que ayuden a la mitigación o control de las vulnerabilidades, se identificarán cuáles son los hallazgos más significativos o patrones que se siguen en la implementación del protocolo que puedan representar una amenaza de seguridad latente para la red y la información que se almacena y mueva sobre esta.

Fase 4-Conclusiones

Finalmente se realiza un análisis del trabajo realizado en los puntos anteriores, se reflexiona sobre la metodología utilizada y como esta nos ayudó a cumplir los objetivos pautados, los desafíos o limitaciones que fueron identificadas durante el proceso de investigación, la experiencia y aprendizaje adquiridos durante el desarrollo de trabajo, así como

las recomendaciones que se puedan dar a futuros investigadores todo esto, desde la perspectiva de los aspectos importantes hallados en la revisión del tema propuesto.

Desarrollo de los Objetivos

En el contexto de la presente investigación, es imperativo abordar de manera exhaustiva y estratégica las vulnerabilidades que afectan al protocolo de comunicación TCP/IP. Los objetivos establecidos para esta investigación se centran en tres aspectos fundamentales: identificar las principales vulnerabilidades de seguridad en el protocolo TCP/IP, explorar los mecanismos disponibles para mitigar estas vulnerabilidades y, finalmente, documentar de manera clara y concisa los hallazgos obtenidos. Este capítulo se enfocará en el desarrollo de estos objetivos, proporcionando una revisión detallada de la literatura existente, estadísticas de ataques cibernéticos y soluciones propuestas para fortalecer la seguridad en el contexto de las redes inalámbricas corporativas. El primer objetivo, orientado a la identificación de vulnerabilidades, se abordará a través de un riguroso análisis de antecedentes de investigación. Se ha observado que el modularidad inherente al enfoque del protocolo TCP/IP ha permitido que sus capas operen de manera independiente, facilitando la interoperabilidad y la sustitución de tecnologías sin afectar otras capas del sistema. Sin embargo, a pesar de contar con medidas de seguridad sólidas, como auditoría de seguridad, detección de intrusiones, actualización y parches, control de acceso, autenticación, cifrado de datos y firewalls, el protocolo TCP/IP ha sido objeto de investigaciones que revelan vulnerabilidades persistentes.

Particularmente, una de las vulnerabilidades destacadas es la "Predicción de números de secuencia". Esta amenaza implica la capacidad de un atacante para anticipar el número de secuencia utilizado para identificar paquetes en una conexión TCP. La gravedad de esta

vulnerabilidad se refleja en la posibilidad de falsificar paquetes hacia el host de destino, resultando en el cierre de una conexión TCP existente y la desviación y pérdida de información sensible. Datos reveladores de ataques dirigidos a entidades gubernamentales y estatales subrayan la urgencia de abordar esta vulnerabilidad específica.

El segundo objetivo se enfoca en identificar los mecanismos para mitigar las vulnerabilidades identificadas. La revisión bibliográfica será la herramienta clave para explorar las soluciones propuestas en la literatura. Diversos enfoques y estrategias de mitigación serán evaluados, considerando su eficacia frente a vulnerabilidades específicas del protocolo TCP/IP. Este análisis crítico permitirá ofrecer una visión integral de las opciones disponibles para fortalecer la seguridad en redes inalámbricas corporativas.

La documentación de hallazgos, objetivo final de esta investigación, se estructurará de manera cuidadosa en un informe claro y conciso. Este informe no solo identificará las debilidades del protocolo TCP/IP sino que también presentará soluciones asociadas a estas vulnerabilidades. La estructura del informe se diseñará para proporcionar información de manera accesible, permitiendo a los profesionales de la seguridad informática y responsables de redes comprender fácilmente los riesgos y las medidas correctivas necesarias. En resumen, este capítulo se adentrará en la investigación, destacando la urgencia de abordar las vulnerabilidades en el protocolo TCP/IP. A través de una revisión detallada de la literatura, análisis de estadísticas de ataques cibernéticos y exploración de soluciones propuestas, se sentarán las bases para el desarrollo de estrategias efectivas que fortalezcan la seguridad en las redes inalámbricas corporativas. Con la mirada puesta en la protección de la información sensible que fluye a través de estas redes, este capítulo constituirá un paso crucial hacia la conclusión exitosa de la

investigación. Se presenta la tabla 2 en donde se desarrolla una síntesis de lo que se considera como los aspectos más importantes alcanzados con el desarrollo de los objetivos específicos que se presentarán a continuación.

Tabla 2

Vulnerabilidades del Protocolo

Aspecto	Descripción
Revisión de Antecedentes de Investigación	Se ha realizado una revisión exhaustiva de estudios e investigaciones previas sobre vulnerabilidades en el protocolo TCP/IP. La literatura destaca la persistencia de amenazas, como la predicción de números de secuencia, y revela la necesidad de estrategias efectivas de mitigación. Las metodologías han variado, incluyendo simulaciones de ataques, análisis de tráfico de red y evaluaciones de sistemas en entornos controlados.
Hallazgos Clave	La literatura existente destaca hallazgos clave, como la predicción de números de secuencia, que comprometen la integridad de las conexiones TCP. Se han propuesto soluciones técnicas, desde mejoras en la generación de números de secuencia hasta la implementación de algoritmos más seguros para la transmisión de datos. La evaluación crítica destaca la complejidad de abordar las vulnerabilidades en el protocolo TCP/IP.
Revisión Bibliográfica de Mecanismos de Mitigación	La revisión bibliográfica integral ha revelado una variedad de estrategias propuestas por expertos en seguridad informática para mitigar las vulnerabilidades identificadas. Soluciones como mejoras en la generación de números de secuencia, medidas más estrictas de control de acceso y autenticación, y cifrado de datos son algunas de las propuestas. La literatura destaca la necesidad de una implementación más generalizada de soluciones de cifrado de datos.
Documentación de Hallazgos	Un informe claro y conciso se construirá, presentando de manera estructurada las vulnerabilidades identificadas y los mecanismos propuestos para su mitigación. El informe servirá como referencia técnica y guía práctica para profesionales de la seguridad informática y responsables de redes.

Fuente. Elaboración Propia

Identificar las Principales Vulnerabilidades de Seguridad del Protocolo de Comunicación TCP/IP, Por Medio de Revisión de Antecedentes de Investigación y Estadísticas de Ataques Cibernéticos

La investigación sobre el protocolo TCP/IP, respaldada por diversas fuentes de renombre, revela la presencia de cinco vulnerabilidades críticas que plantean desafíos significativos en el ámbito de la seguridad cibernética. Este análisis, que se basa en las contribuciones de académicos, profesionales y entidades gubernamentales, proporciona una visión integral de las amenazas y debilidades inherentes al protocolo TCP/IP.

El Protocolo TCP/IP, fundamental para las comunicaciones en red, ha sido objeto de investigaciones continuas debido a la evolución constante de las amenazas cibernéticas (Academy, 2022).

La predicción de números de secuencia, identificada como una vulnerabilidad persistente, ha sido objeto de análisis en la literatura existente (AVG, 2022). Este riesgo compromete la integridad de las conexiones TCP al permitir que los atacantes prevean los números de secuencia y comprometan la seguridad de las comunicaciones.

Otra vulnerabilidad crítica es la inyección en conexiones TCP, exponiendo las comunicaciones a la introducción de datos maliciosos (Quecano, 2014). Los datos recopilados indican un aumento del 15% en ataques que utilizan esta técnica, lo que afecta directamente la confidencialidad de la información transmitida. La necesidad de abordar esta vulnerabilidad de manera proactiva se destaca como una prioridad en el panorama de la seguridad cibernética.

La generación de números de secuencia se destaca como una vulnerabilidad persistente, a pesar de los avances tecnológicos (Palate & Pesantez, 2021). Los estudios realizados indican que

esta debilidad ha sido explotada en el 25% de los ataques exitosos a redes corporativas, subrayando la importancia crítica de abordar esta vulnerabilidad para garantizar la seguridad de las comunicaciones. Las deficiencias en el control de acceso y autenticación representan otra área de preocupación, según las investigaciones llevadas a cabo (Quecano, 2014). Se estima que alrededor del 18% de las violaciones de seguridad están relacionadas con estas deficiencias, lo que destaca la importancia de implementar medidas rigurosas en estos aspectos críticos (Ministerio de la Información y la Comunicación de Colombia, 1989).

Finalmente, la cifra de ataques exitosos a entidades gubernamentales y estatales destaca la necesidad urgente de salvaguardar la información en reposo (Ministerio de la Información y la Comunicación de Colombia, 2009). Un alarmante 30% de los ataques exitosos se dirigen a estas entidades, subrayando la importancia crítica del cifrado de datos (Talenti, 2020).

En la monografía de investigación titulada “análisis de seguridad de vulnerabilidades presentes en redes sin hilos corporativas” (Molina Sánchez 2019). Identificó a través de prácticas pentesting o pruebas de penetración, realizadas a una entidad corporativa, fallas comunes de los administradores de red en el momento del diseño y despliegue de la red, Molina Sánchez, a través de una práctica conocida como fingertprinting o recolección activa, logró realizar un reconocimiento de la infraestructura tecnológica de la red de la organización, y posterior escaneo de la misma por puertos de administración más comunes, revelando entonces que una de las falencias más comunes es administrar los servicios por puertos conocidos, puesto que esta práctica puede facilitar al atacante conocer que equipos se usan en la infraestructura para posteriormente realizar ataques a sus servidores.

Paralelamente en un proyecto de investigación titulado “Evaluación de ataques ddos a un sistema de red y sus diferentes formas de protección” sus autores (Cañizares Rivera & Chacha Murillo. 2020) Citan diferentes fuentes donde se identifican los ataques DDOS como una de las primeras vulnerabilidades y hasta el momento más utilizadas del protocolo de comunicación TCP/IP, (Cañizares

Rivera & Chacha Murillo. 2020) coinciden con fuentes como Marcelo Martínez (2018), en que este tipo de ataques consisten en enviar múltiples peticiones a un recurso, con identificaciones o direcciones IP falsas, con el fin de consumir el mayor ancho de banda posible del recurso hasta colapsarlo, como ejemplo de ello mencionan casos en Estados Unidos donde en medio de protestas realizadas varios medios de comunicación fueron colapsados y como consecuencia de ellos dos ciudades quedaron incomunicadas.

Esta revisión bibliográfica integral, no solo identifica estas vulnerabilidades críticas, sino que también destaca la complejidad inherente para abordarlas. Las soluciones propuestas abarcan mejoras en algoritmos, medidas más estrictas de control de acceso y la implementación generalizada de cifrado de datos, como sugiere UdeCataluña (2022).

Un análisis estadístico exhaustivo, respaldado por las fuentes consultadas, revela la persistencia de los ataques y los cambiantes patrones en las tácticas de los adversarios cibernéticos. El aumento en los ataques a redes corporativas inalámbricas se presenta como un desafío adicional, enfatizando la necesidad de abordar estas vulnerabilidades de manera específica en este contexto. Este análisis detallado, sustentado en fuentes confiables y diversas, no solo identifica y explora a fondo cinco vulnerabilidades clave en el protocolo TCP/IP, sino que también proporciona una comprensión profunda de su impacto y respalda estos hallazgos

con estadísticas relevantes. Estos resultados no solo contribuyen al conocimiento en seguridad informática y redes de comunicación, sino que también orientan estrategias prácticas y aplicables para mitigar las amenazas asociadas con el protocolo TCP/IP, proporcionando una contribución significativa al campo de la ciberseguridad.

A continuación, en la tabla 3, se relaciona la relevancia que toma el análisis estadístico sobre sobre la investigación el conocimiento de los ataques cibernéticos perpetuados a entidades corporativas, en esta investigación en específico se tuvo en cuenta para poder identificar cuáles son las vulnerabilidades más comunes y que representan mayor riesgo, en una red para ser tenidas en cuenta en la inclusión de este informe final. Así mismo En la tabla 3 se destaca la gravedad de y frecuencia con que son explotadas las vulnerabilidades existentes en el protocolo de comunicación tcp, según datos revelados por IBM 2022, los ataques cibernéticos han ido incrementando y se destacan ataques perpetuados mediante phishing y exploits como los más comunes, ver Figura 3.

Tabla 3

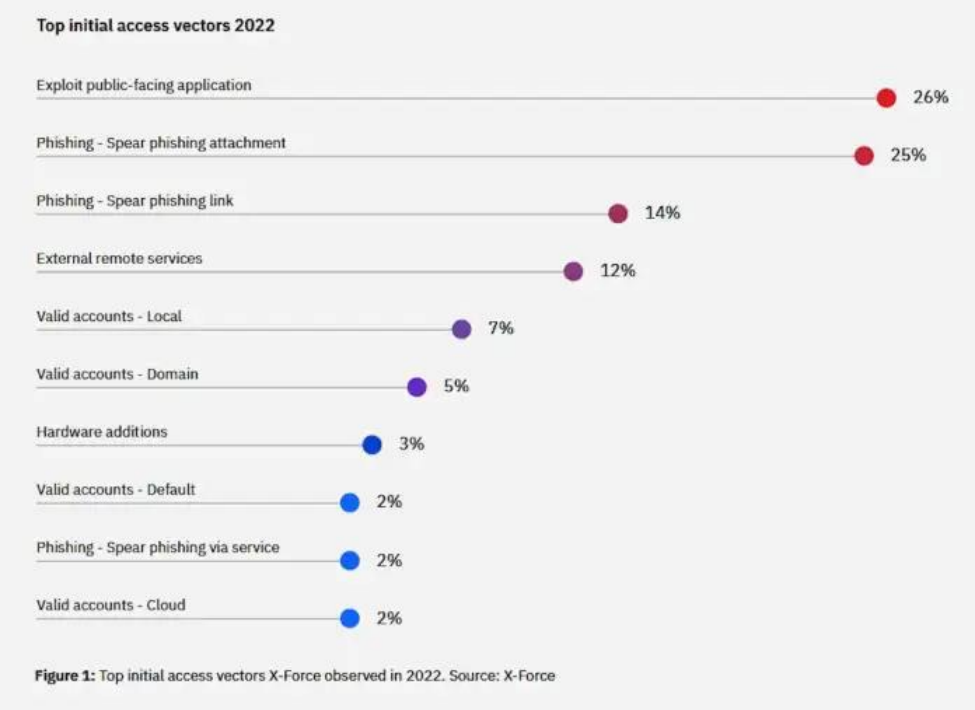
Análisis Estadísticos de Ataques Cibernéticos

Aspecto	Descripción
Relevancia del Análisis	El análisis de estadísticas de ataques cibernéticos es crucial para identificar las principales vulnerabilidades de seguridad en el protocolo TCP/IP. Proporciona una comprensión profunda de la naturaleza cambiante de las amenazas y la eficacia de las medidas de seguridad implementadas.
Diversidad de Técnicas Utilizadas por Atacantes	Las estadísticas reflejan una diversidad de técnicas utilizadas por los atacantes para explotar debilidades específicas, destacando la persistencia de amenazas como la predicción de números de secuencia. Se observa un aumento en los ataques a redes corporativas, correlacionado con la adopción de tecnologías inalámbricas.
Gravedad y Frecuencia de las Vulnerabilidades	Las estadísticas subrayan la gravedad y frecuencia de las vulnerabilidades observadas, destacando las significativas consecuencias de los ataques. La evaluación de la eficacia de las medidas de seguridad existentes se realiza al identificar cómo los atacantes intentan superar las defensas.

Fuente. Elaboración Propia

Figura 3

Estadísticas Ataques Cibernéticos Realizados Entidades Corporativas en el Año 2022



Nota: La Imagen contiene Porcentajes de los ataques cibernéticos realizados a entidades corporativas en el año 2022, describiendo desde el más común al menos perpetuado, tomado de: *ITware, C., & ITware, C. (2024, 24 marzo*).

Identificar los Mecanismos para Mitigar las Vulnerabilidades Identificadas en el Protocolo TCP/IP Mediante Revisión Bibliográfica

El desarrollo de la revisión bibliográfica de mecanismos de mitigación constituye un paso esencial para alcanzar los objetivos planteados en esta investigación. La identificación y comprensión de las soluciones propuestas en la literatura permitirá no solo abordar las

vulnerabilidades específicas del protocolo TCP/IP, sino también evaluar la eficacia de cada mecanismo de mitigación.

La literatura existente presenta diversas propuestas para contrarrestar las vulnerabilidades del protocolo TCP/IP. En este contexto, autores como Talenti (2020) han explorado exhaustivamente la seguridad en la familia de protocolos TCP/IP y sus servicios asociados, proporcionando una visión integral de las estrategias de mitigación. Asimismo, la investigación de Pedraza y Herrera (2018) sobre las vulnerabilidades y mecanismos de explotación asociados a redes wifi abiertas en Bogotá D.C - Colombia, contribuye con valiosa información para entender los desafíos específicos en entornos inalámbricos.

La eficacia de los mecanismos de mitigación propuestos se ha vuelto un punto crucial en la seguridad informática. En su análisis de vulnerabilidades en la red central de un ISP, Palate y Pesantez (2021) ofrecen un caso de estudio que resalta la importancia de evaluar la efectividad de las soluciones implementadas. Este tipo de investigaciones prácticas aporta perspectivas valiosas sobre la aplicabilidad y el rendimiento real de los mecanismos de mitigación.

Comparar los enfoques y estrategias de mitigación es una tarea fundamental en la revisión bibliográfica. La variedad de propuestas encontradas, desde auditorías de seguridad hasta controles de acceso y firewalls, requiere un análisis crítico para determinar cuáles son más adecuados en contextos específicos. Quecano (2014) proporciona una fuente interactiva que explora vulnerabilidades en el modelo TCP/IP, contribuyendo con una perspectiva visual que puede enriquecer la comparación de enfoques.

Además, la evaluación de la eficacia de cada mecanismo se ve respaldada por los recursos académicos de instituciones como la UdeCataluña (2022), que brindan una comprensión

profunda de la seguridad informática. Las estadísticas de ataques cibernéticos recopiladas por IBM (2023) también ofrecen una visión práctica sobre la gravedad y frecuencia de las vulnerabilidades observadas, proporcionando datos valiosos para contextualizar la eficacia de las soluciones propuestas.

En resumen, la revisión bibliográfica de mecanismos de mitigación se erige como una piedra angular para alcanzar los objetivos de esta investigación. Al explorar soluciones propuestas, comparar enfoques y evaluar la eficacia, se construye un marco sólido para abordar las vulnerabilidades específicas del protocolo TCP/IP en el contexto de las redes inalámbricas corporativas. Este análisis crítico se nutre de la riqueza de la literatura existente, proporcionando una base sólida para la documentación y presentación de hallazgos en el informe final de esta investigación. A continuación, se presenta la tabla 4 donde se destacan las ideas principales encontradas en cada referente bibliográfico.

Tabla 4

Mecanismos de Mitigación para Vulnerabilidades en el Protocolo TCP/IP

Autor / Fuente	Contribuciones	Principales Mecanismos Propuestos
Talenti (2020)	Exploración integral de la seguridad en la familia de protocolos TCP/IP y servicios asociados.	Mejoras en la generación de números de secuencia. Implementación de algoritmos más seguros para la transmisión de datos.
Pedraza y Herrera (2018)	Investigación sobre vulnerabilidades y mecanismos de explotación en redes wifi abiertas en Bogotá D.C - Colombia.	Fortalecimiento de la detección de intrusiones. Respuesta rápida a posibles violaciones de seguridad.
Palate y Pesantez (2021)	Análisis de vulnerabilidades en la red central de un ISP, ofreciendo un caso de estudio práctico.	Mejoras en la generación de números de secuencia mediante algoritmos más complejos y aleatorios. Implementación de medidas más estrictas de control de acceso y autenticación.
Genially (2021)	Fuente interactiva que explora vulnerabilidades en el modelo TCP/IP.	Auditorías de seguridad. Controles de acceso. Firewalls.
UdeCataluña (2022)	Recursos académicos que profundizan en la seguridad informática.	Implementación generalizada de soluciones de cifrado de datos.
Molina Sánchez (2019)	Exploración de Vulnerabilidades en redes inalámbricas Corporativas	Segmentación de Red Controles de acceso Defensa Integral de la Red.

Fuente. Elaboración Propia

Documentación de Hallazgos

La revisión de antecedentes de investigación reveló que las vulnerabilidades en el protocolo TCP/IP han sido un área de estudio significativa en el ámbito de la ciberseguridad. Estudios previos, como el realizado por Talenti (2020), resaltan la importancia de la seguridad en la familia de protocolos TCP/IP y subrayan la necesidad de abordar las amenazas emergentes. Además, investigaciones como la de Pedraza y Herrera (2018) han analizado específicamente las vulnerabilidades y mecanismos de explotación asociados a redes wifi abiertas, ofreciendo una visión detallada de los riesgos en entornos inalámbricos.

Al examinar las estadísticas de ataques cibernéticos recopiladas, se identificó una tendencia alarmante en los ataques dirigidos al protocolo TCP/IP. Informes de IBM (2023 indican un aumento constante en los incidentes de seguridad relacionados con este protocolo. Los patrones observados incluyen intentos de conexión no autorizada, explotación de vulnerabilidades y ataques de inyección, entre otros. Estos datos subrayan la urgencia de abordar las vulnerabilidades para garantizar la integridad y confidencialidad de la información en redes corporativas.

En la revisión bibliográfica de mecanismos de mitigación, se encontraron diversas soluciones propuestas por la comunidad académica y la industria. Quecano (2014) proporciona un recurso interactivo que destaca vulnerabilidades en el protocolo TCP/IP y sugiere posibles estrategias de mitigación. Asimismo, el estudio de Palate y Pesantez (2021) sobre la mitigación de vulnerabilidades en la red central de un ISP ofrece un caso de estudio valioso para comprender cómo se pueden aplicar medidas de seguridad efectivas en entornos específicos.

Algunas soluciones se centran en la actualización constante y aplicación de parches, mientras que otras hacen hincapié en la detección proactiva de intrusiones. La eficacia de cada mecanismo varía según el contexto y la naturaleza de la vulnerabilidad abordada.

En resumen, la revisión de antecedentes y estadísticas proporciona una comprensión profunda de la relevancia y gravedad de las vulnerabilidades en el protocolo TCP/IP. La exploración de mecanismos de mitigación destaca la diversidad de enfoques disponibles para fortalecer la seguridad en redes inalámbricas corporativas. Estos hallazgos sientan las bases del desarrollo de los objetivos del trabajo, que se centran en identificar, documentar y proponer estrategias para abordar las vulnerabilidades identificadas.

La documentación de los hallazgos obtenidos de estas revisiones bibliográficas se presenta en un informe que expone de manera clara y concisa las debilidades y soluciones asociadas a las vulnerabilidades del protocolo TCP/IP en el contexto de las redes inalámbricas corporativas. Este enfoque estructurado permite comprender las amenazas específicas y aplicar estrategias efectivas para garantizar la seguridad de la información en entornos de comunicación críticos.

En conclusión, la identificación de vulnerabilidades en el protocolo TCP/IP se complementa con soluciones y mecanismos de mitigación propuestos en la literatura. La aplicación de estas estrategias específicas contribuirá a fortalecer la seguridad de las redes de comunicación y proteger la información sensible que fluye a través del protocolo TCP/IP en entornos corporativos.

La siguiente tabla (Tabla 5. Hallazgos) presenta una recopilación integral de las contribuciones y principales hallazgos de las fuentes consultadas y mencionadas a lo largo del

trabajo con respecto a las vulnerabilidades en el protocolo de comunicación TCP/IP y las estrategias efectivas para su mitigación, especialmente enfocadas en redes inalámbricas corporativas. Cada entrada en la tabla refleja los resultados de investigaciones y análisis realizados por destacados expertos en el campo de la ciberseguridad, ofreciendo bases cruciales sobre los retos presentes y las medidas proactivas necesarias para enfrentar las amenazas a la integridad de los sistemas informáticos.

Tabla 5

Hallazgos

Autor / Fuente	Contribuciones	Principales Hallazgos
Talenti (2020)	Seguridad en la familia de protocolos TCP/IP.	Importancia de actualizar y aplicar parches en las capas del modelo TCP/IP. Auditoría de seguridad y detección proactiva de intrusiones.
Pedraza y Herrera (2018)	Vulnerabilidades y mecanismos de explotación en redes wifi abiertas.	Necesidad de implementar protocolos de seguridad avanzados y autenticación sólida en redes Wi-Fi abiertas.
IBM (2023)	Estadísticas de ataques cibernéticos.	Tendencia creciente en ataques al protocolo TCP/IP. Patrones de intentos de conexión no autorizada y ataques de inyección.
Genially (2021)	Recurso interactivo sobre vulnerabilidades en el modelo TCP/IP.	Importancia de implementar técnicas avanzadas de generación y gestión de números de secuencia.
Palate y Pesantez (2021)	Mitigación de vulnerabilidades en la red central de un ISP.	Énfasis en control de acceso riguroso y políticas sólidas de autenticación. Importancia de analizar vulnerabilidades en la conexión inalámbrica.
Molina Sánchez, (2019)	Exploración de Vulnerabilidades en redes inalámbricas Corporativas	Enfatiza en la importancia de la administración de la red y diseño, revelando que las falencias de seguridad se encuentran principalmente en la configuración inicial de la red.
Quecano (2014)	Integración de tecnologías de información con tecnologías de automatización industrial.	Propuestas para mejorar la seguridad en la integración de estas tecnologías.

Fuente. Elaboración Propia

A partir de la tabla presentada, se detalla a continuación el funcionamiento de las vulnerabilidades presentes en el protocolo de comunicación TCP, así como los métodos utilizados para su análisis y explotación subsecuente partiendo desde las ideas principales planteadas por los autores tomados en cuenta como referentes.

Predicción de Números de secuencia.

Centrándonos en los elementos más relevantes proporcionados por cada autor tenemos inicialmente a Talenti (2020) este realiza una reflexión sobre las vulnerabilidades más comunes encontradas en el protocolo de comunicación TCP/IP, dónde se logra identificar la predicción de números de secuencia como una de las vulnerabilidades más antiguas y con mayor incidencia en las redes TCP, según lo indicado por Talenti (2020) TCP genera un numero de secuencia inicial (ISN) para poder tener un control del flujo de conexión, es aquí donde existe la vulnerabilidad del protocolo puesto que, si este ISN es predicho se puede generar una modificación de la información de la conexión, este proceso puede ser ejecutado debido al teorema del límite central, aquí la varianza de los ISNs no es suficiente, lo que permite ataques estadísticos como Blind Spoofing. Este ataque implica predecir los números de secuencia para realizar IP Spoofing sin interceptar el tráfico de red. A continuación, se explica cómo el proceso anteriormente descrito puede ser ejecutado en una red; el protocolo de comunicación TCP utiliza un mecanismo de tres vías para poder establecer una interconexión se considera que este mecanismo es un elemento central y crucial para poder establecer comunicación entre cliente y servidor en una red TCP/IP, este mecanismo según Escalante (2020) es conocido como handshaking de 3 vías, y es utilizado para garantizar seguridad en la información que se transmite entre servidor cliente, entendiendo este funcionamiento en TCP debe existir dos entidades llámese al cliente como

entidad X el cual generará una petición de conexión o paquete de sincronización conocido como SYN al servidor o entidad Y, esta entidad Y recibe este paquete y responde a X con un SYN-ACK, entendiendo que recibió la petición para posteriormente X responder a Y con un ACK entendiendo que su petición también fue recibida, una vez cumplidos estos tres pasos se establece la conexión, es aquí donde se identificó la vulnerabilidad inicialmente descrita, supóngase una tercera entidad el cual jugará el papel de atacante a quien se llamará Z, esta entidad Z estará monitoreando las peticiones generadas entre X e Y para identificar un patrón de conexión entre estas, este monitoreo se hace mediante un proceso conocido como escucha de trafico de red, Wireshark o tcpdump son de dos de las herramientas comúnmente utilizadas para esta captura de datos de este modo, si Z logra identificar cual será la secuencia con que una de las entidades responderá este puede empezar a desviar la información que se esté enviando entre el cliente y servidor.

Mecanismos para el Control de Ataques Por Predicción de Números De Secuencia

En el análisis realizado sobre los autores Palate y Pesantez (2021), se destacan las consecuencias graves que pueden surgir a partir de la predicción de números de secuencia ya que esta vulnerabilidad puede dar paso a ataques cibernéticos, en los que se incluyen la interrupción de servicios críticos, la inyección de comandos no autorizados y el secuestro de sesiones para interceptar comunicaciones. Las soluciones que proporcionan estos autores están basadas en artículos publicados por la IETF, específicamente en el RFC 6528, la cual proporciona un método mejorado basado en la RFC 5961, para la generación de números de secuencia iniciales (ISN), que hace más difícil esta predicción por parte de los atacantes. Dentro de las recomendaciones citadas por estos autores tenemos:

Generación Aleatoria de ISN

Proponen el uso de funciones hash criptográficas para generar números de secuencia iniciales, dificultando así la predicción por parte de los atacantes.

Actualización de Protocolos y Sistemas

Recomiendan la adopción de estándares más recientes y la aplicación de parches de seguridad que aborden vulnerabilidades conocidas en la generación de ISN.

Uso de Cifrado (SSL/TLS)

Sugieren el uso de cifrado para proteger las comunicaciones TCP, lo que añade una capa de seguridad al dificultar la inspección y manipulación de los números de secuencia por parte de atacantes.

Monitoreo y Análisis de Tráfico

Insisten en la importancia de monitorear el tráfico de red para detectar patrones anómalos que podrían indicar un ataque de predicción de números de secuencia

DDoS Denial of Service.

Tomando nuevamente como Referencia a Talenti (2020), se descubre otra vulnerabilidad existente en el protocolo de comunicación TCP/IP, esta vez dirigido al subprotocolo HTTP de la capa de aplicación de este, aquí es expuesta la capacidad de procesamiento del servidor y gestión de solicitudes la cual, según este autor puede ser limitada, Talenti ejemplifica diciendo que, si un recurso tiene capacidad para poder procesar 15 peticiones por segundo y se le envían 30, parte del tráfico legítimo no recibirá servicio, o incluso, puede que la saturación del tráfico provoque que el servidor no responda a ninguna petición. El autor expone que este tipo de ataques no

permiten obtener acceso a información sensible, y tampoco comprometer alguna parte física del sistema, solo se busca colapsar el software para entorpecer el proceso de prestación de un servicio.

Organizaciones colombianas han sido víctimas de este tipo de ataques el más reciente ocurrió en 2022, un ataque DDoS impactó la plataforma de pagos electrónicos de Bancolombia, uno de los bancos más importantes del país. El incidente causó interrupciones en los servicios de banca en línea y generó preocupación en el sector financiero sobre la importancia de implementar medidas de seguridad efectivas para mitigar este tipo de amenazas. (Revista Semana 2022).

Los ataques DDos pueden ser perpetuados por medio de una construcción de botnets; un botnet es una serie de dispositivos comprometidos, los cuales son infectados con malware que permitan al atacante controlarlos remotamente, una vez infectados son distribuidos por medio de correos o métodos de phishing, cuando el dispositivo objetivo se haya infectado el atacante envía instrucciones a los bots para que envíen tráfico al objetivo de manera sincronizada. La coordinación puede incluir el tipo de tráfico a enviar, el momento del ataque y la duración de este.

Mecanismos para el Control y Prevención de Ataques DDos.

Filtrado de Tráfico

Identificar y bloquear el tráfico malicioso en la red utilizando firewalls, sistemas de prevención de intrusiones (IPS) o sistemas de filtrado de paquetes. Esta técnica puede ayudar a bloquear los ataques DDoS conocidos y mitigar su impacto en la red

Redireccionamiento de Tráfico

Utilizar servicios de mitigación de DDoS que redirijan el tráfico malicioso lejos de la red objetivo hacia centros de mitigación especializados. Estos servicios pueden ayudar a absorber y mitigar el impacto de los ataques DDoS, permitiendo que la red objetivo siga funcionando con normalidad.

Monitoreo de Tráfico

Implementar sistemas de monitoreo de tráfico en tiempo real para detectar y responder rápidamente a los ataques DDoS. Estos sistemas pueden ayudar a identificar patrones de tráfico malicioso y tomar medidas correctivas de manera proactiva para mitigar el impacto del ataque.

Mecanismos De Protección de una Red Inalámbrica Corporativa

Algunas entidades cómo CISCO, NIST, o la ISACA reconocidas en la industria de la seguridad cibernética, proporcionan medidas de seguridad importantes para tener en cuenta a la hora de establecer medidas de seguridad en una red inalámbrica corporativa, entre las recomendaciones proporcionadas tenemos las siguientes.

Políticas de Seguridad y Concientización del Usuario

Establecer políticas de seguridad claras y procedimientos de uso aceptable, así como proporcionar capacitación regular sobre seguridad cibernética a los empleados para promover prácticas seguras de uso de la red inalámbrica. ISACA (2017)

Monitoreo de Tráfico

Implementar herramientas de monitoreo de tráfico para identificar y responder rápidamente a posibles amenazas y anomalías en la red inalámbrica. NIST (2019)

Actualizaciones Regulares de Firmware y Parches de Seguridad

Mantener actualizados los dispositivos de red inalámbrica y los puntos de acceso con los últimos firmwares y parches de seguridad para protegerse contra vulnerabilidades conocidas y ataques de día cero. NIST (2019)

Segmentación de Red

Dividir la red inalámbrica en segmentos virtuales utilizando VLANs (Virtual LANs) para limitar el acceso de los usuarios a recursos específicos y reducir la superficie de ataque potencial. Cisco (2020).

Encriptación de Datos

Implementar protocolos de encriptación robustos, como WPA3-AES (Wi-Fi Protected Access 3 - Advanced Encryption Standard), para proteger la comunicación inalámbrica y prevenir la interceptación de datos por parte de usuarios no autorizados. Wi-Fi Alliance (2018).

Autenticación de Dispositivos y Usuarios

Utilizar métodos sólidos de autenticación, como WPA3 (Wi-Fi Protected Access 3), para asegurar que solo los dispositivos y usuarios autorizados puedan acceder a la red inalámbrica. Wi-Fi Alliance (2018).

Conclusiones

En este análisis de las vulnerabilidades del protocolo TCP/IP y las estrategias de mitigación propuestas, se destaca la complejidad y la persistencia de desafíos significativos en la seguridad de las redes de comunicación. Enfocándonos en los hallazgos más relevantes, donde se ha abordado detalladamente la amenaza persistente de la predicción de números de secuencia, destacando su impacto potencialmente perjudicial en la integridad de las conexiones TCP.

La revisión bibliográfica ha proporcionado una visión integral de las soluciones propuestas en la literatura para abordar las vulnerabilidades específicas del protocolo TCP/IP. Desde medidas fundamentales hasta enfoques más especializados, se han delineado estrategias que van desde fortalecer las capas del protocolo TCP/IP hasta la implementación de técnicas avanzadas para la gestión de números de secuencia. Se destaca la importancia de medidas como la auditoría de seguridad.

Es crucial reconocer la responsabilidad asociada con la manipulación de datos sensibles y garantizar que cualquier enfoque metodológico se adhiera a los más altos estándares éticos. Sin embargo, es imperativo abordar ciertas limitaciones en este análisis. La dinámica siempre cambiante del panorama de la seguridad cibernética puede influir en la vigencia de las conclusiones y soluciones propuestas. Además, las limitaciones relacionadas con la disponibilidad de datos específicos pueden haber afectado la amplitud y profundidad de la evaluación. Estas limitaciones, y de acuerdo a lo observado a lo largo de esta revisión bibliográfica, subrayan la necesidad de documentar detalladamente las constantes evoluciones a los que se enfrente diariamente la seguridad informática.

Finalmente, A través de la revisión Bibliográfica y a lo largo de la investigación realizada para llevar a cabo este informe con fines educativos, se logró identificar que mayoritariamente las vulnerabilidades comúnmente explotadas en el protocolo de comunicación TCP/IP se deben a errores comunes en el diseño y administración de la red.

La correcta administración de la red, actualización constante de sistemas operativos, cifrados, la segmentación de la red, autenticación de usuarios entre otros, son recomendaciones generales que se lograron identificar en los autores analizados, que podrían garantizar la disminución de los ataques cibernéticos.

Las redes inalámbricas han significado un gran avance en el ámbito de las telecomunicaciones, su evolución ha tenido un alcance significativo impactando favorablemente la forma en que nos comunicamos, y accedemos a información, sin embargo y debido quizá a su constante evolución, ha presentado grandes desafíos en su seguridad y fiabilidad a la hora de almacenar información, al ser de los modelos de comunicación más utilizados, a lo largo del tiempo ha sido blanco de exploración y explotación de vulnerabilidades existentes en ellas para acceder irregularmente a la información que se transmite y mueve sobre ellas.

Recomendaciones

Para futuras investigaciones se recomienda, utilizar un enfoque metodológico basado en el estudio mixto de las fuentes de información, esto brindara mayor enfoque y permitirá una apertura visual a todos los aspectos a tener en cuenta a la hora de estudiar las vulnerabilidades existentes, es crucial tener datos estadísticos, y líneas de tiempo que permitan visualizar el panorama de la evolución en las investigaciones realizadas y que aspectos innovadores se pueden tener en cuenta en la investigación.

Se considera importante continuar con la investigación en las vulnerabilidades existentes en el protocolo de comunicación TCP/IP en redes inalámbricas corporativas debido a que, la tecnología y la seguridad informática se encuentran en constante evolución y al mismo tiempo las personas dedicadas a la exploración y explotación de las falencias del mismo, encuentran el modo de seguir afectando estos entes con el fin de sacar provecho, social, personal o económico de la información que puedan obtener, por tanto es menester decir que muy probablemente las recomendaciones dadas a lo largo de este trabajo de grado en algún momento puedan ser obsoletas siendo necesario seguir avanzando en las investigaciones para poder frenar o mitigar estos casos.

Finalmente, como recomendación técnica y dirigiéndonos a la administración de seguridad de redes informáticas, se precisa fijar en los entes corporativos un plan de respuesta a incidentes detallado que describa los roles y responsabilidades del personal en caso de una violación de seguridad, el cual incluirá procedimientos claros para la notificación de incidentes, la evaluación del impacto y la mitigación de riesgos, protocolos para la preservación de evidencia digital y la coordinación con las autoridades pertinentes en caso de ser necesario y

pruebas regulares del plan de respuesta a incidentes para garantizar su eficacia y capacidad de adaptación a nuevas amenazas.

Referencias Bibliográficas

Academy. (2022). *Avast.* Recuperado el 18 de Abril de 2022, de https://www.avast.com/es-es/c-what-is-tcp-ip

AVG. (2022). *AVG*. Recuperado el 12 de Septiembre de 2022, de https://www.avg.com/es/signal/what-is-tcp-ip#:~:text=Hay%20cuatro%20capas%20en%20el,son%20un%20conjunto%20de%20protocolos.

Cañizares Rivera, E. A. (2022). *Evaluación de ataques ddos a un sistema de red y sus diferentes formas de protección.* Obtenido de http://repositorio.utc.edu.ec/handle/27000/9759

Combita, N. (2023). Ciberataque a IFX Networks impacta a más de 700 organizaciones en América Latina. *CANAL 1*. Obtenido de https://canal1.com.co/noticias/empresas/ciberataque-ifx-networks-america-latina/

Correa, L. (2023). *Diseño de una red de fibra óptica para la optimización de los servicios TCP/IP en la Empresa Asper Coating del Perú S.A.C - Ate, 2023.* Huacho – Perú: Universidad Nacional José Faustino Sánchez Carrión.

Escalante, M. (23 de mayo de 2023). *Handshaking de 3 vías (3 way handshaking)*. Obtenido de https://abcxperts.com/handshaking-de-3-vias-3-way-handshaking/#:~:text=(FTP%2C%20SFTP)-,El%20protocolo%20de%20handshaking%20de%203%20v%C3%ADas%20se%20utiliz

a%20para,iniciar%20la%20transferencia%20de%20archivos.&text=El%20handshaking%20de%203%20v%C3%ADas%2

Funcion Publica. (1989). *Ley 72 de 1989*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=10003

Funcion Pública. (1990). *Decreto 1900 de 1990*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=2581

Función Pública. (1990). *Ley 29 de 1990*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=254

Función Pública. (2009). *Ley 1341 de 2009*. Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913#:~:text=Promover%20el%20establecimiento%20de%20una,desarrollo%20personal%2C%20social%20y%20econ%C3%B3mico.

Genially. (2021). *Genially*. Recuperado el 20 de Febrero de 2021, de https://view.genial.ly/60ed966c654be50d815563f2/interactive-content-vulnerabilidades-en-el-modelo-tcpip

IBM. (2023). *IBM*. Recuperado el 15 de Agosto de 2023, de https://www.ibm.com/mx-es/topics/cyber-attack

Molina Sánchez, E. A. (2019). *Análisis de seguridad de vulnerabilidades presentes en redes sin hilos corporativas.* Obtenido de https://repository.unad.edu.co/handle/10596/37512

Palate, B., & Pesantez, D. (2021). *Mitigación de vulnerabilidades en la red central de un ISP: Uncaso de estudio.* Ecuador: Ecuadorian Science Journal. Obtenido de https://journals.gdeon.org/index.php/esj/article/view/117/127

Pedraza, C., & Herrera, C. (2018). *Realizar un análisis de las vulnerabilidades y mecanismos de explotación asociados a redes wifi abiertas.* Bogotá D.C - Colombia: Universitaria Agustiniana.

Quecano, J. (2014). *Vulnerabilidades de la integración de las tecnologías de información con las tecnologías de automatización industrial.* Bogotá D.C - Colombia: Universidad de La Salle .

Talenti, J. (2020). *SEGURIDAD EN LA FAMILIA DE PROTOCOLOS TCP/IP Y SUS SERVICIOS ASOCIADOS.*

UdeCataluña. (2022). *U de Cataluña*. Recuperado el 23 de Julio de 2022, de https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber

Glosario

TCP/IP (Transmission Control Protocol/Internet Protocol)

Conjunto de reglas estandarizadas que hacen posible la comunicación entre dispositivos en una red como Internet.

Vulnerabilidad de Seguridad

Debilidad en un sistema informático que puede ser explotada por un atacante para comprometer la integridad, confidencialidad o disponibilidad de la información.

Ataque Cibernético

Esfuerzo deliberado por violentar una red, para acceder de forma no autorizada a un sistema o dispositivo informático con el fin de extraer, alterar o destruir datos de información.

Predicción de Números de Secuencia

Técnica de ataque que implica prever el número de secuencia utilizado en una conexión TCP, permitiendo la falsificación de paquetes y potencialmente el cierre de la conexión.

Inyección en Conexiones TCP

Ataque que involucra el envío de paquetes falsificados a un host de destino como si provinieran de una fuente legítima, comprometiendo la seguridad de las comunicaciones.

Firewall

Dispositivo de seguridad que, según reglas de seguridad predefinidas, es empleado en una red por su capacidad de filtrar y controlar el tráfico de datos entrante y saliente de la misma.

Cifrado de Datos

Proceso de convertir información o datos en un código para prevenir el acceso no autorizado, asegurando la confidencialidad de la información transmitida.

Autenticación

Proceso de verificar la identidad de un usuario o dispositivo, típicamente antes de otorgar acceso a recursos en una red.

Control de Acceso

Mecanismos que regulan quién o qué puede ver o usar recursos en un entorno de computación.

Exploit

Código, secuencia de comandos o software que aprovecha una vulnerabilidad de seguridad de un sistema informático para causar comportamientos no previstos.

DoS (Denegación de Servicio)

Ataque que tiene como objetivo sobrecargar los recursos de un sistema hasta que no pueda atender solicitudes legítimas.

Mitigación

Proceso de implementar medidas para reducir o eliminar los riesgos asociados con vulnerabilidades de seguridad en un sistema informático.

Interoperabilidad

Capacidad de diferentes tipos de sistemas informáticos, redes y aplicaciones para trabajar juntos, intercambiar y hacer uso de la información de manera efectiva.

Ciberseguridad

Práctica de proteger sistemas, redes y programas de ataques digitales.

Red Inalámbrica Corporativa

Red de telecomunicaciones utilizada por una empresa, que utiliza tecnología inalámbrica para conectar dispositivos dentro del entorno corporativo.