Estudio monografía: Detección y prevención de ataques en redes Wi-Fi públicas: Estrategias y herramientas una versión documental

Diego Fernando Jimenez González

Asesora

Milena Ávila Orozco

Universidad Nacional Abierta y a Distancia UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería ECBTI

Ingeniería de Telecomunicaciones

2024

Dedicatoria

A Dios y a mis padres

Dedico esta elaboración de trabajo a papá Dios que es el encargado de guiarme y ayudarme a entender cada uno de mis esfuerzos, el cual me ayudado profundamente en salir adelante cuando más lo necesito.

a mis padres el motor de inspiración en todo lo que hago, el apoyo fundamental que me brindaron para poder empezar con esta travesía y que nunca dudaron de mis conocimientos fundamentales. Por estar siempre cuando los necesito, este trabajo está dedicado para ustedes.

A mis dos reinas de la casa mi hermana y mi sobrina la ratona, son las que me ayudan a salir con una sonrisa y un consejo para poder lograr lo que yo quiero.

Agradecimientos

A Dios

A Dios, fuente de sabiduría y guía eternal, le dedico este trabajo de grado. En cada descubrimiento, en cada palabra escrita, reconozco su gracia y dirección. Que este esfuerzo refleje mi agradecimiento y mi compromiso con su voluntad. Amen

A mis padres

A mi papá Luis Fernando Jiménez y mi mamá Myriam González, los mejores padres del mundo, les doy las gracias por siempre confiar en mí, que tengo el apoyo de ellos es lo más sagrado y fuerte que tengo y hoy les digo que sin ayuda de ellos no hubiera sido capaz de terminar este trabajo, y que este trabajo es un comienzo de lo que quiero seguir estudiando y ser profesionalmente. Y si volviera a nacer los escogería sin pensarlo que fueran de nuevo mis padres. Los amos.

A mi hermana y mi sobrina

A mi hermana Mayra Alejandra mi segunda madre, mi mejor amiga, le quiero agradecer por todo lo que me ha ayudado y por siempre saber que es el título de hermana mayor, por protegerme y ayudarme entender el camino que debo de tomar, le doy las gracias por estar cuando más la necesito, y a mi sobrina la ratona Luisa Fernanda, esa bebé que día a día nos enseña esa inocencia que cada ser debe tener y por quien luchar, quiero agradecerle y dedicarle este trabajo a mi sobrina y que tiene un tío para cuidarla y protegerla.

A mis tutores

A la tutora De la universidad Unad milena, que me ayudaron a orientarme a realizar este trabajo y poder encontrar el objetivo que necesitaba. A un profesor que me dio la mano para poder escoger mi trabajo de grado y poder entender el significado de la investigación el profesor

Santiago Morales de la universidad CES de Medellín, quiero darle las gracias por tener tanta paciencia y enseñarme ese valor tan significativo que es elaborar cada investigación. A los profes de cada materia de mi carrera de ingeniería que colocaron un granito de arena para poder terminar mis estudios muchas gracias a todos.

Resumen

Las redes Wi-Fi son comunes en lugares públicos como centros comerciales, aeropuertos, universidades y hoteles, proporcionando acceso a Internet. Sin embargo, estas redes presentan vulnerabilidades significativas, lo que las convierte en un blanco fácil para los ciberdelincuentes, quienes explotan las debilidades de seguridad cuando los usuarios no implementan medidas adecuadas en sus dispositivos o conexiones. Para mitigar estos riesgos, se recomienda el uso de contraseñas seguras, páginas con protocolos HTTPS y evitar compartir información sensible como datos personales o de tarjetas.

La detección y prevención de ataques en redes Wi-Fi públicas es fundamental para proteger la seguridad y privacidad de los usuarios. Para esto, es crucial implementar estrategias como el cifrado de datos, sistemas de detección de intrusiones y la concienciación de los usuarios. El cifrado de datos, mediante protocolos como WPA2 o WPA3, es una medida clave para asegurar la información que circula por la red. Además, el uso de redes virtuales privadas (VPN) agrega una capa extra de protección, encriptando el tráfico y reforzando la privacidad de los usuarios.

Sin embargo, la falta de conocimiento y de recursos en muchas redes públicas dificulta la implementación de estas medidas de seguridad, exponiendo a los usuarios a riesgos de ataques y violaciones de datos. Las redes públicas suelen carecer de las herramientas necesarias debido a la falta de capacitación de los administradores o a limitaciones económicas. Por lo tanto, es necesario realizar una investigación exhaustiva sobre la seguridad de estas redes para comprender la magnitud del problema y proponer soluciones efectivas.

En este contexto, resulta fundamental realizar una investigación documental sobre las estrategias y herramientas más eficaces para la detección y prevención de ataques en redes Wi-Fi públicas. Esta investigación debe centrarse en publicaciones científicas de entre 2019 y 2024, con

el fin de identificar las mejores prácticas y tecnologías para fortalecer la seguridad en estos entornos

Palabras claves: Wi-Fi Publicas, Ataques, Seguridad de usuarios, Cifrado.

Abstract

Wi-Fi networks are common in public places such as shopping malls, airports, universities and hotels, providing Internet access. However, these networks have significant vulnerabilities, making them an easy target for cybercriminals, who exploit security weaknesses when users do not implement adequate measures on their devices or connections. To mitigate these risks, it is recommended to use strong passwords, pages with HTTPS protocols and avoid sharing sensitive information such as personal or card data.

Detecting and preventing attacks on public Wi-Fi networks is essential to protect the security and privacy of users. To do this, it is crucial to implement strategies such as data encryption, intrusion detection systems and user awareness. Data encryption, using protocols such as WPA2 or WPA3, is a key measure to secure the information circulating on the network. In addition, the use of virtual private networks (VPN) adds an extra layer of protection, encrypting traffic and reinforcing user privacy.

However, the lack of knowledge and resources in many public networks makes it difficult to implement these security measures, exposing users to the risks of attacks and data breaches. Public networks often lack the necessary tools due to lack of training of administrators or financial constraints. Therefore, thorough research on the security of these networks is necessary to understand the magnitude of the problem and propose effective solutions.

In this context, it is essential to conduct desk research on the most effective strategies and tools for detecting and preventing attacks on public Wi-Fi networks. This research should focus on scientific publications from 2019 to 2024, in order to identify best practices and technologies to strengthen security in these environments.

Keywords: Public Wi-Fi, Attacks, User Security, Encryption.

Tabla de Contenido

Introducción 10

Planeamiento del Problema 11

Justificación 17

Objetivos 20

Objetivos General 20

Objetivos Específicos 20

Marco Teórico 21

Marco de Antecedentes 21

Estudios en el Ámbito Internacional 21

Estudios en el Ámbito Nacional 22

Marco Conceptual 23

Marco Legal 27

Nacional 27

Internacional 29

Marco Metodológico 31

Caracterizar las Fuentes de Información Relacionadas con el Objeto de Estudio 33

Amenazas Contra las Redes de Wifi Públicas Identificadas 38

Posibles Consecuencias que Generarían en la Red las Amenazas Identificadas 46

Herramientas de Mayor Eficiencia para la Prevención de los Ataques en las Redes Wifi-Públicas 53

Conclusiones 62

Referencias Bibliográficas 65

Lista de Figuras

Figura 1 *Distribución porcentual lugar de publicación* 34

Figura 2 *Distribución porcentual año de publicación* 35

Figura 3 *Distribución porcentual idioma de publicación* 36

Figura 4 *Distribución porcentual tipo de articulo de publicación* 37

Introducción

La expansión de redes Wifi-públicas ha revolucionado la conectividad, brindando acceso a internet en lugares públicos como cafeterías, aeropuertos, parques entre otros. Sin embargo, Este servicio gratuito viene acompañado de riesgos significativos, ya que las redes WiFi-abiertas son susceptibles a una amplia gama de ataques cibernéticos.

Este trabajo de grado se centra en explorar y analizar los ataques dirigidos a las redes WiFi-públicas, con el objetivo de comprender su naturaleza, impacto y posibles contramedidas. a partir de la revisión documental para identificar las estrategias y herramientas de mayor eficacia en la detección y prevención de ataques de redes Wifi-públicas,

Finalmente, se espera que este trabajo proporcione una visión integral de los desafíos de seguridad asociados a las redes WiFi-públicas, así como recomendaciones prácticas para mitigar estos riesgos y proteger la información personal y sensible de los usuarios.

Planeamiento del Problema

Las redes de wifi públicas se pueden entender como “un conjunto de computadores y equipos informáticos con el fin de interactuar entre sí y generar un proceso de intercambio de paquetes de datos e información; este comportamiento aplica para redes cableadas y redes Wireless (inalámbricas sin cables de comunicación). Cuando se crea una red de puntos de acceso, el alcance de este equipo para usuarios que se quieren conectar a él se llama “celda”. Usualmente se hace un estudio para alcanzar máxima cobertura con la mínima cantidad de un punto de conexión inalámbrico. De este modo, un usuario con un portátil podría moverse de un punto de conexión inalámbrico a otro sin perder su conexión de red.).” Cataño García, D. S. (2021, p.26)

Verde Costas (2022) citando al Instituto Nacional de Ciberseguridad INCIBE expone que las redes de wifi públicas son aquellas que transmiten información a través de señales de radiofrecuencia. Para identificar una red, existe el Service Set Identifer (SSID), que es el nombre de la red. El SSID es anunciado continuamente por los puntos de acceso para que los usuarios puedan encontrarlo. (p.11)

Existen diversos dispositivos que se sirven para lograr una comunicación a través de las redes públicas como las computadoras, teléfonos inteligentes entre los que se encuentran los smartphones, además de otros dispositivos de uso frecuente en los diversos contextos como el laboral, el académico o el mejoramiento de la vida cotidiana, entre ellos se encuentran: tablets, cámaras de seguridad, impresoras, bombillas entre otros. “Para tratar de proteger estos dispositivos y la información que trasmiten, existen diferentes protocolos de cifrado como el Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) o Wi-Fi Protected Access 2 (WPA2)” (Verde Costas, 2022, p 40)

Las redes inalámbricas públicas permiten a los dispositivos conectarse a Internet sin cables,

utilizando puntos de acceso Wi-Fi que emiten señales de radio en frecuencias como 2.4 GHz o 5 GHz. Estos puntos de acceso se vinculan a un enrutador que gestiona el tráfico entre los dispositivos y el proveedor de servicios de Internet. Aunque los usuarios suelen autenticarse mediante contraseñas o registros, muchas de estas redes públicas no cuentan con cifrado adecuado, lo que facilita que los datos transmitidos sean interceptados por terceros (Nabki et al., 2021).

La vulnerabilidad de las redes inalámbricas públicas se debe a la falta de medidas de seguridad avanzadas. La ausencia de cifrado sólido puede permitir a los atacantes interceptar la comunicación y llevar a cabo ataques Man-in-the-Middle (MitM), interceptando y alterando los datos entre los usuarios y el punto de acceso (Cheng et al., 2022). Además, los atacantes pueden crear puntos de acceso falsos que imitan redes legítimas para engañar a los usuarios y recolectar información sensible. Estas debilidades se agravan por la alta densidad de dispositivos conectados en estas redes, que a menudo carecen de controles de seguridad robustos (Hossain et al., 2022).

Teniendo en cuenta que son redes de uso público pueden tener riesgos de ataques cibernéticos, que, de acuerdo con Ponce Larreategui, (2021), se pueden entender como “cualquier acción o evento que tenga el potencial de comprometer la seguridad de los sistemas de información o de la tecnología de la información (TI) de una organización”. p.17. estas pueden causar daños que afectan la información privada de las personas, las instituciones u organizaciones y generar un impacto, que se materializa, en el daño de los equipos, vulneración en la información confidencial, secuestro y pérdida de los datos, infección en la red a través de los virus informáticos, interrupción del servicio y exposición pública de la información. Las amenazas cibernéticas están en constante evolución y cada vez son más sofisticadas, siendo el Programa maligno el método más comúnmente empleado para lograr el objetivo deseado.

Algunos ataques que registran la literatura son:

Modificación de mensajes, implica la alteración del contenido original de un mensaje, ya sea de forma intencionada o accidental, con el fin de cambiar su sentido, propósito o efecto. Este proceso puede afectar la interpretación y la comunicación de la información transmitida.

DdoS, consiste en la saturación de un servicio en línea mediante la inundación de tráfico falso, lo que impide a los usuarios legítimos acceder al mismo. Esta técnica, ampliamente utilizada en ciberataques, busca dejar fuera de servicio los recursos digitales objetivo

Interferencia de señal, es la introducción no deseada de perturbaciones que pueden afectar la transmisión o recepción de señales eléctricas, electromagnéticas o acústicas, lo cual puede ocasionar distorsiones o interrupciones en la comunicación entre dispositivos electrónicos o sistemas de telecomunicaciones.

Inundación de paquetes, es una técnica de ataque cibernético en la que se envían grandes volúmenes de datos a un sistema objetivo, sobrecargando su capacidad de procesamiento y saturando su ancho de banda. Esto puede causar una interrupción en el servicio o incluso una caída completa del sistema afectado.

Ip spoofing, es una técnica utilizada para alterar la dirección IP de origen de un paquete de datos, haciéndolo parecer que proviene de una fuente diferente a la real. En otras palabras, es la práctica de falsificar la dirección IP en los encabezados de un paquete de datos para ocultar la identidad del remitente o para hacer que el paquete parezca provenir de otra ubicación.

Sincronización, se refiere al proceso de coordinación temporal entre los dispositivos dentro de una red inalámbrica para garantizar una comunicación eficiente y sin interferencias. Esencialmente, implica que los dispositivos en la red están sincronizados en términos

Reenvió selectivo de paquetes, es una técnica utilizada en redes de computadoras para enviar únicamente los paquetes de datos perdidos o corruptos en lugar de reenviar todos los

paquetes desde el último punto de confirmación. En otras palabras, en lugar de volver a enviar todos los datos desde el principio cuando se pierde un paquete, el reenvío selectivo identifica y reenvía solo los paquetes perdidos, lo que optimiza el uso del ancho de banda y reduce la congestión en la red.

Enrutamiento no autorizado, es cuando un dispositivo de red o un usuario intenta redirigir el tráfico de datos a través de una ruta no permitida o no autorizada. En lugar de seguir las reglas y políticas establecidas para el enrutamiento, el enrutamiento no autorizado busca desviar el tráfico hacia destinos no aprobados o manipular la ruta del tráfico de manera indebida.

Túnel de agujero de gusano, es una técnica en redes informáticas que permite la creación de una conexión segura entre dos redes privadas a través de una red pública, como Internet, sin exponer los datos transmitidos a posibles interceptaciones. Funciona encapsulando los datos en paquetes que son enviados a través de la red pública y luego se liberan al destino final, lo que crea un "túnel" virtual privado entre los puntos de origen y destino. Este método proporciona un medio seguro para la comunicación entre redes privadas a través de una red no segura, como Internet

Sybil, es un término utilizado en el contexto de redes y sistemas distribuidos para describir una situación en la que un único usuario o entidad crea múltiples identidades falsas o nodos en la red con el fin de influir o manipular el comportamiento de la red. En otras palabras, Sybil se refiere a la acción de generar múltiples identidades aparentemente independientes, pero controladas por una sola entidad, con el propósito de distorsionar la percepción o el funcionamiento de la red en su conjunto.

Phishing, es una táctica maliciosa utilizada por ciberdelincuentes para engañar a individuos y obtener información confidencial, como nombres de usuario, contraseñas, detalles de tarjetas de crédito, etc. Los ataques de phishing suelen implicar el envío de correos electrónicos, mensajes de

texto o mensajes instantáneos que parecen ser de fuentes legítimas y conocidas, como bancos, empresas o servicios en línea populares.

Envenenamiento de DNS. es una técnica maliciosa utilizada por ciberdelincuentes para manipular o corromper los datos de la resolución de nombres de dominio (DNS). En lugar de dirigir a los usuarios a los sitios web legítimos que están buscando, los atacantes redirigen el tráfico de Internet a sitios web falsificados o maliciosos. Esto se logra al modificar las tablas de caché del sistema DNS con información falsa, lo que hace que los usuarios sean dirigidos a direcciones IP incorrectas cuando intentan acceder a sitios web específicos.

Algunos estudios que se han llevado a cabo en los ámbitos nacional e internacional plantean que al usar las redes de wifi el usuario puede estar expuestos a ataques como Spoofing o suplantación de DNS, ataque de denegación de servicio o DoS, ataques de Phishing, Man in the middle y ARP Spoofing; poniendo en riesgo los datos, la información sensible y la privacidad de los usuarios. Ramírez Herrera (2017)

Las redes inalámbricas públicas ofrecen conveniencia al permitir conexiones sin cables, pero presentan serias vulnerabilidades debido a la falta de cifrado sólido y medidas de seguridad adecuadas. Esta deficiencia en el cifrado facilita que los atacantes puedan interceptar datos y llevar a cabo ataques Man-in-the-Middle (MitM), lo que les permite espiar y manipular la comunicación entre los dispositivos de los usuarios y el punto de acceso (Cheng et al., 2022). Además, los atacantes pueden crear puntos de acceso falsos que imitan redes legítimas para engañar a los usuarios y robar información sensible. La densidad de dispositivos conectados en estas redes también aumenta el riesgo de exposición a ataques (Hossain et al., 2022).

Para mejorar la seguridad en redes Wi-Fi públicas, se recomienda el uso de herramientas como las redes privadas virtuales (VPN), que cifran el tráfico de datos y protegen la comunicación

contra posibles interceptaciones. Además, es fundamental evitar conectarse a redes Wi-Fi desconocidas o sospechosas y mantener el software del dispositivo actualizado para protegerse contra vulnerabilidades. Muchas de las amenazas en estas redes se deben al mal uso y la falta de precaución por parte de los usuarios, como conectarse a puntos de acceso no verificables o compartir información sensible en conexiones inseguras. Implementar estas medidas puede reducir significativamente los riesgos asociados con el uso de redes Wi-Fi públicas (Nabki et al., 2021).

Para abordar estos desafíos, la literatura reciente (2019-2024) ha documentado diversas estrategias y herramientas para la detección y prevención de ataques en redes Wi-Fi públicas. Entre las estrategias más destacadas se encuentran la implementación de protocolos de seguridad avanzados como WPA3, el uso de VPN (Redes Privadas Virtuales) para cifrar el tráfico de datos, y la integración de sistemas de detección de intrusiones específicos para redes inalámbricas. Estas herramientas y estrategias han demostrado ser efectivas en la mejora de la seguridad de las redes públicas, proporcionando un nivel de protección robusto tanto para la infraestructura de red como para los usuarios individuales.

Teniendo en cuenta lo expresado se puede plantear como pregunta de investigación

¿Cuáles son las estrategias y herramientas con mayor eficiencia implementadas para la detección y prevención de ataques de redes wifi-públicas de acuerdo con lo reportado por la literatura entre los años 2019 y 2024?

Justificación

La detección y prevención de ataques en redes Wi-Fi públicas es un tema de mucha importancia en el presente, tanto para las universidades en sus procesos internos y formativos, los ingenieros y los usuarios de estas redes en general. A medida que la conectividad inalámbrica se vuelve más común y las redes Wi-Fi públicas se utilizan ampliamente, se hace vital resguardar la información confidencial y garantizar la seguridad de los usuarios.

En primer lugar, para las universidades, contar con estrategias y herramientas eficaces de detección y prevención de ataques en redes Wi-Fi públicas es fundamental para proteger los datos sensibles de estudiantes, profesores y personal administrativo. En el entorno de aprendizaje, se maneja una cantidad de información restringida, como datos personales, investigaciones y proyectos, en los cuales se debe salvaguardar los derechos de autor tanto morales como patrimoniales, que podrían ser el blanco de ataques cibernéticos. Por lo tanto, implementar medidas de seguridad adecuadas es esencial para cuidar esta información y mantener la integridad en todos los sistemas.

Además, en el ámbito universitario, los ingenieros desempeñan un papel muy importante en el desarrollo, mantenimiento y seguridad de las redes Wi-Fi públicas. Como ingenieros, es necesario comprender los diferentes tipos de ataques que pueden ocurrir en una red Wi-Fi pública en la que la mayoría de las personas tendrán acceso y estar al pendiente de las herramientas y técnicas utilizadas por los ciberdelincuentes. Esto les permite identificar y mitigar posibles amenazas, asegurando así la estabilidad y el funcionamiento óptimo de la red.

No obstante, los ingenieros pueden desempeñarse en una amplia variedad de campos donde las redes de Wi-Fi públicas están presentes, como en el desarrollo de sistemas de conectividad, la administración de redes, y la implementación de soluciones tecnológicas en entornos urbanos. En

estos contextos, es crucial identificar y evaluar los riesgos asociados a las redes Wi-Fi públicas, ya que la seguridad de la información y la protección de los equipos de los usuarios pueden estar comprometidas. Una adecuada gestión de estos riesgos es esencial para minimizar posibles daños, garantizar la integridad de los datos personales y preservar la funcionalidad de los dispositivos. Por lo tanto, los ingenieros deben aplicar sus conocimientos para desarrollar estrategias de seguridad efectivas y asegurar un entorno de red más seguro y confiable para todos los usuarios.

En cuanto a la comunidad en general, la detección y prevención de ataques en redes Wi-Fi públicas es esencial para conformar la seguridad de los usuarios. En tanto, estas son utilizadas por una cantidad de personas, tanto en entornos educativos como en lugares públicos tales como: cafeterías, centros comerciales, aeropuertos y hoteles. Los usuarios confían en que estas redes sean seguras y protegidas, y es responsabilidad de la comunidad proporcionarles un entorno seguro para su conectividad. La implementación de estrategias y herramientas de detección y prevención de ataques en redes Wi-Fi públicas ayuda a evitar el robo de información personal, el acceso no autorizado a cuentas y la propagación de malware, protegiendo así a los usuarios de posibles amenazas.

Proporciona una capa adicional de seguridad para proteger los datos confidenciales y garantizar la integridad de las redes. Los ingenieros desempeñan un papel demasiado importante en la implementación de soluciones de seguridad y en la protección de las redes Wi-Fi públicas. Para la comunidad, contar con redes Wi-Fi públicas de fácil acceso seguras garantiza la privacidad y seguridad de los usuarios mientras se conectan a estas redes en diferentes entornos. En definitiva, la detección y prevención de ataques en dichas redes Wi-Fi públicas es esencial en la actualidad, donde la conectividad inalámbrica es una parte integral de nuestro presente y la seguridad de la información es de suma importancia.

Finalmente, Esta investigación es crucial debido a la necesidad de proteger la información en redes inalámbricas, las cuales están presentes en diversos entornos y son utilizadas por una amplia variedad de usuarios. Las redes inalámbricas se encuentran comúnmente en oficinas, cafeterías, aeropuertos, universidades y hogares, facilitando actividades que abarcan desde el trabajo y la comunicación personal hasta el acceso a servicios en línea. La conveniencia que ofrecen estas redes permite una conectividad flexible y eficiente en diferentes contextos.

No obstante, esta facilidad de acceso conlleva ciertos riesgos, especialmente en el caso de las redes públicas. Las redes ubicadas en lugares como cafeterías o aeropuertos suelen ser más vulnerables a ataques debido a su diseño abierto y a la carencia de medidas de seguridad adecuadas. La falta de cifrado efectivo y de autenticación sólida en estas redes facilita la interceptación de información sensible y el acceso no autorizado, lo que pone en peligro los datos de los usuarios.

Objetivos

Objetivos General

Analizar las estrategias y herramientas de mayor eficiencia para la detección y prevención de ataques en redes de wifi públicas que se evidencian en publicaciones científicas, divulgadas entre el 2019 y 2024 en el ámbito mundial.

Objetivos Específicos

Caracterizar las fuentes de información relacionadas con el objeto de estudio.

Identificar las diversas amenazas contra las redes de wifi públicas.

Describir las posibles consecuencias que generarían en la red las amenazas identificadas.

Evidenciar las herramientas de mayor eficiencia para la prevención de los ataques en las redes Wifi-Públicas".

Marco Teórico

Marco de Antecedentes

Estudios en el Ámbito Internacional

Evaluación del desempeño de protocolos de seguridad para combatir ataques en redes inalámbricas WiFi, Perú 2022. El objetivo principal fue Evaluar el desempeño de los protocolos de seguridad de redes para combatir ataques en redes inalámbricas Wi-Fi. La investigación es de tipo cuantitativa – cuasiexperimental porque mediante la recopilación y análisis de información se logró comprobar la hipótesis de la investigación. las redes inalámbricas se han considerado inseguras, a diferencia de las cableadas. Para hacer que las redes inalámbricas sean más seguras y efectivas, se han desarrollado y actualizado protocolos de seguridad Wi-Fi para compensar las fallas de seguridad. El presente trabajo ha optado por seleccionar el total de protocolos de seguridad de Wi-Fi, a saber, WPA, WPA2 y WPA3, y realizó una evaluación de estos para permitir a los usuarios obtener una comprensión profunda de la seguridad de Wi-Fi al elegir dispositivos inalámbricos.

Aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red wifi, Ecuador 2023, sus objetivos fueron analizar con la aplicación de hacking ético para identificar amenazas, riesgos y vulnerabilidades en la red wifi, Identificar los factores de amenaza, riesgos y las vulnerabilidades que se presentan en la red Wifi, determinar los posibles puntos de accesos vulnerables dentro la red Wifi a través de hacking ético, recomendar las mejores prácticas para la seguridad de la red wifi. Se trabajó bajo el estudio de caso y algunas de las recomendaciones que presentó fueron: Es importante tener en cuenta los factores de amenaza, riesgos y vulnerabilidades que se presentan en la red Wifi para poder determinar y fortalecer los posibles puntos de acceso vulnerables mediante una prueba de hacking ético. A partir de esto, las

recomendaciones de las mejores prácticas de seguridad de la red Wifi deben ser implementadas para mejorar la privacidad y confidencialidad de los datos que compartimos a través de ella, garantizando así la integridad y protección de nuestro entorno digital.

Estudios en el Ámbito Nacional

Determinar los principales ataques a los que se exponen los usuarios que utilizan la red-wifi "idea internet en el parque" del municipio de Urrao realizado en el año 2017, Ramírez Herrera, su objetivo principal fue determinar los principales ataques y las vulnerabilidades informáticas que intervienen, en la red WIFI "IDEA internet en el parque", de la plaza Rafael Uribe Uribe, del municipio de Urrao. Alguna de las conclusiones que se presentan es que, al hacer uso de este tipo de redes de uso masivo y público, se puede correr riegos como los ataques de Spoofing que pueden dañar los archivos, suplantación en los datos que se usan en las redes, ataque de denegación de servicio o DoS, en el cual se puede dar la pérdida en la conectividad, ataques de Phishing, Man in the middle y ARP Spoofing; poniendo en riesgo los datos, la información sensible y la privacidad de los usuarios, al poder robar los datos de los usuarios entre otros.

Método para la prevención y mitigación de vulnerabilidades en redes WI-FI, Manizales 2021, el objetivo principal fue adoptar un método de pentest para la prevención y mitigación de vulnerabilidades en red WIFI a partir del análisis de pruebas de pentesting en el ambiente controlado, Se analizaron de forma precisa los conceptos del origen y marco histórico de las redes WIFI y cómo han evolucionado, asimismo el modo en que se han generado diferentes vulnerabilidades a los sistemas de información irrumpiendo así los principios de integridad, confidencialidad y disponibilidad, al dar cumplimiento a los tres objetivos propuestos de este proyecto, se elabora este trabajo para que el usuario final lo utilice como una herramienta tipo manual para aplicar las pruebas de testeo, de manera sencilla y orientada a partir de la simulación

en ordenadores y ambientes controlados. Tras el análisis que arrojó el escáner de vulnerabilidades NESSUS a partir de un ordenador víctima, al cual se les ejecutaron todas las pruebas y ataques a vulnerabilidades debidamente halladas, fue posible y pudo constatarse las grandes vulnerabilidades que tenemos en los hogares, en telecomunicaciones, en la red internet de hogar y dispositivos de conexión inalámbrica.

Marco Conceptual

Para entender los componentes de esta propuesta investigativa es fundamental tener claros algunos conceptos como son:

Access Point. De acuerdo con Puedmag, C. A. C. (2021). Un dispositivo para establecer una conexión inalámbrica entre equipos y pueden formar una red inalámbrica externa (local o Internet) con la que interconectar dispositivos móviles o tarjetas de red inalámbricas. Esta red inalámbrica se llama WLAN (Wireless local área network) y se usan para reducir las conexiones cableadas (lawebdelprogramador, s.f).

Amenaza. Incidente bien sea nuevo o recién descubierto que puede llegar a dañar un sistema de información e incluso la organización como tal. Es un proceso que puede llegar a violar la seguridad de una empresa a través de vulnerabilidades. Giraldo, L. V. (2021).

Antivirus. sirve para rastrear, diagnosticar, detectar y eliminar virus; asimismo desinfectar archivos y prevenir infecciones masivas a los archivos. Dentro de las buenas prácticas de seguridad información, se recomienda instalar y actualizar sólidamente el antivirus en sistema operativo, Cataño García, D. S. (2021).

Ataques. Intento que busca acceder a los equipos tecnológicos de una organización, bien sea computadores o servidores, entre otros. Esto lo realiza a través de técnicas como introducción

de virus o malware mediante el uso de diferentes técnicas que insertan el código malicioso en el equipo. Giraldo, L. V. (2021).

Ataques Cibernéticos. Se trata del aprovechamiento de las vulnerabilidades del software o hardware para ingresar con el objetivo de destruir, exponer, alterar, inhabilitar un sistema informático o la información que almacena o la red. Olaya, A. (2021).

Ciberseguridad. en la actualidad toda organización sea privada o pública son muy rigurosos con la preservación y cuidado de los activos cibernéticos, es entonces cuando surge la necesidad de implementar medidas y programas en seguridad de la información, de acuerdo con Giraldo, L. V. (2021) hace referencia al proceso que se encarga de defender los computadores, servidores e incluso dispositivos móviles y cualquier otro recurso tecnológico de ataques maliciosos. Cataño García, D. S. (2021).

Eficiencia. Lo define como la capacidad de realizar una tarea o alcanzar un objetivo utilizando la menor cantidad de recursos posible. La eficiencia implica maximizar la productividad y minimizar el desperdicio de recursos, como tiempo, dinero, energía, materiales o esfuerzo. Smith, J. (2020).

Firewall. De acuerdo con la investigación de Verde Costas, I. (2022). Sistema cuya función es prevenir y proteger una red privada, de intrusiones o ataques de otras redes, bloqueándoles el acceso. Cataño García, D. S. (2021) llamado cortafuegos en español. Es un sistema que previene y protege una red privada, cuando se siente amenazado por intrusiones o ataques de otras redes, generando una interrupción en el tráfico entrante, pueden trabajar tanto en el hardware como en el software.

Hacker. Es un individuo de la sociedad moderna con conocimientos informáticos que se dedica a crear y modificar herramientas de hardware y software para desarrollar opciones que beneficien al usuario. Barahona Uriña, S. M., & González Crespo, J. R. (2022)

Malware. Se entiende como un programa malicioso y desagradable que produce daños en los sistemas y equipos informáticos invadiendo y deshabilitando el control y las operaciones de estos equipos Barahona Uriña, S. M., & González Crespo, J. R. (2022). De acuerdo con la investigación de Verde Costas, I. (2022). Término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.

Phishing. Es un método que utilizan los atacantes informáticos para delinquir utilizando técnicas de fraude y engaño para manipular a los usuarios y robar información confidencial de estos, Barahona Uriña, S. M., & González Crespo, J. R. (2022). así mismo la investigación de Verde Costas, I. (2022). Lo asume como el conjunto de técnicas que tienen como objetivo obtener a través de internet datos privados de los usuarios.

Ransomware. Es un tipo de programa malicioso que limita a los usuarios a acceder a su sistema o archivos, exigiendo un rescate monetario para que el usuario recupere su información o sistema, Barahona Uriña, S. M., & González Crespo, J. R. (2022). De acuerdo con la investigación de Verde Costas, I. (2022). Tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos.

Redes Wifi. de acuerdo con Perez, J. T. (2022). es una red informática que utiliza conexiones de radiofrecuencia entre los nodos de la red. Las redes inalámbricas son usadas tanto en hogares como en empresas. La gente suele asumir que todo lo inalámbrico es Wi-Fi, pero no es así. Hay muchos tipos diferentes de redes inalámbricas en toda una gama de tecnologías como

Bluetooth, ZigBee, LTE, 5G, mientras que Wi-Fi es específico del protocolo inalámbrico definido por el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) en la especificación 802.11 y sus enmiendas.

Redes Wifi Publica. La conceptualizan como la conectividad inalámbrica que no utiliza ningún tipo de encriptación (WEP / WPA) para proteger los datos a medida que viaja a través del aire entre un dispositivo y el punto de acceso inalámbrico. Los datos transmitidos a través de una red Wifi no segura pueden ser interceptadas o vistos por usuarios no autorizados. Ramírez Herrera, G. A. (2017)

Riesgo. De acuerdo con Pérez, J. T. (2022) es una combinación de la probabilidad de amenaza y el impacto de una vulnerabilidad. En otras palabras, el riesgo es la probabilidad de que un agente de amenaza explote con éxito una vulnerabilidad.

Seguridad Informática. Preciado Cortez, Y. Y. (2022) la definen como la seguridad de la información garantiza la confidencialidad, disponibilidad e integridad de la información.

Spyware. En relación con lo planteado por Ramírez Herrera, G. A. (2017) es el software que se produce o subrepticiamente instalado en un sistema de información para reunir información sobre personas u organizaciones sin su conocimiento; un tipo de código malicioso.

Vulnerabilidad. Barahona Uriña, S. M., & González Crespo, J. R. (2022) lo asumen como el fallo o riesgo que se puede presentar en un sistema informático, lo que puede ocasionar un error en la seguridad de la red, permitiendo a que intrusos puedan conectarse y acceder a la misma, por lo que es necesario eliminar estos fallos. Cataño García, D. S.(2021) La entienden como una debilidad en un sistema informático, la cual puede ser aprovechada por un ciberataque, con el propósito de ingresar sin autorización, pasar por alto las restricciones y protocolos de seguridad,

para ejecutar código malicioso, ingresar a una memoria, robar, sustraer datos de alta sensibilidad y privacidad.

Wep. De acuerdo con la investigación Ballestas Cañas, P. J. (2020). Fue desarrollado para redes inalámbricas y aprobado como estándar de seguridad Wi-Fi en septiembre de 1999. WEP debía ofrecer el mismo nivel de seguridad que las redes cableadas, sin embargo, hay un montón de problemas de seguridad conocidos en WEP, que también es fácil de romper y difícil de configurar.

WPA. De acuerdo con la investigación Ballestas Cañas, P. J. (2020), al igual que WEP, después de haber sido sometida a pruebas de concepto y a demostraciones públicas aplicadas, resultó ser bastante vulnerable a la intrusión. Sin embargo, los ataques que más amenazaban el protocolo no fueron los directos, sino los que se realizaron con el sistema WPS (Wi-Fi Protected Setup), un sistema auxiliar desarrollado para simplificar la conexión de los dispositivos a los puntos de acceso modernos.

Marco Legal

Nacional

Colombia cuenta con la siguiente legislación que se relacionan con el objeto de estudio:

Ley 2108 de 2021 "Ley de internet como servicio público esencial y universal o por medio de la cual se modifica la ley 1341 de 2009 y se dictan otras disposiciones" el objetivo de esta ley es establecer dentro de los servicios públicos de telecomunicaciones. El acceso a internet como uno de carácter esencial, con el fin de propender por la universalidad para garantizar y asegurar la prestación del servicio de manera eficiente, continua y permanente, permitiendo la conectividad de todos los habitantes del territorio nacional.

Ley 1581 de 2012, Por medio de la cual se dictan disposiciones generales para la

Protección de Datos Personales. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

De acuerdo con la Ley 1273 de 2009 en la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

El Congreso de Colombia Decreta.

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor: CAPITULO. I De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269ª. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96)

meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C. Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D. Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena28 de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E. Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F. Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes

Internacional

Política informática y la gestión de la seguridad de la información con base en la norma.

ISO 27001. Ayuda a las organizaciones a establecer la política y los objetivos de gestión de la seguridad de la información y a comprender cómo se pueden gestionar los aspectos importantes, aplicar los controles necesarios y establecer objetivos claros para mejorar la seguridad de la información.

Marco Metodológico

Este ejercicio se inscribe en la investigación de enfoque cualitativo de tipo documental, la cual involucra un proceso riguroso y cuidadoso para la identificación, revisión, selección y análisis de información que proviene de fuentes secundarias académicas materializadas en artículos de revistas especializadas, trabajos de grado y guías prácticas incluidas en bases de datos reconocidas.

La investigación documental no solo es considerada una etapa de un proceso exploratorio, sino, una estrategia del enfoque cualitativo que permite la generación y creación de conocimiento científico, en tanto, tiene sus particularidades metodológicas propias en su diseño y desarrollo, Galeano, M. (2007).

La investigación documental permite hacer una reflexión sistemática del conocimiento acumulado en relación con un objeto de estudio, que ha sido referenciado por otros investigadores que, para el presente caso, son las estrategias y herramientas con mayor eficiencia implementadas para la detección y prevención de ataques de redes wifi-públicas.

Para el desarrollo de esta investigación se identificaron los siguientes pasos:

Identificación de las Fuentes. Consistió en la identificación, selección y recopilación de las fuentes de información acordes con los objetivos propuestos para ello, se tuvo en cuenta los siguientes aspectos

Año de Búsqueda. Acordes con las condiciones de las publicaciones en lo referente a su temporalidad, se trabajaron textos entre el 2019 y 2024.

Tipo de Bibliografía Consultada. Por el tipo de tema abordado no solo se trabaja con artículos de revistas sino además con trabajos de trabajos de grado de pre y posgrados y una guía práctica.

Base de Datos y Buscadores. Los textos se buscaron en Google académico y Academic

Search Ultimate.

Palabras Claves de Acceso. Para poder identificar los textos se utilizaron las siguientes palabras claves. Wifi-públicas, ataques Wifi-públicas, seguridad Wifi-públicas, Wifi-abiertas, vulnerabilidad Wifi-públicas.

Selección de Textos. Una vez identificado los textos se procedió a verificar que no existieran repeticiones, y a la lectura de los resúmenes para validar que la información que tuvieran si aportaran al desarrollo de los objetivos, en total se lograron identificar 50 textos, todos estos textos eran de acceso gratuito en la red.

Lectura y Sistematización de Información. Con los textos seleccionados se procede a la lectura completa de cada uno de ellos y a la selección de fragmentos de forma textual, que permitieran llenar de contenido las categorías previas que están plasmadas en los objetivos. Para la selección de la información, se diseñó una matriz temática en Excel como se puede ver seguidamente, en relación con cada uno de los objetivos específicos. Caracterizar las fuentes de información relacionadas con el objeto de estudio.

Análisis de la Información. organizada la información por categorías se hace nuevamente una lectura detallada y analítica, construyendo los textos a partir de las recurrencias, los aspectos comunes, y aquellas cosas que si bien, no son tan comunes, se resaltan como parte de los hallazgos y que pueden ser interesante sen futuras investigaciones en tanto ya se evidencia en la literatura.

Es de resaltar que todo este proceso investigativo, cumplió con los criterios éticos de la investigación documental, que consiste en el respeto por el derecho de autor y la debida citación, de allí, que todo lo que es textual aparece en comillas y lo parafraseado o apoyado en lo plasmado por cada uno de los autores se encuentra debidamente referenciado acorde con lo dispuesto en las normas APA versión 7

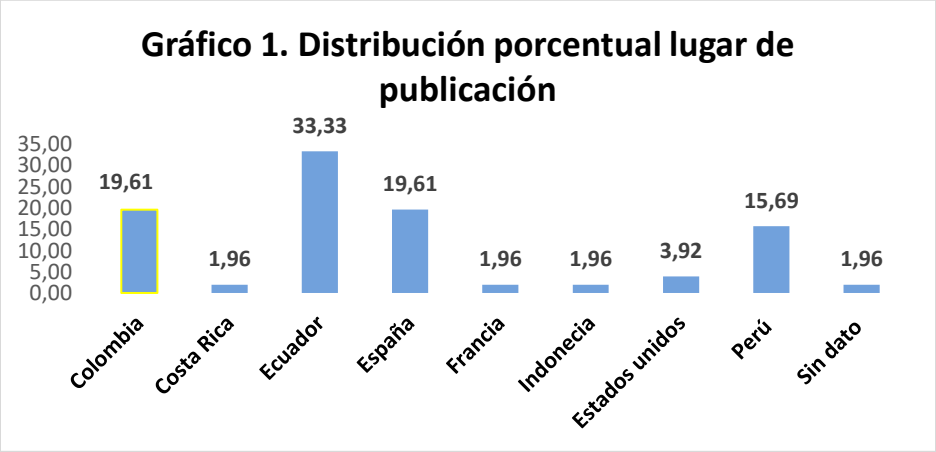
Caracterizar las Fuentes de Información Relacionadas con el Objeto de Estudio

A continuación, se presentan los resultados obtenidos del proceso investigativo documental que permiten dar cuenta de los objetivos planteados, estos se presentaran en cuatro a partes: en el primero, se hace una descripción de las características fundamentales de los textos que sirvieron de base para este estudio; el segundo, se esbozan las amenazas que se identifican en los textos contra las redes de wifi públicas; el tercero, devela las consecuencias que generan las amenazas a las redes; en el cuarto, se muestran las estrategias y herramientas que permiten detectar los ataques a estas redes; y finalmente, se presentan las herramientas de mayor eficiencia para la prevención de los ataques a las redes de wifi públicas.

De acuerdo con el lugar de publicación de los textos encontrados uno de cada tres se realizó en Ecuador, representado en un 33,33% (17); uno de cinco de los textos fue desarrollado en Colombia y en España, cada uno de ellos con un 19.61% (10); en Perú se ubican el 15,69% de los textos (8); los demás países con menor representación porcentual están por fuera de América latina, ellos son Francia, Indonesia. Ver figura 1

Figura 1

Distribución porcentual lugar de publicación

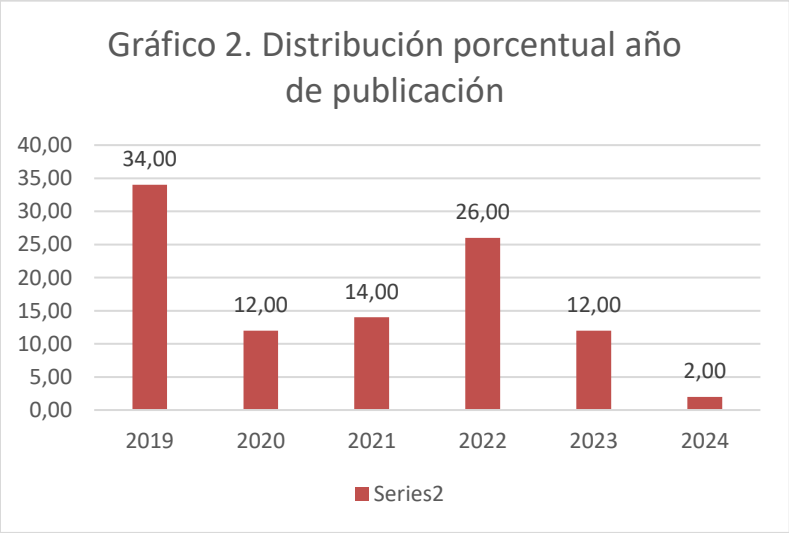


Fuente. Autoría propia

De acuerdo con el gráfico de la distribución porcentual del año de publicación, uno de tres publicaciones se realizó en el año 2019, representando un 34,00% (17), uno de cuatro publicaciones se realizó en el año 2022, representando un 26,00% (13), uno de seis publicaciones se realizó en el año 2020 y 203, representando un 12,00% (6), y en el 2021 se encontró un 14,00%(6) en año de publicación. Y lo que va de este año se encuentra un 2% lo que equivale a 1 publicación sobre la investigación. Ver figura 2.

Figura 2

Distribución porcentual año de publicación

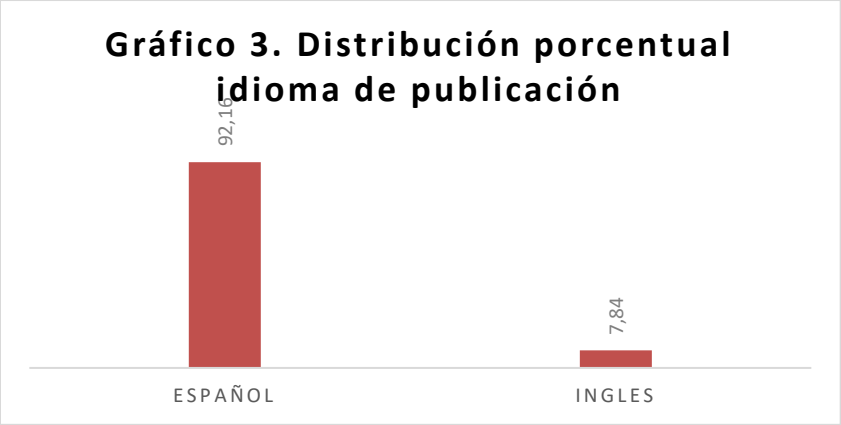


Fuente. Autoría propia

Con respecto al idioma de publicación, el mayor peso porcentual se encuentra en aquellos que están en español con un 92,16% (47), mientras que el idioma inglés tiene un 7,84% (4).

Figura 3

Distribución porcentual idioma de publicación

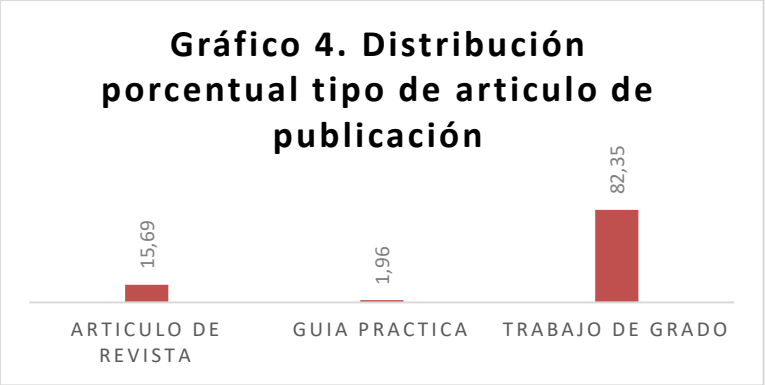


Fuente. Autoría propia

El análisis revela una predominancia significativa de trabajos de grado, que constituyen el 82,35% de los artículos revisados, lo que sugiere un enfoque académico sólido en la investigación sobre seguridad en WiFi. Por otro lado, la presencia de artículos de revista (15,69%) indica un interés moderado en la divulgación científica, aunque en menor medida. La inclusión de una guía práctica sugiere un intento de vincular la teoría con aplicaciones reales, lo que podría enriquecer la comprensión del tema. En conjunto, estos hallazgos reflejan una diversidad en los enfoques de estudio, aunque con un claro énfasis en la academia.

Figura 4

Distribución porcentual tipo de articulo de publicación



Fuente. Autoría propia

Para caracterizar las fuentes de información relacionadas con el objeto de estudio sobre la seguridad y los ataques a una red Wi-Fi, es fundamental identificar las fuentes que proporcionan datos sobre vulnerabilidades, amenazas y mejores prácticas de protección. Estas fuentes incluyen literatura académica, artículos técnicos, reportes de seguridad de empresas especializadas en ciberseguridad y blogs de expertos. Las publicaciones académicas, como investigaciones en revistas especializadas, ofrecen teorías y análisis profundos sobre los tipos de ataques más comunes a redes Wi-Fi, como el ataque de desautenticación, el ataque de diccionario o el man-in-the-middle. Además, los informes anuales de seguridad de firmas como Cisco o Symantec proporcionan estadísticas actualizadas y detalles sobre tendencias emergentes en ataques a redes inalámbricas.

Asimismo, las fuentes prácticas como foros especializados, tutoriales en línea y conferencias sobre ciberseguridad ofrecen una visión más dinámica sobre cómo los atacantes explotan vulnerabilidades específicas en los protocolos Wi-Fi (como WPA2 o WPA3) y cómo los

profesionales de seguridad pueden defenderse. El uso de herramientas como Aircrack-ng o Wireshark, mencionadas en estos foros, es fundamental para comprender cómo los atacantes pueden interceptar y descifrar tráfico de redes Wi-Fi. Estas fuentes proporcionan tanto información técnica detallada como ejemplos prácticos, permitiendo así una comprensión completa sobre los desafíos y soluciones en la seguridad de redes inalámbricas.

Amenazas Contra las Redes de Wifi Públicas Identificadas

A continuación, se presentan las amenazas que se describen en las fuentes consultadas, teniendo en cuenta las más frecuentes y seguidamente las menos recurrentes, pero que por el tipo de investigación implementado es importante presentarlas como parte de los hallazgos.

Uno de los ataques que más se referencian en la literatura científica consultada son los de **Denegación de Servicio (DoS),** entendidos estos como: acciones informáticas dirigidas a deshabilitar un sistema mediante la inundación de solicitudes en un período corto, con el propósito de sobrecargar el servidor y provocar su colapso, Guallasamín Haro, A. S., & Santos Guerrero, G. A. (2022), lo que conlleva a una incapacidad del sitio web para funcionar correctamente, negando así el acceso a los servicios. Jumbo Delgado, R. V. (2019).

Estos tienen el potencial de perjudicar el rendimiento de la red e incluso pueden llegar a interrumpir su funcionamiento por completo. Arango Gómez, O. D. (2023); una de las formas en que se materializan el ataque es que los criminales sobrecargan la red con tráfico no genuino, lo que resulta en una disminución del rendimiento o incluso la inaccesibilidad para los usuarios legítimos. Cuvi Mencias, B. M. (2023).

Dado que las aplicaciones en línea tienen capacidades limitadas, se convierten en objetivos claros para este tipo de ataques en momentos específicos. Guallasamín Haro, A. S., & Santos Guerrero, G. A. (2022). La forma en la cual se puede presentar este ataque a las redes de wifi públicas es cuando los usuarios autorizados de un sistema o aplicación no pueden acceder a los recursos de información, dispositivos o cualquier otro elemento de red debido a la saturación del host o red objetivo con un volumen excesivo de tráfico, lo que provoca que la red objeto de ataque deje de responder o se bloquee, impidiendo así el acceso legítimo de los usuarios. Collado Ramírez, B. (2021)

Otra forma de ataque se da cuando se priva del servicio a un cliente o punto de acceso legítimo, por ejemplo, enviar tramas de invalidación, también enviar señales de canal ocupado o inundar con solicitudes de autenticación. Medina Rojas, J. D., & Rivas Montalvo, Y. Y. (2020), o se interrumpe la comunicación entre un dispositivo y un punto de acceso (AP), por medio del uso de tramas de invalidación. Otero Dans, A. (2021).

Seguidamente se encuentran los ataques **Man-in-the-Middle** entendido como: Un ataque en el que el agresor se posiciona entre dos entidades en comunicación, con el fin de interceptar o modificar los datos que comparten. Generalmente, el propósito de este ataque es el robo de información de los usuarios. Puede dirigirse hacia individuos, páginas web o bases de datos financieras, con el objetivo final de interceptar o alterar la información Verde Costas (2022).

También encontramos que una de sus características principales es el enfoque que solo requiere que el agresor se ubique entre las dos partes que intentan comunicarse, capturando los mensajes enviados e imitando al menos a una de ellas Quiña Haro & Reza Zurita, 2022 y también El ataque MitM se emplea con diversos propósitos, tales como robar credenciales y espiar. Un ejemplo notable es el ataque **KRACK**, que implica situarse entre el cliente y el punto de acceso real para interceptar el tráfico (Esteban Sánchez, 2021). Un ataque que no es tan común, pero se ha venido investigando últimamente es el ataque krack Este tipo de ataque, conocido como ataque de reinstalación de clave, tiene el potencial de impactar todos los estándares y protocolos de cifrado de Wi-Fi. La noticia cobró gran importancia a nivel global, ya que puso en riesgo la seguridad de la mayoría de los dispositivos. Sin embargo, debido a que se mantuvo en secreto por un tiempo, las empresas responsables de abordar estas fallas tuvieron la oportunidad de desarrollar un parche de actualización que contribuyó a mitigar esta vulnerabilidad. Duque, S. & Rojas, Y. (2019).

Para descubrir información sensible que una persona desea comunicar a otra sin obtener

permiso, un atacante podría engañar al emisor haciéndole creer que está hablando con el destinatario, por ejemplo, usando un correo electrónico falso. En ciberseguridad, esta técnica se llama Man-in-the-Middle, uno de los ataques más comunes Almendral Fernández, (2020).

Otro ataque común en esta investigación es el Ataque de fuerza bruta, Conocidos como los ataques que pueden emplear herramientas para intentar adivinar contraseñas y conseguir acceso no autorizado a la red. Arango Gomez, O. D. (2023).

Los ataques de **fuerza bruta** difieren de otros enfoques de ataques de datos, ya que no intentan engañar a los usuarios ni eludir las defensas del sistema; en cambio, simplemente se lanzan contra una red de manera directa y sin sutilezas. Jumbo Delgado, R. V. (2019). Su fuerte o su característica principal está en el método de ataque que implica la búsqueda de contraseñas mediante la prueba de todas las combinaciones posibles, ya sea de forma manual o utilizando extensas bases de datos de palabras. Estos ataques son comúnmente empleados para el robo de contraseñas en línea, ya que no requieren un alto grado de conocimiento en seguridad informática; existen programas automatizados que realizan esta tarea con relativa facilidad. Sin embargo, el tiempo necesario para este proceso puede variar considerablemente según la complejidad y longitud de la contraseña, pudiendo extenderse durante varias horas. Rosas Paredes, K. (2020).

Lo que busca este ataque es intentar diferentes combinaciones de claves desde un conjunto predefinido (diccionario) o generarlas de manera aleatoria (fuerza bruta) para encontrar la correcta mediante ensayo y error. Medina Rojas, J. D., y Rivas Montalvo, Y. Y. (2020).

Otro ataque que se encuentra en esta investigación y es conocida como **Ataque de suplantación de identidad** se conoce como los métodos de phishing que adoptan diversas modalidades, pero comparten un objetivo común: persuadir a individuos reales para que divulguen información confidencial. Estas tácticas suelen resultar más efectivas que otros métodos de

intrusión de datos, ya que aprovechan la interacción humana para alcanzar sus objetivos. Cuvi Mencias, B. M. (2023).

Existen dos tipos principales de ataques de suplantación de identidad: los **ataques de dirección MAC y los ataques a las tablas ARP**. El primero implica cambiar la dirección MAC de un dispositivo para hacerse pasar por otro. El segundo consiste en enviar mensajes ARP falsificados a la red WLAN para asociar la dirección IP del atacante con la de la víctima. El objetivo de ambos ataques es el mismo: hacerse pasar por un usuario con acceso a la red para obtener permisos o mantenerse en el anonimato. Esteban Sánchez, J. (2021).

Finalmente se encuentra que los ciberdelincuentes tienen la capacidad de generar puntos de acceso falsos que imitan a redes Wi-Fi legítimas gratuitas. Esto puede inducir a los usuarios a conectarse inadvertidamente a una red fraudulenta, permitiendo así que los hackers intercepten y accedan a la información de los usuarios. Este escenario aumenta el riesgo de robo de identidad y otros tipos de actividades delictivas en línea. Jumbo Delgado, R. V. (2019).

Una investigación que se realizó sobre este ataque saca el resultado de la explotación de 10 vulnerabilidades encontradas en los componentes clave, con una en el punto de acceso y nueve en el cliente. Por lo tanto, es crucial que los clientes estén actualizados con los últimos parches de seguridad para prevenir tales ataques. Pau García, E. (2019). Este resultado de la investigación es fundamental, especialmente en el contexto de los sistemas operativos sin licencias, ya que presentan muchas falencias en materia de seguridad.

Su principal operación es verificar cada vez que el cliente se conecte al punto de acceso recreado y se obtenga un handshake. En este momento, se evaluará si el cliente es susceptible o no a ser comprometido. Fernández-Oliva Madrigal, M. E. (2020).

Otro termino más común para la investigación sobre los ataques son los **ataques Phishing**,

los ataques, son una táctica utilizada para engañar a personas y obtener información confidencial, como credenciales de acceso, datos bancarios o de tarjetas de crédito, mediante técnicas de ingeniería social. Esto suele manifestarse a través de correos electrónicos no deseados, sitios web fraudulentos, mensajes electrónicos o instantáneos que aparentan ser de fuentes legítimas, como bancos o redes sociales. Collado Ramírez, B. (2021).

El objetivo es desviar el tráfico de clientes, ingresos o búsquedas hacia un sitio falso. Aunque está principalmente dirigido a tiendas en línea, el phishing también afecta a servicios financieros y otros sitios con un flujo constante de usuarios. Una estrategia común consiste en pagar para aparecer en los primeros resultados de los motores de búsqueda, lo que aumenta la confusión del usuario y lo dirige al sitio falso. (Rosas Paredes, K. 2020).

Los ataques phishing Se manifiestan a través de correos electrónicos no deseados, sitios web fraudulentos, mensajes electrónicos o instantáneos que aparentan ser de fuentes legítimas, como bancos o redes sociales. Collado Ramírez, B. (2021).

A continuación, se presentan otros ataques que registra la literatura, que, si bien no son tan frecuentes, son importantes resaltarlos como parte de estudio, en tanto, pueden ser posibles ataques que se pueden ir perfeccionando y evitar atacar las redes wifi pública. Además, lo que no se indica como objeto de estudio puede tener implicaciones a mediano y largo plazo, y son:

Ataques Comunes. **Falsos AP**, creación de un punto de acceso falso para engañar a los usuarios y robar información. Esteban Sánchez, (2021). Deauthentication Attack, obliga a clientes a autenticarse nuevamente, capturando el handshake. Esteban Sánchez, (2021). Ataques diccionario sobre el 4-way handshake, compara el handshake capturado con una lista de contraseñas para intentar recuperar la clave de acceso. Esteban Sánchez, (2021). ARP Spoofing, manipulación de las tablas ARP para interceptar tráfico. Quiña Haro, y Reza Zurita. (2022).

Software Malicioso. Rootkit, conjunto de herramientas diseñadas para encubrir intrusiones en un sistema operativo. Ovalle-Velez. (2019). Troyanos, se ocultan como programas benignos y comprometen la privacidad del usuario. Ovalle-Velez. (2019). Ransomware: Cifra archivos y exige rescate en criptomonedas. Ovalle-Velez. (2019).

Estrategias de Ciberseguridad. **Control de Acceso**, restringe acceso a dispositivos no autorizados, permitiendo solo acceso a ciertos sitios web. Salinas Valencia. (2021). Parches de seguridad: Archivos que corrigen vulnerabilidades en software. Ovalle-Velez. (2019). Mecanismos de autenticación SKA y OSA, mejoran la seguridad en redes mediante autenticación de estaciones y verificación de solicitudes.

Métodos de Engaño. **Espionaje**, obtención clandestina de información sobre un gobierno o empresa competidora. Lluís, G. y Alberto, L. (2022). Ladrones de identidad, obtienen información personal de manera deshonesta. Lluís, G. y Alberto, L. (2022). Baiting, propagación de malware a través de dispositivos de almacenamiento. Rosas Paredes. (2020).

Tipos de Ataques. **Ataque activo**, Alteración de la información transmitida. Jimenez Sanchez, (2019). Ataque pasivo, observación del tráfico sin alterar la información. Jimenez Sanchez, (2019). SQL Injection, Inserción de código dañino en bases de datos. Rosas Paredes, K. (2020). DDoS, Saturación de un servidor con tráfico no deseado. Rosas Paredes, (2020).

Vulnerabilidades de Contraseñas, Uso de contraseñas, a menudo el eslabón más débil en seguridad, comprometiendo la protección de los sistemas. Galego Carro, (2019).

Seguridad en Redes. **Ataque Sniffer,** software especializado en capturar y analizar paquetes de datos en redes. Guallasamín Haro, y Santos Guerrero, (2022). Ataque Evil Twin, creación de un punto de acceso falso que imita el original. Pau García, (2019). Ataque a WPS, utilización de fuerza bruta para descifrar la clave de WPS. Pau García, (2019).

Otras Amenazas y Vulnerabilidades. **MAC Spoofing**, ocultar la dirección MAC original y sustituirla por otra. Medina Rojas, y Rivas Montalvo, (2020). Secuestro de sesión, obtención de información utilizando la identificación de sesión del usuario. Jumbo Delgado, (2019).

Técnicas de Intercepción. Ataques de Vigilancia, captura de datos en redes inalámbricas. Medina Rojas. y Rivas Montalvo, (2020). Info leaks, revelación de datos confidenciales de diversas fuentes. Rosas Paredes, (2020).

Para mitigar los riesgos asociados con el uso de redes públicas, es esencial que los usuarios tomen medidas preventivas que protejan su privacidad y seguridad en línea. Las redes públicas, como las de cafeterías, aeropuertos y otros lugares públicos, son vulnerables a los ciberataques debido a su naturaleza abierta y la falta de cifrado en la comunicación. Los ciberdelincuentes pueden aprovechar estas redes para interceptar datos sensibles, como contraseñas, números de tarjeta de crédito y otros detalles personales.

Una de las formas más efectivas de protegerse es evitar realizar transacciones sensibles, como compras en línea o accesos a cuentas bancarias, cuando se está conectado a una red pública. Incluso si es necesario hacer alguna transacción, se recomienda utilizar una herramienta de seguridad, como una red privada virtual (VPN). Una VPN crea una conexión cifrada entre el dispositivo del usuario y el servidor, lo que hace mucho más difícil que los atacantes puedan interceptar o manipular los datos transmitidos.

El uso de VPN no solo protege la confidencialidad de los datos, sino que también ayuda a ocultar la ubicación geográfica del usuario, lo que añade una capa adicional de privacidad. En resumen, para evitar los riesgos de seguridad asociados con las redes públicas, los usuarios deben ser conscientes de los peligros y adoptar soluciones como las VPN para cifrar sus conexiones y

proteger sus transacciones y datos sensibles.

Posibles Consecuencias que Generarían en la Red las Amenazas Identificadas

Las redes Wi-Fi públicas, aunque convenientes, presentan una serie de riesgos de seguridad que pueden comprometer la privacidad y la integridad de los datos de los usuarios. Estos riesgos incluyen la posibilidad de ataques de intermediarios (man-in-the-middle), donde un atacante intercepta la comunicación entre el usuario y el punto de acceso, así como la amenaza de redes maliciosas que se hacen pasar por redes legítimas. Además, la falta de cifrado en muchas de estas redes facilita que los atacantes accedan a información sensible, como credenciales de inicio de sesión y datos financieros, lo que pone en riesgo la seguridad personal y empresarial.

El análisis de los ataques específicos en redes Wi-Fi públicas ha revelado diversas técnicas utilizadas por los atacantes para explotar las vulnerabilidades de estas conexiones. Entre los métodos más comunes se encuentran la suplantación de redes, donde se crean puntos de acceso falsos para atraer a usuarios desprevenidos, y el uso de sniffers para capturar paquetes de datos no cifrados que circulan en la red. Además, se han identificado ataques de desautenticación, que permiten a los atacantes desconectar a los usuarios legítimos y obligarlos a conectarse a redes controladas por el atacante. Este análisis subraya la importancia de emplear medidas de seguridad adicionales, como el uso de VPN y protocolos de cifrado, para mitigar estos riesgos en entornos de red pública.

El Ataque Denegación de Servicio (DoS). Puede degradar el rendimiento de la red significativamente, e incluso llegar a interrumpir su funcionamiento total. Arango Gómez, (2023). Los usuarios podrían enfrentar desconexiones constantes, volviendo la red inestable e imposible de utilizar.

El Ataque Man-in-the-Middle. Compromete al usuario final mediante una conexión fraudulenta para apropiarse de sus datos. Almendral Fernández. (2020). Los atacantes pueden

obtener nombres de usuario, contraseñas y otras credenciales, así como interceptar y utilizar maliciosamente información financiera y personal.

El Ataque de Fuerza Bruta. Tiene como objetivo robar contraseñas y obtener acceso no autorizado a la red. Según Arango Gómez (2023), estos ataques se aprovechan de la conexión WiFi para sus propios propósitos, consumiendo el ancho de banda y reduciendo el rendimiento de la red.

Ataque de Suplantación de Identidad. Establecen puntos de acceso falsos que aparentan ser redes Wi-Fi gratuitas. Cuando los usuarios se conectan a una de estas redes fraudulentas sin darse cuenta, los delincuentes pueden interceptar su información. Esto puede llevar al robo de identidad y otros crímenes cibernéticos. Según Cuvi Mencias (2023), estos atacantes capturan datos sensibles como contraseñas, números de tarjetas de crédito, correos electrónicos y otra información personal.

El ataque KRACK. Compromete fácilmente la comunicación a través de redes Wi-Fi debido a la falta de parches de seguridad actualizados en los dispositivos. Según García (2019), este ataque permite interceptar y leer datos transmitidos por la red Wi-Fi, incluyendo contraseñas, números de tarjetas de crédito, mensajes y otros datos sensibles, siempre que no estén cifrados adicionalmente (como con HTTPS).

Los ataques de Phishing. Consisten en imitar la identidad de un usuario o empresa a través de medios electrónicos, como correos electrónicos o mensajería instantánea, con el objetivo de conseguir información personal y bancaria. Según Rosas Paredes (2020), estos ataques pueden llevar a la obtención de datos personales sensibles, como nombres y detalles financieros, así como a la instalación de virus, ransomware o spyware que pueden dañar o cifrar datos.

En el Acceso no Autorizado. Como otro de los ataques frecuentes, una persona sin

autorización puede acceder a la red, se infiltra en ella y sustrae información confidencial de los usuarios. Arango Gómez, (2023). Es este tipo de ataque quien roba la información, tienen la capacidad de vigilar las actividades en línea de los usuarios, como los sitios web que visitan, correos electrónicos y mensajes.

Es de resaltar que, en este mundo de la tecnología, se pueden presentar personas que se encargan de infiltrar la red con diversos objetivos, unos para proteger, para dañar y robar información, estos se reconocen como Hacker de Sombrero Blanco se dedica a la penetración y evaluación de seguridad, según Arcia Plua (2021). A diferencia de los hackers maliciosos, su objetivo es distinto: los hackers de sombrero blanco, o hackers éticos, se enfocan en identificar vulnerabilidades y fortalecer la seguridad.

Los Hackers de Sombrero Negro. Acceden ilegalmente a sistemas de información con intenciones maliciosas. Arcia Plua (2021). Buscan explotar vulnerabilidades para obtener beneficios propios o causar perjuicio.

Los Hackers de Sombrero Gris. Infringen la ley, aunque generalmente no lo hacen con intenciones maliciosas. puede acceder a una red Wi-Fi sin permiso, lo que constituye una violación de la privacidad y la seguridad. ARCIA PLUA, (2021). Después de acceder a una red Wi-Fi, un hacker de sombrero gris tiene la capacidad de capturar los datos que se están transmitiendo en la red. Esto puede abarcar correos electrónicos, mensajes de texto, credenciales de inicio de sesión, y otros datos confidenciales.

El ataque denominado "**Mora**" infecta dispositivos móviles como tablets y smartphones, afectando redes Wi-Fi al interceptar y manipular las comunicaciones inalámbricas entre los dispositivos, según Arias Silva (2019).

Un Ataque Jenx. Se centra en llevar a cabo ataques DDoS dirigidos a los dispositivos de

los jugadores Arias Silva, (2019), así como en la inyección de paquetes, la suplantación de identidad o la captura de tráfico.

El Ataque OMG. Permite el acceso remoto a dispositivos, lo que posibilita que un atacante redirija cualquier tipo de tráfico que pase por el dispositivo infectado. Además, este ataque facilita la interceptación y manipulación de la comunicación entre dispositivos en una red inalámbrica Arias Silva, (2019).

El Ataque Wicked. Se fundamenta en identificar enrutadores Netgear con vulnerabilidades específicas; una vez comprometidos, estos dispositivos descargan y ejecutan malware que genera nuevas botnets. Según Arias Silva (2019), el proceso implica explotar debilidades en el protocolo de comunicación de redes inalámbricas, aprovechando fallos en la autenticación y la encriptación para vulnerar la seguridad.

Un Ataque Sora. Intenta obtener acceso a dispositivos vulnerables mediante ataques de fuerza bruta. Una vez que accede remotamente, puede ejecutar comandos para descargar y gestionar el binario Arias Silva (2019). Este tipo de ataque se enfoca en la manipulación y explotación de protocolos de comunicación inalámbrica.

Los Ataques de Interceptación de Tráfico. Permiten a los atacantes desviar el tráfico del sitio web de la institución educativa hacia un sitio web fraudulento que podría contener malware o phishing. Cuvi Mencias (2023). Estos ataques implican la captura y el análisis de los datos transmitidos a través de una red inalámbrica.

Los atacantes crean un punto de acceso falso que imita a una red Wi-Fi legítima y confiable para engañar a los usuarios y lograr que se conecten a él, permitiéndoles así robar información. Sánchez (2021).

Un Ataque Sniffer. Tiene como objetivo extraer datos confidenciales, incluyendo

información de cada usuario y sus contraseñas. Estos proyectos son valiosos para identificar problemas de seguridad en las comunicaciones y mejorar el control de la red. Según Guallasamín Haro y Santos Guerrero (2022), se trata de capturar y analizar los paquetes de datos transmitidos a través de una red inalámbrica.

Un Ataque de Secuestro de Sesión. Ocurre cuando los hackers logran suplantar la identidad de su computadora o teléfono móvil, robando información de las sesiones activas y luego accediendo a datos en otros servidores. Esta técnica avanzada de hacking puede resultar en la pérdida de datos Jiménez Sánchez, (2019). Los atacantes interceptan y capturan las cookies de sesión, lo que les permite acceder a cuentas de redes sociales, correo electrónico, cuentas bancarias y otros servicios en línea como si fueran el usuario legítimo.

Los ladrones de identidad obtienen datos personales de manera engañosa, tales como el nombre, la dirección, el número de la Seguridad Social y el correo electrónico Lluís y Alberto, (2022). Luego, el atacante usa esta información para hacerse pasar por la persona afectada.

Los Ataques AP. Se basan en replicar la configuración de puntos de acceso auténticos con el propósito de engañar a los clientes. Según Medina Rojas y Rivas Montalvo (2020), un cibercriminal puede establecer un punto de acceso Wi-Fi que aparenta ser legítimo, pero está realmente diseñado para interceptar y manipular el tráfico de los usuarios que se conectan a él.

Los Parches de Seguridad. Están diseñados para corregir deficiencias, vulnerabilidades o fallos en el funcionamiento. Ovalle Vélez (2019). Los dispositivos que no se han actualizado con los últimos parches de seguridad pueden ser explotados a través de vulnerabilidades conocidas.

El Ataque de Tipo Troyano. Es un programa que llega al ordenador de forma disimulada, haciéndose pasar por algo inofensivo. Una vez instalado, lleva a cabo acciones que comprometen la privacidad del usuario afectado. Según Ovalle Vélez (2019), estos ataques pueden capturar

nombres de usuario, contraseñas y otros datos de inicio de sesión, lo que posibilita a los atacantes acceder a cuentas bancarias, correos electrónicos, redes sociales y otros servicios en línea.

El Ransomware. Se infiltra en el ordenador de la víctima y cifra su información, bloqueando el acceso a archivos importantes como documentos, fotos y videos. Luego, exige el pago de un rescate en Bitcoins a través de mensajes emergentes para recuperar los archivos cifrados Ovalle Vélez, (2019).

Un Ataque DDoS. (Denegación de Servicio Distribuida) implica bloquear el acceso a un sitio web mientras se ataca simultáneamente al servidor con una gran cantidad de datos irrelevantes, como el llenado de formularios con información falsa o el envío masivo de solicitudes Rosas Paredes, (2020). Esto puede saturar la infraestructura de una red Wi-Fi pública, ocasionando su caída o un rendimiento extremadamente lento, lo que impide a los usuarios conectarse o utilizarla de manera efectiva.

Como se puede evidenciar, son muchas las consecuencias que se pueden presentar por los ataques en las redes Wifi-Públicas, colocando en alta vulnerabilidad no solo a las personas sino a las instituciones lo que conlleva riesgos en datos altamente sensibles, la pérdida de datos y por ende de la privacidad, además de los costos económicos por los daños de los dispositivos.

Existen otros ataques que se evidencian en los textos estudiados, sin embargo, no manifiestan las consecuencias que se pueden presentar, ellos son: Evil Twin, Baiting, Info leaks, Ataque beck-tews y ohigahi-morri, Ataque chopchop, rootkit, es importante nombrarlos y tenerlos presentes, en tanto, son una amenaza latente que se pueden convertir en objeto de estudio de otras investigaciones a mediano y corto plazo.

Las amenazas identificadas en una red pueden tener diversas consecuencias graves que afecten su funcionalidad y seguridad. Una de las principales consecuencias sería la interrupción

del servicio, lo que podría resultar en la caída de sistemas críticos, afectando la operatividad de las organizaciones y la disponibilidad de los recursos. Esto podría generar una pérdida significativa de datos, con la consecuente dificultad para recuperar la información valiosa. Además, los ataques como el ransomware o las infecciones de malware pueden propagarse rápidamente, bloqueando el acceso a servicios y exponiendo los sistemas a riesgos de filtración de información sensible.

Otra consecuencia importante es el daño a la reputación de las entidades afectadas. Los usuarios y clientes pueden perder confianza en la capacidad de la organización para proteger sus datos e información personal, lo que puede resultar en una pérdida de clientes y, en algunos casos, en acciones legales por negligencia en la protección de datos. Además, los costos financieros asociados con la respuesta ante un ataque, como la recuperación de sistemas, la implementación de medidas correctivas y las posibles sanciones, pueden ser elevados. En resumen, las amenazas a las redes no solo impactan la infraestructura tecnológica, sino también la estabilidad económica y la confianza en la organización.

Herramientas de Mayor Eficiencia para la Prevención de los Ataques en las Redes Wifi-Públicas

En este capítulo final se presentan las herramientas más efectivas para mejorar la seguridad en redes Wi-Fi públicas que evidencian los textos estudiados, con el fin de prevenir ataques cibernéticos. Esto implica evaluar distintas soluciones tecnológicas, como sistemas de detección de intrusiones y protocolos de cifrados avanzados, para recomendar las mejores prácticas y herramientas que garanticen una protección robusta contra amenazas comunes en estos entornos vulnerables.

La literatura analizada para este estudio logró identificar los siguientes programas que sirven para prevenir, minimizar y corregir los ataques cibernéticos, a continuación, se hace la descripción de cada uno de ellos con sus respectivas características y usos.

TamoSoft Throughput Test y TamoSoft COMN View for Wi-fi 6

TamoSoft Throughput Test. Es un software de utilidad para probar el rendimiento de una red inalámbrica o cableada. Esta utilidad envía continuamente flujos de datos TCP y UDP a través de su red y calcula métricas importantes, como valores de rendimiento ascendente y descendente, pérdida de paquetes y tiempo de ida y vuelta, y muestra los resultados en formatos numéricos y gráficos. La prueba de rendimiento de TamoSoft admite conexiones IPv4 e IPv6 y permite al usuario evaluar el rendimiento de la red según la configuración de calidad de servicio (QoS) p14 Zambrano Arellano, (2022). es útil en la seguridad de la red principalmente porque ayuda a garantizar que la red esté funcionando eficientemente y de manera estable, lo que es un componente clave en la protección contra posibles amenazas.

TamoSoftCOMNViewforWi-fi6. Es un poderoso monitor de red inalámbrica y analizador de redes 802.11 a/b/g/n. Cargado con muchas características fáciles de usar, CommView for WiFi

combina rendimiento y flexibilidad con una facilidad de uso incomparable en la industria. CommView for WiFi capta todos los paquetes en el aire para mostrar información importante como la lista de puntos de acceso y estaciones, por nodo y las estadísticas por canal, potencia de la señal, una lista de paquetes y conexiones de red, protocolo de distribución gráficos, etc. p17 Zambrano Arellano, (2022). es una herramienta fundamental para la seguridad de redes inalámbricas, ya que ofrece capacidades de monitoreo, detección de intrusos, análisis de protocolos, y auditoría de seguridad, todo adaptado a las características avanzadas del estándar Wi-Fi 6.

Usar una **VPN** aporta seguridad extra: a pesar de que no consiga proteger al usuario si cae en algún engaño de suplantación web, una VPN cifrará el tráfico que genere, haciendo más difícil para un posible atacante sacar información valiosa P72 Verde Costas, (2022). Usar doble factor de autenticación nos ayuda evitar que los atacantes puedan usar esas credenciales para iniciar sesión donde corresponda, es muy útil implementar el Two-factor authentication (2FA). De esta manera, aunque hayan robado información valiosa de un usuario, no podrán utilizarla P72 Verde Costas, (2022). Desactivar auto-conexión a redes disponibles es inevitable que un atacante clone una red real y la inunde (si así lo quiere) para echar a los usuarios de ella y así se vean tentados a conectarse al clon. P72" Verde Costas, (2022).

Kali Linux, Wifislax, Obtención de claves (Vulneración con Wifislax)

Kali Linux Kali (antes conocida como Backtrack). Es una distribución de Linux que posee todo tipo de herramientas preinstaladas que sirven para realizar Penetration Testing. Posee un menú muy extenso con más de 300 herramientas para pentesters y se las puede categorizar de la siguiente manera: information gathering (son herramientas orientadas a la recolección de datos que ofrecen información sobre los objetivos, especialmente herramientas de DNS, dominios y

direcciones IP. Vargas, Guarda, Muyón, y Quiña, (2019). es una distribución de Linux diseñada específicamente para realizar pruebas de penetración y auditorías de seguridad en redes y sistemas. Ofrece una amplia gama de herramientas preinstaladas para análisis de vulnerabilidades, pruebas de penetración, y evaluación de seguridad, lo que permite a los profesionales identificar y corregir fallos de seguridad antes de que puedan ser explotados. Además, su entorno personalizable facilita la automatización de tareas y la creación de scripts personalizados. Es una herramienta esencial para cualquier profesional de ciberseguridad que busque fortalecer la seguridad de una red.

Wifislax. El software **wifislax** una distribución Gnu/Linux basada en Slackware y especializada en la auditoria de redes inalámbricas además de poseer herramientas de gestión y uso cotidiano como, Reparadores de arranque, procesadores de texto, etc. Vargas, Guarda, Muyón, & Quiña, (2019). es una distribución de Linux enfocada en la auditoría y seguridad de redes inalámbricas. Está equipada con diversas herramientas para la prueba de seguridad en redes Wi-Fi, permitiendo a los usuarios realizar ataques de penetración, auditorías de seguridad y recuperación de contraseñas. Sus beneficios incluyen la detección de vulnerabilidades en redes inalámbricas, pruebas de robustez de contraseñas, y análisis de la configuración de seguridad de puntos de acceso. Es útil para identificar y corregir posibles debilidades en la seguridad de redes Wi-Fi antes de que sean explotadas.

Obtención de claves (Vulneración con Wifislax) Este proceso se basa en trabajar con herramientas para vulnerar al protocolo WPS (WiFi Protected Setup) en redes WPA (Wi-Fi Protected Access) para la obtención de la clave de acceso a la red inalámbrica. Vargas, Guarda, Muyón, & Quiña, (2019).

En NetSurveyor. Es una herramienta 802.11 (wifi) descubrimiento de la red que reúne información sobre los puntos de acceso inalámbricos cercanos en tiempo real y la muestra en

formas útiles. Con un propósito similar a NetStumbler, que incluye muchas más 5 características. Los datos se muestran utilizando una variedad de diferentes puntos de vista diagnóstico y gráficos. Los datos pueden ser registrados por períodos prolongados y reproducida en una fecha posterior/hora. Además, los informes se pueden generar en formato PDF de Adobe p4 Sanchez Ramirez, (2019).es una herramienta de análisis y monitoreo de redes inalámbricas que ayuda a identificar y diagnosticar problemas en la red Wi-Fi. Permite visualizar el rendimiento de la red, identificar interferencias, y analizar la cobertura y la calidad de la señal. Los beneficios incluyen la detección de puntos de acceso no autorizados, optimización del uso de canales, y mejora de la cobertura y rendimiento de la red. Es una herramienta valiosa para asegurar que la red Wi-Fi opere de manera eficiente y segura, minimizando riesgos de seguridad asociados con configuraciones inadecuadas.

InSSider. Es una solución de problemas wifi y una herramienta de optimización que lleva la administración de pequeña red wifi a un nivel completamente nuevo. Con un rápido vistazo, se podrá encontrar la colocación deficiente del canal, baja intensidad de la señal y la interferencia en las bandas de 2,4 y 5 GHz. p5 Sanchez Ramirez, (2019). permite evaluar la fuerza de la señal, la congestión de canales, y la configuración de seguridad de las redes inalámbricas. Facilita la identificación de problemas como interferencias de señal y la competencia entre redes en el mismo canal. Los beneficios incluyen la optimización de la configuración del router para mejorar la cobertura y el rendimiento, la identificación de posibles puntos de acceso no autorizados, y la verificación de la seguridad de la red. Es útil para asegurar un entorno Wi-Fi más robusto y seguro.

Ekahau HeatMapper. Proporciona una vista a nivel del suelo de la WLAN cobertura y el rendimiento basado en los datos recogidos durante las encuestas pasivos y activos. También es capaz de realizar encuestas predictivas que facilitan la planificación de WLAN en la etapa previa

al despliegue. Además, la aplicación es capaz de realizar análisis de espectro, lo que requiere un analizador de espectro basados en USB. Ekahau Site Survey está optimizado para redes wifi 802.11n de gestión centralizada. Ekahau también ofrece una, a escala reducida herramienta de estudio del sitio básico llamado HeatMapper y una herramienta de evaluación WLAN básico para teléfonos inteligentes y tablets basados en Android llamada Ekahau Mobile Survey p5 Sanchez Ramirez, (2019). herramienta gratuita para mapear la cobertura de señal Wi-Fi en tiempo real. Permite visualizar la distribución de la señal en un plano, identificando áreas con cobertura deficiente o interferencias. Sus beneficios incluyen la optimización de la colocación de puntos de acceso, mejora de la cobertura de la red, y detección de problemas que podrían comprometer la seguridad o el rendimiento de la red Wi-Fi.

Vistumbler. Utiliza la API de Windows nativo wifi o netsh para encontrar los puntos de acceso y obtener la información inalámbrica, soporte GPS basado COM descodificadores de NMEA, puntos de exportación/importación de acceso de Vistumbler TXT/VS1/o VSZ Netstumbler TXT/NS1 texto, exportación punto de acceso ubicaciones GPS a un archivo KML de Google Earth o GPX (GPS exchange format), muestra automáticamente los puntos de acceso en Google Earth. Además, es una herramienta Open Source p6 Sanchez Ramirez, (2019). herramienta de código abierto para escanear y visualizar redes Wi-Fi cercanas. Permite identificar redes disponibles, analizar la intensidad de la señal, y verificar la configuración de seguridad, como el tipo de cifrado utilizado. Sus beneficios incluyen la detección de redes inseguras o mal configuradas, la identificación de puntos de acceso no autorizados, y la optimización de la señal y seguridad de la red Wi-Fi. Es útil para asegurar una red inalámbrica frente a posibles amenazas y mejorar su rendimiento.

WiFi SiStr. Es una pequeña utilidad bastante simple que permite determinar la intensidad de señal de una red inalámbrica. Funciona en Windows 2000 y XP (Escuela Politécnica Superior de la Universidad de Alicante, 2015). P6 Acrylic WiFi versión Free. Con Acrylic WiFi Home se puede ver y escanear las redes wifi que hay al alcance, obtener información de seguridad de la red y obtener contraseñas wifi-genéricas gracias un sistema de plugin incluido, incluso en redes 802.11ac. Acrylic WiFi es un scanner wifi gratis para Windows. P6 Sanchez Ramirez, (2019). es una herramienta para escanear y analizar redes Wi-Fi, proporcionando información sobre la intensidad de la señal, la configuración de los puntos de acceso, y el tipo de cifrado utilizado. Facilita la identificación de redes cercanas y ayuda a detectar posibles problemas de seguridad, como redes abiertas o mal configuradas. Sus beneficios incluyen la optimización de la seguridad y el rendimiento de la red, así como la mejora en la cobertura al identificar interferencias o puntos débiles en la señal.

El programa Nessus. Tiene como función escanear las vulnerabilidades de varios sistemas operativos, es un proceso especial que se ejecuta en segundo plano, mostrando el avance del escaneo del sistema. Salinas Valencia, (2021). identifica y evalúa debilidades en sistemas y redes. Realiza análisis exhaustivos para detectar fallos de seguridad, configuraciones incorrectas y vulnerabilidades conocidas. Sus beneficios incluyen la detección proactiva de amenazas, la mejora de la seguridad mediante la corrección de vulnerabilidades antes de que puedan ser explotadas, y la generación de informes detallados para gestionar riesgos y cumplir con normativas de seguridad.

Sistemas de detección y prevención de intrusos (IDS/IPS) Herramientas de análisis de registro Herramientas de análisis de, tráfico Sistemas de gestión de información de seguridad (SIEM) p70

son herramientas que monitorean el tráfico de red en busca de actividades sospechosas o maliciosas, como ataques de denegación de servicio (DDoS). P70 Arango Gomez, (2023).

OpenWRT. Es un sistema operativo basado en Linux dirigido a dispositivos embebidos, el cual proporciona un sistema totalmente libre de la selección y configuración de la aplicación proporcionada por el proveedor, que permite personalizar el dispositivo mediante el uso de paquetes para adaptarse a cualquier aplicación como el marco para crear una aplicación sin tener que crear un firmware completo a su alrededor, esto para los usuarios significa tener la posibilidad de una personalización completa de los puntos de accesos de formas nunca imaginadas p38 Collado Ramírez, (2021). un sistema operativo basado en Linux para routers y dispositivos de red, que permite una personalización y configuración avanzada de la red. Ofrece herramientas para mejorar la seguridad, como cortafuegos configurables, VPN y controles de acceso detallados. Sus beneficios incluyen la capacidad de reforzar la seguridad del router, adaptar la red a necesidades específicas, y mejorar el rendimiento mediante la optimización del firmware y la gestión avanzada del tráfico.

802.11w. Este es un protocolo para la seguridad que utiliza un mecanismo mejorado, denominado Temporary Safe Tunnel (TST), combina la criptografía de clave pública y el sistema de almohadilla de un solo uso. Dado que se diseñó meticulosamente, su costo es lo suficientemente bajo, provee mecanismos que brindan protección a las tramas de unidifusión y las tramas de difusión / multidifusión, que también otorga un método denominado BIP (Protocolo de integridad de difusión / multidifusión), para proporcionar integridad a las tramas de difusión / multidifusión p39 Collado Ramírez, (2021).

WIPS. Como lo indica su nombre en inglés -Wireless Intrusion Prevention System-, es un sistema para la prevención de intrusos en las redes inalámbricas, el cual debe brindar protección

contra ataques de DoS, spoofing de direcciones MAC, monitoreo de tráfico, protección para proporcionar comunicaciones seguras entre cada sensor y servidor para evitar la manipulación por parte de un atacante, entre otras funciones más a nivel de prevención de ataques p39 Collado Ramírez, (2021). es una herramienta diseñada para detectar y prevenir intrusiones en redes inalámbricas. Monitorea el tráfico de la red Wi-Fi para identificar actividades sospechosas, ataques o accesos no autorizados. Sus beneficios incluyen la protección contra amenazas como ataques de man-in-the-middle y acceso no autorizado, la mejora de la seguridad de la red inalámbrica mediante la respuesta automática a incidentes, y la reducción del riesgo de comprometer datos sensibles.

WIDS. Este mecanismo de defensa, como su nombre en inglés lo indica -Wireless Intrusion Detection System-, es un sistema para la detección de intrusos en las redes inalámbricas p40 Collado Ramírez, (2021).

Cambiar Contraseñas Impuestas

Muchas de las empresas asignan las **contraseñas** a su modo, y muchas de las veces tienen patrones específicos los cuales, son una gran debilidad porque pueden ser susceptibles a ataques de fuerza bruta, se recomienda que si se tiene una red con una contraseña por default del proveedor sea cambiada de manera inmediata. Implementación de contraseñas fuertes. Este es de los menores controles disponibles para la seguridad de las redes. P62 Duque, y Rojas, (2019).

Configuración del cifrado de red, Doble autenticación, Ocultación de SSID, Filtrado de direcciones Mac, Reducción del rango, P63, Siempre tener activo un cortafuego (Firewall). No dejar la red inalámbrica encendida cuando no se esté usando P64 Duque, y Rojas, (2019).

La prevención de ataques en redes WiFi públicas es esencial para proteger la privacidad y seguridad de los usuarios. Una de las herramientas más eficaces en este sentido es el uso de

protocolos de seguridad robustos, como WPA3, que mejora la encriptación de las conexiones WiFi y dificulta el acceso no autorizado a la red. Además, el uso de VPN (Red Privada Virtual) es altamente recomendable, ya que cifra todo el tráfico de datos entre el dispositivo del usuario y el servidor al que se conecta, impidiendo que los atacantes intercepten información sensible. Otra herramienta importante es la autenticación multifactor (MFA), que añade una capa extra de seguridad, dificultando el acceso a la red incluso si un atacante obtiene las credenciales del usuario.

Adicionalmente, la implementación de sistemas de detección y prevención de intrusiones (IDS/IPS) permite monitorear y bloquear posibles amenazas en tiempo real. Los puntos de acceso deben estar configurados para deshabilitar la difusión de SSID (nombre de la red), lo que reduce la posibilidad de que los atacantes localicen y se conecten a la red. Asimismo, las redes públicas deben ser segmentadas, de modo que los dispositivos conectados no puedan acceder directamente entre sí, limitando la propagación de ataques. Finalmente, educar a los usuarios sobre los riesgos de conectarse a redes WiFi públicas y fomentar el uso de conexiones seguras como HTTPS puede ser una herramienta complementaria crucial para minimizar los ataques.

Conclusiones

La presente investigación ha explorado a fondo el panorama de seguridad y los posibles ataques en redes WiFi-públicas, revelando una serie de desafíos significativos y estrategias para mitigarlos. En redes Wi-Fi públicas, los datos significativos incluyen información personal como nombres, direcciones, contraseñas, detalles bancarios y comunicaciones privadas, que pueden ser fácilmente interceptados por atacantes debido a la falta de seguridad en estas redes. Para mitigar los riesgos, es crucial utilizar herramientas como VPN (Redes Privadas Virtuales) para cifrar el tráfico de datos, impidiendo que los atacantes accedan a la información transmitida. Además, el uso de autenticación multifactor (MFA) y contraseñas fuertes aumenta la protección de las cuentas, mientras que la implementación de cifrado de extremo a extremo en aplicaciones de mensajería y correo electrónico garantiza que las comunicaciones sean ilegibles incluso si se interceptan. También es recomendable emplear navegadores seguros y mantener actualizado el software de seguridad para detectar y prevenir ataques maliciosos.

A través del análisis exhaustivo de literatura especializada, la experimentación práctica y la evaluación de medidas de seguridad, se ha llegado a varias conclusiones clave.

Se ha confirmado que las redes WiFi-públicas son inherentemente vulnerables a una variedad de ataques debido a su naturaleza abierta y la falta de control sobre quiénes acceden a ellas. Desde ataques de tipo "Man-in-the-Middle" hasta el robo de datos sensibles, estas redes son un blanco principal para los ciberdelincuentes que buscan explotar su debilidad en la seguridad.

se demuestra que la conciencia y la educación son componentes cruciales para protegerse de los ataques en redes WiFi-públicas. Los usuarios deben comprender los riesgos asociados con el uso de estas redes y adoptar prácticas de seguridad sólidas, como el uso de la VPN, la verificación de la autenticidad de las redes, y evitar la transmisión de información confidencial a

través de conexiones no seguras.

Se identifica que las medidas técnicas, como el cifrado de extremo a extremo y la implementación de autenticación robusta, son esenciales para fortalecer la seguridad de las redes WiFi-públicas. Las organizaciones y proveedores de servicios deben adoptar políticas de seguridad sólidas y mantenerse actualizados con las últimas tecnologías y protocolos de seguridad para garantizar la protección de los usuarios.

Asimismo, se ha destacado la importancia de la colaboración entre los distintos actores del ecosistema de seguridad cibernética, incluyendo a usuarios, empresas, gobiernos y organismos reguladores. Solo a través de un enfoque conjunto y coordinado se podrá hacer frente eficazmente a las amenazas en las redes WiFi-públicas y garantizar un entorno digital más seguro y protegido para todos.

Las herramientas más efectivas para proteger a los usuarios en redes públicas incluyen el uso de las VPN para cifrar la conexión y ocultar la identidad, la autenticación multifactor (MFA) para añadir una capa extra de seguridad, y el cifrado de extremo a extremo en comunicaciones para garantizar la privacidad de los mensajes. Además, el empleo de antivirus, firewalls personales y navegadores seguros ayuda a prevenir malware, intrusiones y el rastreo de datos. Junto con estas tecnologías, la educación en seguridad cibernética es crucial para que los usuarios reconozcan y eviten amenazas como el phishing. Combinando estas herramientas y enfoques, los usuarios pueden mejorar significativamente su protección en redes públicas.

Si bien las redes WiFi-públicas ofrecen una conveniencia indudable en términos de conectividad, también plantean serios riesgos para la seguridad de la información. Es imperativo que los usuarios y las partes interesadas tomen medidas proactivas para protegerse contra posibles ataques, y que las organizaciones implementen las medidas de seguridad adecuadas para mitigar

los riesgos asociados. Con un enfoque integral que abarque la conciencia, la educación y la tecnología, es posible minimizar las vulnerabilidades y salvaguardar la integridad de las comunicaciones en redes WiFi-públicas.

Referencias Bibliográficas

Álava, W. L. S., Rodríguez, A. R., Ávila, X. L. A., & Cornelio, O. M. (2022). Redes Inalámbricas, Su Incidencia En La Privacidad De La Información. Journal Techinnovation, 1(2), 104-109.

Ali, S., Osman, T., Mannan, M., & Youssef, A. (2019). On Privacy Risks Of Public Wifi Captive Portals. In Data Privacy Management, Cryptocurrencies And Blockchain Technology: ESORICS 2019 International Workshops, DPM 2019 And CBT 2019, Luxembourg, September 26–27, 2019, Proceedings 14 (Pp. 80-98). Springer International Publishing.

Almendral Fernández, P. (2020). Desarrollo De Portales Cautivos Wifi E Implicaciones En Seguridad (Bachelor's Thesis).

Arango Gomez, O. D. (2023). El ABC De La Seguridad Informática: Guía Práctica Para Entender La Seguridad Digital. Https://Www. Autoreseditores. Com/Libro/22997/Oscar-Dario-Arango-Gomez/El-Abc-De-La-Seguridad-Informatica-Guia-Practica-Para-Entender. Html.

ARCIA PLUA, A. A. (2021). Análisis De Tráfico De Datos En La Capa De Enlace De Redes Lan, Para La Detección De Posibles Ataque O Intrucciones Sobre Tecnologías Ethernet Y Wifi 802.11 En La Carrera De Ingeniería En Sistemas Computacionales De La Universidad Estatal Del Sur De Manabí (Bachelor's Thesis, Jipijapa. UNESUM).

Arias Silva, N. A. (2019). Análisis De Seguridad De Vulnerabilidades Y Ataques Presentados En 4 Dispositivos De Internet De Las Cosas.

Bono García, R. (2020). Redes Wifi: ¿Realmente Se Pueden Proteger?

Cataño, D. S. (2021). Método Para La Prevención Y Mitigación De Vulnerabilidades En Redes WI-FI[Monografía]. Repositorioinstitucionalunad.Https://Repository.Unad.Edu.Co/Handle/10596/44590

Chabla Peñarrieta, R. D. (2019). Análisis De Vulnerabilidades En Redes Inalámbricas Mediante Test De Intrusión Wifi-Pineapple Y Metodologías De Seguridad Informática Owisam Y Osstmm Para El Aeropuerto José Joaquín De Olmedo De La Ciudad De Guayaquil (Doctoral Dissertation, Universidad De Guayaquil. Facultad De Ciencias Matemáticas Y Físicas. Carrera De Ingeniería En Networking Y Telecomunicaciones).

Cieza Celis, J. A., & Ojeda Romero, A. J. (2022). Evaluación Del Desempeño De Protocolos De Seguridad Para Combatir Ataques En Redes Inalámbricas Wi-Fi.

Collado Ramírez, B. (2021). Creación De Un Sistema Para Mitigación De Ataques Tipo Spoofing En Dispositivos Y Redes Inalámbricas (Doctoral Dissertation, Universidad Cenfotec).

Cuvi Mencias, B. M. (2023). Análisis De La Vulnerabilidad Del Sistema De Conexión A La Red WI-FI Genérica De Un Instituto Educativo.

Díaz Amorín, J. (2023). Estudio De La Adopción De Los Estándares De Seguridad En Redes Wifi Domésticas.

Duque, S. & Rojas, Y. (2019). Fallas De Seguridad En Sistemas De Comunicación Inalámbricas. [Monografia, Universidad Nacional Abierta Y A Distancia UNAD]. Repositorio Institucional UNAD. Https://Repository.Unad.Edu.Co/Handle/10596/25971

Esteban Sánchez, J. (2021). Seguridad Actual En Redes Wifi.

Fernández-Oliva Madrigal, M. E. (2020). Vulnerabilidades En Redes Wifi.

Galeano, M. (2007). *Estrategias De Investigación Social Cualitativa. El Giro A La Mirada*. Medellín: La Carreta Editores.

Galego Carro, J. P. (2019). WIFI-HASHING: Recopilación Automatizada De Hashes Y Análisis De Patrones De Contraseñas En Redes Wi-Fi.

González Londoño, J. (2020). Estudio Del Estado Actual De La Seguridad Informática En Las Organizaciones De Colombia.

Guallasamín Haro, A. S., & Santos Guerrero, G. A. (2022). Análisis De Datos Y Hackeo Ético Para La Detección De Vulnerabilidades En La Red Wi-Fi Con Usuarios Del Laboratorio Iot De La Universidad Politécnica Salesiana (Bachelor's Thesis).

Guzmán Moreno, H. (2022). Hacking Wireless Usando Parrot Y Un Adaptador Inalámbrico.

How To Stay Safe On Public Wifi. (2019). USA Today Magazine, 147(2887), 6–7

Jaime Carrasco, L. G. Implementación De Un Software Libre Para Mejorar Las Vulnerabilidades De Redes Inalámbricas En La Seguridad De Información De La Escuela De Ingeniería De Sistemas De La ULADECH-Chimbote; 2017.

Jimenez Sanchez, J. F. (2019). Diagnóstico De Las Debilidades De La Estructura De La Red Inalámbrica Del Gad Del Cantón Montalvo (Bachelor's Thesis, Babahoyo, UTB 2019).

Jumbo Delgado, R. V. (2019). Análisis De Vulnerabilidades De Redes Inalámbricas Para Evitar La Inseguridad De La Información De Los Usuarios En El Laboratorio De Telecomunicaciones De La Carrera De Ingeniería En Computación Y Redes (Bachelor's Thesis, Jipijapa-Unesum).

Lluís, G., & Alberto, L. (2022). Estudio De Los Ataques Y Su Defensa En La Ingeniería Social.

Machuca Ramirez, J. F., & Ortegon Molina, J. D. (2019). Diagnostico De Riesgos Y Vulnerabilidades Generados Por Software Malicioso A La Red Wifi_Ucc_Estudiantes De La Universidad Cooperativa De Colombia Sede Bogota Basados En La Aplicación De La Norma ISO 27001: 2013.

Medina Rojas, J. D., & Rivas Montalvo, Y. Y. (2020). Evaluación Del Rendimiento De Un Sistema De Detección De Intrusos Para Redes Inalámbricas 802.11 Contra Ataques Informáticos.

Morejón Mosquera, T. S. (2022). Análisis Para La Implementación De Políticas Y Equipamientos Para Fortalecer Las Redes Inalámbricas De La UTB (Bachelor's Thesis, Babahoyo: UTB-FAFI. 2022).

Neninger, J. C. B., & Guerrero, J. L. P. (2023). Impacto En La Seguridad De Las Redes Inalámbricas. Journal Techinnovation, 2(1), 62-71.

Núñez López, S. D. L. A. (2024). Hacking Ético Para La Detección De Vulnerabilidades Mediante La Utilización De Herramientas Open Source En La Red Inalámbrica De La Unidad Educativa Pelileo (Bachelor's Thesis, Universidad Técnica De Ambato. Facultad De Ingeniería En Sistemas, Electrónica E Industrial. Carrera De Tecnologías De La Información).

Osorio Fajardo, D. E., & Rivera Molina, O. D. (2019). Estudio Del Funcionamiento De Los Puntos Wifi De La Ciudad De Latacunga (Bachelor's Thesis, Ecuador: Latacunga: Universidad Técnica De Cotopaxi (UTC).).

Otero Dans, A. (2021). Herramienta De Auditoría De Seguridad En Redes Inalámbricas Para Pequeñas Empresas.

Ovalle-Velez, A. K. (2019). Uso De Herramientas Informáticas Para Descubrir Vulnerabilidades En Las Redes Wifi Domésticas.

Pau García, E. (2019). Redes Wifi, ¿Realmente Se Pueden Proteger?

Perez, J. T. (2022). Análisis De Los Protocolos De Seguridad Inalámbrica Implementadas En Las Redes Wifi En La Ciudad De Bogotá. [Proyecto Aplicado]. Repositorio Institucional UNAD. Https://Repository.Unad.Edu.Co/Handle/10596/51604

Pipa Huamán, J. (2019). REDES INALÁMBRICAS (Doctoral Dissertation, UNIVERSIDAD NACIONAL DE EDUCACIÓN Enrique Guzmán Y Valle).

Poveda Espin, W. O., & Moreta Changoluiza, J. E. Implementación De Una Red Wifi Con Servidor Radius, Para Controlar El Acceso Y Mejorar La Seguridad De La Red Inalámbrica Presente En La Sala De Docentes De La Unidad Educativa "Camino Del Inca".

Quiña Haro, E. D., & Reza Zurita, C. P. (2022). Análisis De Vulnerabilidades En La Comunicación Inalámbrica Utilizando El Esp32 Para Mitigar Intrusiones (Bachelor's Thesis).

Rodrigo García, J. (2022). Entorno Para La Concienciación De Riesgos De Seguridad En Redes Inalámbricas Compartidas.

Rodríguez Correa, J. R. (2019). WI-ME: Sistema De Medición De Seguridad De Redes Inalámbricas Con Protocolo WEP, WPA Y WPA2 Utilizando Wardriving, Wireless Penetration Testing Y Otras Herramientas En Un Sector Del Distrito De Víctor Larco Herrera-Trujillo.

Rosas Paredes, K. (2020). Análisis Exploratorio De Ataques Informáticos Aplicando Herramientas De Minería De Datos, Para La Gestión De La Seguridad De Redes Inalámbricas En Universidades De Arequipa.

Rosas Paredes, K. (2020). Análisis Exploratorio De Ataques Informáticos Aplicando Herramientas De Minería De Datos, Para La Gestión De La Seguridad De Redes Inalámbricas En Universidades De Arequipa.

Salinas Valencia, F. A. (2021). Análisis De Vulnerabilidad De La Red Wifi, Del Departamento De TICS Del GAD Municipal Del Cantón Baba (Bachelor's Thesis, BABAHOYO: UTB, 2021).

Salinas Vasquez, R. I. (2023). Análisis De Las Vulnerabilidades Del Protocolo De Seguridad WPA Y WPA2 En Redes Inalámbricas (Bachelor's Thesis, La Libertad: Universidad Estatal Península De Santa Elena, 2023).

Sanchez Ramirez, R. (2019). Redes Wireless.

Susanto, A., & Raharja, W. K. (2021). Simulation And Analysis Of Network Security Performance Using Attack Vector Method For Public Wifi Communication. The IJICS (International Journal Of Informatics And Computer Science), 5(1), 7-15.

Vargas, G., Guarda, T., Muyón, C., & Quiña, G. N. (2019). Obtención De Claves En Redes WLAN/WPS Usando Wifislax Y Denegación De Servicios Con Kali Linux. Revista Ibérica De Sistemas E Tecnologias De Informação, (E18), 318-331.

Velez, A. K. O. (2019). Uso De Herramientas Informáticas Para Descubrir Vulnerabilidades En Las Redes Wifi Domesticas (Doctoral Dissertation, Universidad Católica De Colombia).

Verde Costas, I. (2022). Análisis De Riesgos De Conexión A Redes Públicas.

Vivar Franco, I. A. (2023). Aplicación De Hacking Ético Para Identificar Amenazas, Riesgos Y Vulnerabilidades En La Red Wifi (Bachelor's Thesis, Babahoyo: UTB-FAFI. 2023).

Yisselpape. (2022). Hidalgo County Brings Free, Public Wifi To Students And Workers. American City & County Exclusive Insight, N.PAG.

Zambrano Arellano, D. N. (2022). Estudio Preliminar De La Implementación De WIFI 6 Para Las Estaciones De Metrovía Cerro Mapasingue-Dolores Sucre Y Prosperina (Doctoral Dissertation).