Estudio ético sobre las percepciones de los usuarios de las redes Wi-Fi públicas: Caso práctico Quevedo

William Guaranda[1], Charles Lopez[1], Dexy Reyes[1] y Jordy Zamora[1]
[1] Facultad de Ciencias de la Ingeniería, Universidad Técnica Estatal de Quevedo

***Resumen*—El uso de redes Wi-Fi públicas ha crecido en entornos urbanos, académicos y comerciales, facilitando el acceso a Internet, pero también exponiendo a los usuarios a riesgos. Este estudio analiza las percepciones de los usuarios de redes Wi-Fi públicas en la ciudad de Quevedo, Los Ríos, Ecuador, con un enfoque en los desafíos de ciberseguridad y las implicaciones éticas del uso de estas conexiones. Mediante encuestas aplicadas en universidades y centros comerciales, se identificaron niveles de conocimiento sobre los riesgos, prácticas de seguridad adoptadas y la percepción de responsabilidad tanto de usuarios como de administradores de redes. Los resultados revelan una alta dependencia de estas redes, pero con un bajo nivel de conciencia sobre sus vulnerabilidades, lo que resalta la necesidad de estrategias educativas y medidas de protección más efectivas.**

***Index Terms*—Redes Wi-Fi públicas, percepción de usuarios, implicaciones éticas.**

I. Introducción

En la era digital, las redes Wi-Fi públicas se han convertido en un pilar fundamental de la conectividad en entornos urbanos y académicos. Su accesibilidad permite a los usuarios navegar por Internet sin costos adicionales, pero también los expone a riesgos significativos debido a vulnerabilidades en los protocolos de seguridad, la falta de autenticación robusta y la posibilidad de explotación de datos personales [1]. Estos riesgos son especialmente críticos en espacios de alta concurrencia, como universidades y centros comerciales, donde miles de personas se conectan diariamente sin contar con medidas de protección adecuadas [2].

A lo largo de los años, los estándares Wi-Fi han evolucionado con el objetivo de mejorar la seguridad. El protocolo inicial, *Wired Equivalent Privacy (WEP)*, rápidamente demostró ser insuficiente ante ataques que comprometían su cifrado [3]. Como respuesta, se introdujeron *Wi-Fi Protected Access (WPA)* y posteriormente *Wi-Fi Protected Access 2 (WPA2)*, el cual implementó el *handshake* de cuatro pasos para la autenticación de dispositivos [4]. Sin embargo, WPA2 también presentó vulnerabilidades, como el *Key Reinstallation Attack (KRACK)*, que permitía la interceptación y manipulación de datos [5].

Para mitigar estas amenazas, el estándar *Wi-Fi Protected Access 3 (WPA3)* incorporó mecanismos de autenticación más robustos, mejorando la protección frente a ataques *Man-in-the-Middle (MITM)* y ataques de diccionario offline [6]. Adicionalmente, se desarrolló el protocolo *Wi-Fi CERTIFIED Enhanced Open*, diseñado para mejorar la seguridad en redes públicas mediante el cifrado individual de conexiones [7].

A pesar de estos avances, múltiples estudios han evidenciado que muchas redes públicas continúan operando sin cifrado adecuado, exponiendo a millones de usuarios a ataques cibernéticos [8]. Un estudio en Moscú reveló que el 25 % de las redes públicas carecían de medidas de seguridad apropiadas, mientras que un análisis global identificó vulnerabilidades críticas en 19 millones de puntos de acceso Wi-Fi [9]. En países como Estados Unidos y Alemania, se han implementado iniciativas para fortalecer la seguridad de estas redes mediante la adopción de protocolos avanzados y campañas de concienciación sobre ciberseguridad [6].

En Ecuador, espacios como centros comerciales, parques públicos y universidades ofrecen redes Wi-Fi públicas para sus usuarios. Sin embargo, la falta de medidas de protección adecuadas podría facilitar la interceptación de datos sensibles, incrementando el riesgo de ataques cibernéticos [1].

Dado este contexto, el presente estudio se desarrollará en la ciudad de Quevedo, provincia de Los Ríos, Ecuador, centrándose en tres ubicaciones clave: los Campus Central y La María de la Universidad Estatal de Quevedo (UTEQ, https://www.uteq.edu.ec/) y el Centro Comercial Paseo Shopping (https://www.elpaseoshopping.com/quevedo).

El objetivo principal es analizar la percepción de los usuarios sobre los riesgos asociados al uso de redes Wi-Fi públicas y evaluar las implicaciones éticas de sus prácticas de seguridad. A través de este estudio, se busca generar conciencia sobre la importancia de implementar medidas de protección efectivas y fomentar el uso responsable de estas redes en entornos académicos y urbanos.

II. Revisión del Estado del Arte

En esta sección se presenta una revisión del estado del arte sobre la seguridad en redes Wi-Fi públicas, abordando los principales riesgos de seguridad, los principios éticos relacionados con la ciberseguridad y la percepción de los usuarios frente a estas amenazas.

Para la selección de los artículos, se consultaron las principales bases de datos académicas, incluyendo IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library y Scopus. Se priorizaron estudios recientes y relevantes.

II-A. Riesgos de Seguridad en Redes Wi-Fi Públicas

Las redes Wi-Fi públicas presentan vulnerabilidades significativas frente al MITM y la propagación de malware. Estas debilidades suelen ser consecuencia de la falta de cifrado y autenticación en dichas redes. Choi et al. [10] destacan que estas vulnerabilidades aumentan por el comportamiento de los usuarios, quienes, en general, priorizan la comodidad sobre

la seguridad al conectarse a puntos de acceso no protegidos, incluso cuando son conscientes de los riesgos.

Entre los ataques más comunes en redes Wi-Fi públicas se encuentra el denominado Evil Twin, una amenaza en la que un atacante crea un punto de acceso falso que imita a uno legítimo con el mismo nombre, engañando a los usuarios para que se conecten a él en lugar del verdadero. Una vez establecida la conexión, el atacante puede interceptar, modificar o bloquear el tráfico de datos, facilitando ataques como el MITM, robo de credenciales o incluso la incorporación de malware [11].

Además del ataque Evil Twin, otro método ampliamente utilizado en redes públicas es el *sniffing* o captura de paquetes. En este ataque, los ciberdelincuentes emplean herramientas como Wireshark o Tcpdump para interceptar el tráfico de datos transmitido sin cifrar, permitiéndoles recopilar información sensible como credenciales de acceso, datos bancarios o correos electrónicos [12], [13].

Por otro lado, la propagación de malware en redes Wi-Fi públicas es una amenaza en crecimiento. Ataques como los *drive-by downloads* permiten a los atacantes inyectar código malicioso en sitios web frecuentados por los usuarios de una red insegura. De esta forma, cualquier dispositivo que visite la página puede infectarse sin necesidad de interactuar con enlaces sospechosos [14], [15].

Estos tipos de ataques son peligrosos en redes Wi-Fi públicas debido a la falta de fuertes mecanismos de autenticación y encriptación [16]. Para detectar la presencia de un Evil Twin, se han desarrollado múltiples métodos, como el análisis de tráfico, detección de anomalías en paquetes Wi-Fi y técnicas basadas en aprendizaje automático [13]. Un enfoque innovador es EvilScout, un sistema basado en redes definidas por software (SDN) que monitorea la distribución de direcciones IP y detecta APs falsos sin requerir modificaciones en el hardware o software de los clientes.

En términos de mitigación, el uso de VPNs es una de las soluciones más recomendadas. Sin embargo, tecnologías recientes como el protocolo WPA3 han introducido mejoras significativas en la seguridad de las redes Wi-Fi públicas, reduciendo la vulnerabilidad a ataques de diccionario y proporcionando cifrado individualizado para cada usuario [17], [18], [19].

En entornos académicos, como señalan Mahyoub et al. [20], los usuarios acceden con frecuencia a datos sensibles, lo que los convierte en un objetivo atractivo para estas amenazas. Los ataques MITM, por ejemplo, pueden emplear métodos que engañan a los dispositivos conectados o manipulan las direcciones en la red, permitiendo a los atacantes espiar o modificar la información transmitida [21] [22]. Esto compromete la privacidad de los usuarios, ya que los atacantes pueden acceder a datos confidenciales como contraseñas o información personal. Tales problemas son especialmente prevalentes en redes públicas con niveles de seguridad insuficientes, donde los usuarios confían en conexiones aparentemente legítimas, pero que en realidad no lo son [23] [24].

II-B. Principios éticos relacionados con la ciberseguridad

La incorporación de consideraciones éticas en el ámbito de la ciberseguridad resulta fundamental para garantizar la protección de la información, así como el respeto a los derechos y el bienestar de los usuarios. Esta cuestión adquiere especial relevancia en el contexto de las redes Wi-Fi públicas, las cuales forman parte de un ecosistema digital en el que convergen productos tecnológicos y cadenas de servicios digitales [25]. Dado que estos productos y servicios se proporcionan a través de dichas redes, cualquier vulnerabilidad o falta de principios éticos en su diseño e implementación puede comprometer directamente la seguridad y privacidad de los usuarios.

En este sentido, Formosa et al. [26] propusieron un marco ético basado en cinco principios fundamentales: beneficencia, no maleficencia, autonomía, justicia y explicabilidad. Los autores destacan que estos principios pueden entrar en conflicto y, por lo tanto, su aplicación debe equilibrarse cuidadosamente según el contexto en el que se implementen. Desde una perspectiva no técnica, Kozhuharova et al. [25] enfatizan la necesidad de integrar dichos principios en el diseño y desarrollo de productos tecnológicos con el fin de mitigar posibles efectos adversos en los usuarios. Por su parte, Tronnier et al. [27] aplicaron el marco de Formosa et al. para analizar los dilemas éticos que surgen en las cadenas de servicios digitales, evaluando el impacto de cada principio en los distintos procesos involucrados.

A partir de esta revisión, se identifican los elementos clave del marco ético:

- Beneficencia y No Maleficencia: La implementación de tecnologías de ciberseguridad debe orientarse hacia la promoción del bienestar de los usuarios y la prevención de daños intencionados [25], [26]. Este principio cobra particular importancia en las redes Wi-Fi públicas, donde la exposición a riesgos cibernéticos es elevada y la protección de la información resulta crítica.
- Autonomía: Es esencial garantizar que los usuarios cuenten con información suficiente para tomar decisiones informadas respecto al uso de servicios tecnológicos. La autonomía implica la capacidad de evaluar el impacto de estos productos y servicios en la vida cotidiana [26], [27].
- Justicia: Se debe promover la equidad y accesibilidad en el acceso y uso de tecnologías y servicios digitales, evitando sesgos y discriminaciones. En este sentido, los servicios ofrecidos a través de redes Wi-Fi públicas deben beneficiar a todos los usuarios sin distinción [26], [27].
- Explicabilidad: Las políticas, prácticas y tecnologías en materia de ciberseguridad deben ser comprensibles y transparentes, permitiendo una rendición de cuentas efectiva y garantizando la confianza de los usuarios en su implementación [26].
- Privacidad: Aunque no se plantea como un principio independiente, la protección de la información personal se integra de manera transversal en el análisis de los cinco principios, constituyendo un eje central en la salvaguarda

de los derechos digitales [26].

Es importante destacar que estos principios pueden entrar en conflicto, lo que requiere una aplicación contextualizada y equilibrada. Formosa et al. [26] subrayan que los dilemas éticos en ciberseguridad no pueden resolverse únicamente mediante soluciones técnicas, ya que omitir estas consideraciones no elimina los problemas inherentes. Tronnier et al. [27] evidencian que las problemáticas éticas en las cadenas de servicios digitales afectan de manera diferenciada a cada principio, lo que demanda estrategias compensatorias específicas. En consecuencia, Kozhuharova et al. [25] recomiendan la implementación de enfoques organizativos y tecnológicos, como la elaboración de listas de requisitos éticos, con el fin de garantizar la protección de los derechos y libertades de los usuarios en el desarrollo y aplicación de nuevas tecnologías.

II-C. Percepción de Seguridad en Redes Wi-Fi Públicas

La percepción de seguridad de los usuarios de redes Wi-fi públicas se ve influenciada por múltiples factores, incluyendo confianza, emociones, conveniencia y conocimiento en ciberseguridad. A continuación, en la Tabla I se presentan los principales aspectos que condicionan esta percepción:

Factor	Descripción
Confianza en Redes Wi-Fi Públicas	Oruma y Petrovic [28] indican que los usuarios confían en redes de cafeterías y aeropuertos por la percepción de seguridad. Sin embargo, Bongiovanni et al. [29] advierten que las redes en eventos masivos carecen de cifrado robusto, exponiéndolas a ataques como MITM y DNS spoofing. David et al. [30] señalan que la necesidad de acceso inmediato suele superar las preocupaciones de seguridad.
Influencia de las Emociones	Van Twist et al. [31] destacan que los usuarios pueden sentir ansiedad al realizar transacciones en redes públicas. Bongiovanni et al. [29] refuerzan que en eventos masivos, la preocupación por la seguridad es mayor, especialmente entre víctimas de ataques previos. Oruma y Petrovic [28] advierten sobre el optimismo irrealista de ciertos usuarios, quienes minimizan los riesgos. David et al. [30] encuentran que los jóvenes y personas con menor educación en ciberseguridad adoptan comportamientos más riesgosos.
Conveniencia vs. Seguridad	Van Twist et al. [31] argumentan que, aunque los riesgos son conocidos, la accesibilidad gratuita es prioritaria en entornos urbanos. David et al. [30] resaltan que la falta de alternativas seguras refuerza la elección de redes públicas. Oruma y Petrovic [28] sugieren que la autenticación en redes públicas puede generar una mayor sensación de seguridad en los usuarios, ya que el acceso requiere credenciales o verificaciones adicionales. No obstante, Bongiovanni et al. [29] cuestionan la efectividad de estos mecanismos, pues técnicas como el phishing o la suplantación de portales de autenticación pueden comprometer la seguridad de los usuarios incluso en redes que requieren registro previo.
Desconocimiento en Ciberseguridad	David et al. [30] advierten que muchas personas desconocen ataques como evil twin o sniffing de paquetes, confiando en indicadores visuales como el candado en la barra de direcciones. Oruma y Petrovic [28] enfatizan que la educación en ciberseguridad es clave, pero su impacto depende de la disposición del usuario a adoptar prácticas seguras. Van Twist et al. [31] sostienen que, incluso con conocimientos avanzados, algunos usuarios siguen comportamientos riesgosos por comodidad. Bongiovanni et al. [29] proponen regulaciones más estrictas y mecanismos de seguridad automatizados para mitigar los riesgos.

Tabla I
FACTORES QUE INFLUYEN EN LA PERCEPCIÓN DE SEGURIDAD EN REDES WI-FI PÚBLICAS.

III. ESTUDIO PROPUESTO

El presente estudio tiene como objetivo analizar la percepción de los usuarios sobre los riesgos de seguridad y los aspectos éticos asociados al uso de redes Wi-Fi públicas. Para ello, se llevará a cabo un análisis basado en la recopilación de datos a través de encuestas dirigidas a los usuarios, lo que permitirá evaluar su nivel de conocimiento, sus preocupaciones y sus prácticas en relación con la seguridad de estas redes.

Los objetivos específicos del análisis son los siguientes:

- Evaluar el nivel de conocimiento que poseen los usuarios respecto a los riesgos de seguridad asociados a la conexión en redes Wi-Fi públicas.
- Identificar la percepción de los usuarios sobre la seguridad de estas redes y las estrategias que consideran adecuadas para la protección de su información personal.
- Analizar los datos recopilados para obtener una visión detallada sobre el grado de conciencia y las prácticas actuales de los usuarios al utilizar redes Wi-Fi públicas.

IV. MATERIALES Y MÉTODOS

El presente estudio adoptó un enfoque exploratorio con el objetivo de obtener información sobre las percepciones éticas y de seguridad de los usuarios de redes Wi-Fi públicas en la ciudad de Quevedo. La metodología utilizada se desarrolló en las siguientes etapas:

1. **Revisión del estado del arte**: En esta etapa, se realizó un análisis exhaustivo de la literatura científica relacionada con los riesgos de seguridad y la percepción ética en el uso de redes Wi-Fi públicas. Se consultaron artículos académicos, libros y documentos relevantes en las principales bases de datos académicas, como IEEE Xplore, ScienceDirect, SpringerLink, ACM Digital Library y Scopus. Esta revisión permitió identificar estudios previos que abordaron diversas problemáticas relacionadas con la seguridad de redes Wi-Fi, los desafíos éticos asociados con su uso, y las percepciones que tienen los usuarios sobre los riesgos involucrados en su acceso y utilización.

   El objetivo principal de esta revisión fue entender los enfoques previos en cuanto a la protección de datos personales, las vulnerabilidades comunes en redes públicas y las mejores prácticas en términos de seguridad. Además, se exploraron estudios sobre la forma en que

los usuarios perciben los riesgos asociados con las redes Wi-Fi públicas y cómo estas percepciones influyen en su comportamiento. Esta fase fue esencial para construir un marco teórico que sustentara el diseño del cuestionario utilizado para la recolección de datos, ayudando a estructurar las preguntas de acuerdo con los temas más relevantes identificados en la literatura revisada.

El análisis de los artículos permitió identificar vacíos en la investigación existente, lo que justificó la necesidad de realizar un estudio enfocado en la ciudad de Quevedo, dado que los estudios previos se han centrado principalmente en áreas urbanas más grandes o en países de contextos diferentes. La revisión del estado del arte también facilitó la identificación de variables clave y permitió comparar resultados previos con la situación particular de la ciudad en cuestión.

2. **Diseño del instrumento de recolección de datos**: A partir de los hallazgos obtenidos en la revisión del estado del arte, se diseñó un cuestionario estructurado, organizado en varias áreas temáticas para obtener una visión completa de la percepción de los usuarios. Las áreas incluidas fueron:
   - Información demográfica.
   - Frecuencia de uso de redes Wi-Fi públicas.
   - Conocimiento sobre los riesgos asociados.
   - Medidas de seguridad implementadas por los usuarios.
   - Percepción ética del uso de redes Wi-Fi públicas.
3. **Determinación de la población y muestra**: La población objetivo estuvo conformada por usuarios mayores de 18 años que utilizaban redes Wi-Fi públicas en la ciudad de Quevedo. Para determinar el tamaño de la muestra, se utilizó la fórmula para poblaciones infinitas propuesta por Lohr [32], ya que se asumió que la población total es lo suficientemente grande como para ser considerada infinita. La fórmula utilizada fue la siguiente:

$$n = \frac{Z^2 \cdot P \cdot Q}{e^2} \tag{1}$$

Donde:

- ***Tamaño de la muestra*** (n)***:*** Representa el número mínimo de encuestas necesarias para garantizar la precisión de los resultados obtenidos.
- ***Proporción de aceptación*** ($P = 0{,}5$) ***y proporción de rechazo*** ($Q = 0{,}5$)***:*** Se asume la máxima variablidad de la población. Esto se debe a la distribución de probabilidades binomiales ($P + Q = 1$).
- ***Nivel de confianza del 95 %*** ($Z = 1{,}96$)***:*** Este valor refleja la probabilidad de que la muestra seleccionada sea representativa de la población total. En estudios de encuestas, un nivel de confianza del 95 % es comúnmente utilizado para asegurar que el intervalo de confianza de los resultados abarca aproximadamente 1.96 desviaciones estándar de la media.
- ***Margen de error*** $e = 0{,}05$***:*** Se seleccionó un margen de error del 5 %, lo que implica que los resultados obtenidos pueden variar en ±5 puntos porcentuales respecto a la población total. Este margen es estándar en estudios de percepción, permitiendo un equilibrio adecuado entre precisión y viabilidad en el tamaño de la muestra.

Aplicando la Ecuación 1, da como resultado que la muestra mínima de encuestados para llevar a cabo este estudio fue de 385 encuestados.

4. **Aplicación del cuestionario**: Una vez determinado el tamaño de la muestra, se distribuyó el cuestionario utilizando la plataforma Google Forms, lo que facilitó la recolección de respuestas de manera eficiente y accesible. Para garantizar la confidencialidad y anonimato de las respuestas, se cumplió con los principios éticos de la investigación, asegurando la privacidad de los participantes.
5. **Procesamiento y análisis de datos**: Una vez completada la fase de recolección de datos, las respuestas fueron organizadas y analizadas utilizando las herramientas proporcionadas por Google Forms, las cuales permitieron generar resúmenes estadísticos visuales, como gráficos de barras y diagramas circulares [33]. Este proceso facilitó la interpretación de los resultados y permitió la extracción de conclusiones clave sobre las percepciones y comportamientos de los usuarios de redes Wi-Fi públicas en la ciudad de Quevedo.

V. Resultados

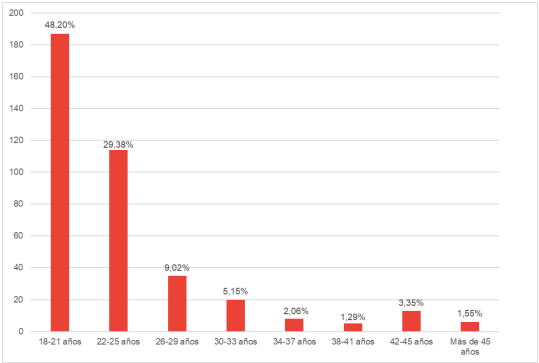

Figura 1. Rango de edad de los encuestados

La (Figura 1) presenta la distribución de edad de los encuestados en el estudio sobre el uso de redes Wi-Fi públicas, evidenciando que casi la mitad pertenece al grupo de 18-21 años, seguido por un 29,38 % en el rango de 22-25 años. Estos resultados destacan que la muestra está compuesta por jóvenes, probablemente vinculados al ámbito universitario, lo que concuerda con los lugares de conexión mencionados en el estudio (campus universitarios y centros comerciales).

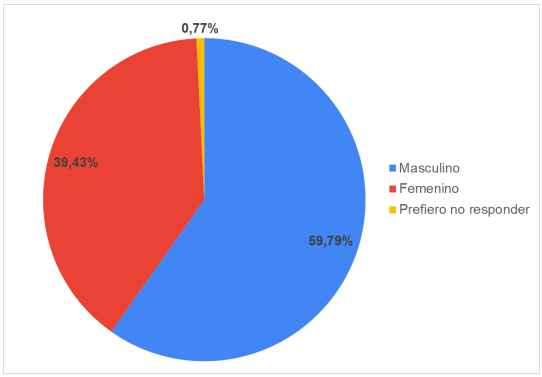

Figura 2. Género de los encuestados

Los datos de género revelan una distribución desigual entre los participantes del estudio, donde el 59,79 % se identifica como masculino, el 39,43 % como femenino y solo un 0,77 % prefirió no responder. Esta predominancia masculina podría reflejar diferencias en el acceso o interés por la tecnología (ver Figura 2).

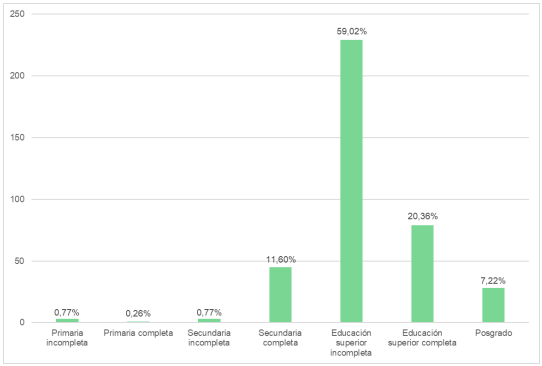

Figura 3. Nivel educativo de los encuestados

La Figura 3 muestra el nivel educativo de los encuestados, revelando que la mayoría tiene educación superior incompleta, lo que afirma que la muestra está compuesta principalmente por estudiantes universitarios en proceso de formación. Le sigue un 20,36 % con educación superior completa y un 11,60 % con secundaria completa, mientras que los niveles de primaria incompleta (0,77 %) y secundaria incompleta (0,77 %) y primaria incompleta (0,26 %) son minoritarios. Esta distribución refuerza los hallazgos previos sobre el perfil joven de los participantes y su vinculación con entornos académicos.

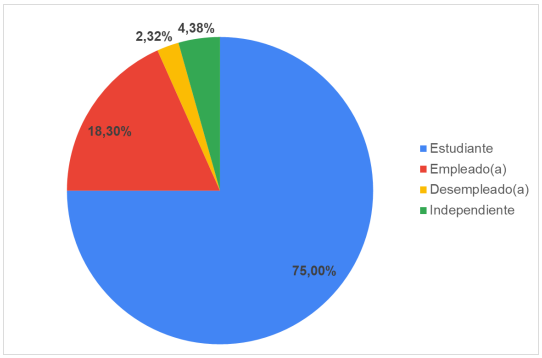

Figura 4. Ocupación principal de los encuestados

La Figura 4 sobre ocupación principal muestra una clara predominancia de estudiantes entre los encuestados, lo que concuerda con los datos previos de edad (18-25 años) y nivel educativo (59,02 % con educación superior incompleta). Le siguen en proporción los empleados (18,3 %), mientras que las categorías de independientes y desempleados son minoritarios. Esta distribución confirma que la muestra está mayormente compuesta por población estudiantil universitaria, lo que explica su alto uso de redes Wi-Fi públicas en entornos académicos como campus y centros comerciales.

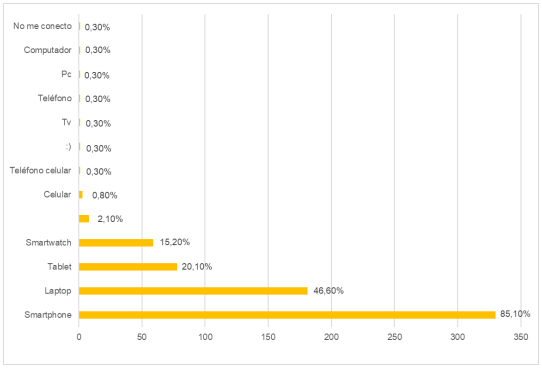

Figura 5. Tipo de dispositivo usado

La Figura 5 muestra que los smartphones son claramente los dispositivos más utilizados para conectarse a redes Wi-Fi públicas, representando la opción más escogida en la encuesta. Les siguen en importancia las laptops, que aparecen como la segunda opción más frecuente, lo que refleja un patrón de uso combinado entre movilidad (smartphones) y productividad académica o laboral (laptops).

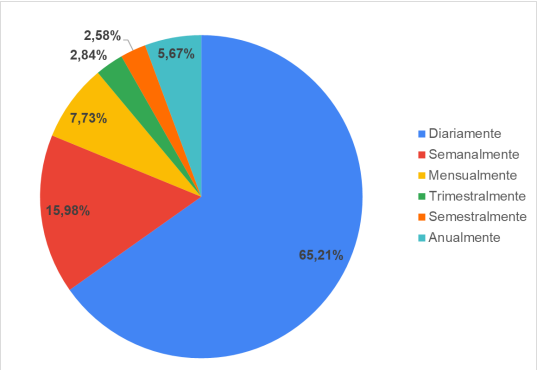

Figura 6. Frecuencia de uso de redes Wi-Fi públicas

Los resultados revelan una alta dependencia de las redes Wi-Fi públicas entre los encuestados, donde el 65,21 % declara usarlas diariamente, destacando su integración en la rutina cotidiana, sobre todo en entornos académicos y comerciales. Un 15,98 % las utiliza semanalmente, mientras que las frecuencias menores (mensual, trimestral, semestral y anual) suman apenas 18,82 %, confirmando que se trata de una población con alta exposición a estos servicios (ver Figura 6).

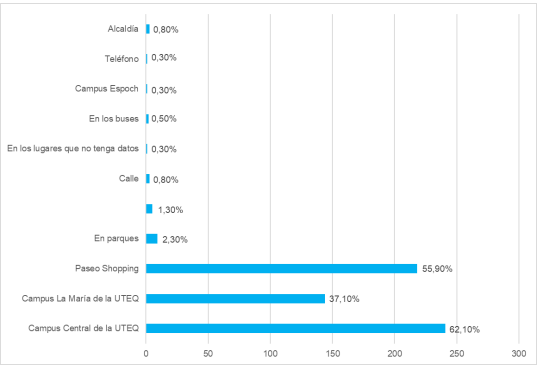

Figura 7. Lugares de conexión

La Figura 7 muestra que los lugares más frecuentes para conectarse a redes Wi-Fi públicas son entornos educativos y comerciales, siendo el Campus Central de la UTEQ la ubicación más utilizada, seguido de cerca por el Paseo Shopping, un centro comercial. Estos datos reflejan el perfil mayoritariamente estudiantil de los encuestados, así como su necesidad de conectividad en espacios de estudio y ocio. El Campus La María también aparece como un punto relevante, aunque con menor frecuencia, lo que podría indicar diferencias en la afluencia de usuarios o en la disponibilidad de redes entre campus.

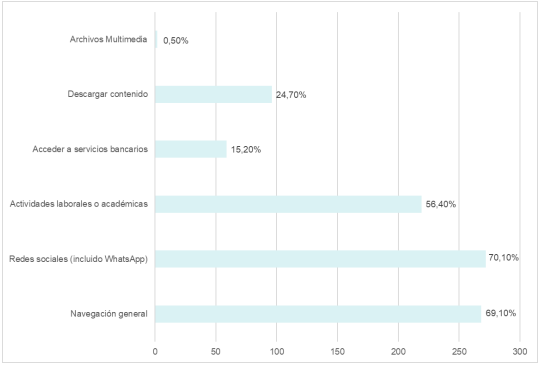

Figura 8. Uso de las redes Wi-Fi

La Figura 8 destaca que los usos principales de las redes Wi-Fi públicas se concentran en redes sociales y navegación general, actividades que suelen requerir conectividad constante pero no siempre requieren alto nivel de seguridad. Le siguen en importancia las actividades laborales o académicas, lo que coincide con el perfil estudiantil de la mayoría de los encuestados y su necesidad de acceder a plataformas educativas o herramientas de trabajo. Llama la atención el bajo uso para acceder a servicios bancarios, lo que sugiere cierta conciencia sobre los riesgos al manejar información financiera en redes públicas.

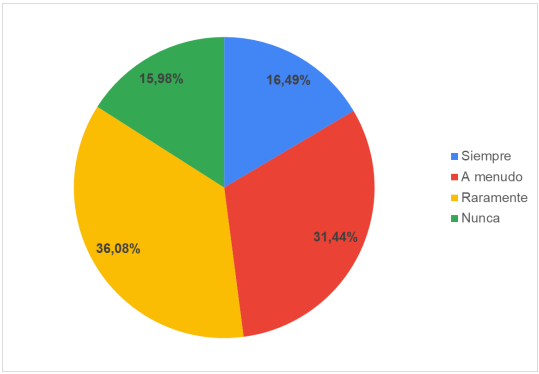

Figura 9. Verificación de redes auténticas

Los resultados revelan una preocupante falta de verificación de la autenticidad de las redes Wi-Fi públicas entre los usuarios: mientras solo el 16,49 % afirma siempre confirmar su legitimidad, un 36,08 % lo hace raramente y otro 15,98 % nunca realiza esta comprobación. Aunque un 31,44 % declara verificarlas a menudo, la suma de comportamientos de riesgo (raramente + nunca) supera el 52 %, lo que expone a la mayoría de los encuestados a amenazas como Evil Twin o ataques MITM (ver Figura 9).

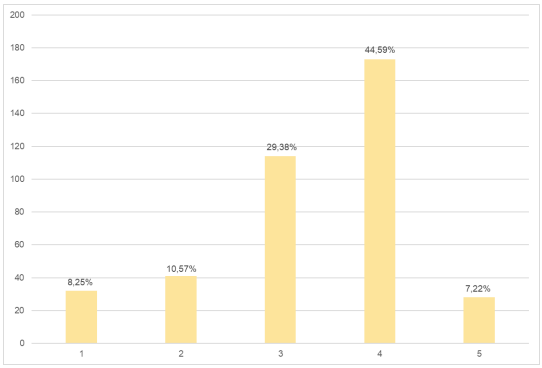

Figura 10. Nivel de conocimiento sobre seguridad

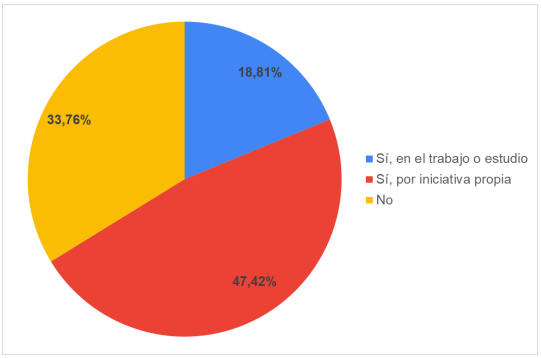

Figura 12. Nivel de capacitación

La Figura 10 revela que el nivel 4 (”bastante informado”) es la opción más seleccionada por los encuestados, lo que indica que una parte significativa de los usuarios percibe tener un conocimiento sólido sobre los riesgos de seguridad en redes Wi-Fi públicas. Sin embargo, esta autopercepción contrasta con otros hallazgos del estudio donde se observan prácticas de seguridad deficientes, como que el 36,08 % rara vez verifica la autenticidad de las redes y el 15,98 % nunca lo hace. Esta discrepancia sugiere un exceso de confianza o una brecha entre el conocimiento teórico y su aplicación práctica.

Los resultados muestran una gran brecha en la capacitación sobre seguridad en redes Wi-Fi públicas, mientras el 47,42 % de los encuestados aprendió por iniciativa propia (lo que refleja esfuerzos individuales por capacitarse), solo el 18,81 % recibió información en su entorno laboral o académico, evidenciando una falta de institucionalización de este conocimiento clave. Preocupa que el 33,76 % nunca haya recibido ningún tipo de capacitación, grupo vulnerable que coincide con el 10,6 % que desconocía los riesgos de las redes Wi-Fi públicas (ver Figura 12).

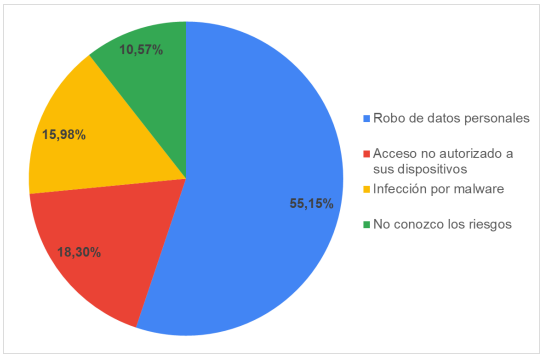

Figura 11. Mayor riesgo de uso

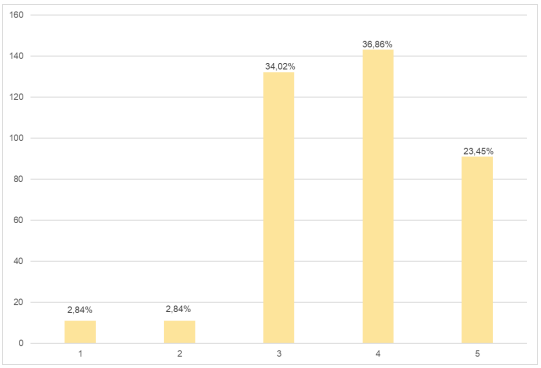

Figura 13. Percepción de los encuestados

La Figura 11 revela que el robo de datos personales es percibido como el principal riesgo al usar redes Wi-Fi públicas, con un 55,15 % de las respuestas, lo que demuestra una clara conciencia sobre esta amenaza entre los usuarios. Le siguen en importancia el acceso no autorizado a dispositivos (18,30 %) y la infección por malware (15,98 %), riesgos técnicos que también preocupan a los encuestados. Sin embargo, un 10,57 % admite directamente no conocer los riesgos, cifra preocupante que coincide con otros hallazgos del estudio donde un 36,08 % raramente verifica la autenticidad de las redes.

En la Figura 13, se observa que la concentración de respuestas en los niveles 3 a 5 revela que los encuestados perciben un desconocimiento moderado-alto sobre los riesgos de las redes Wi-Fi públicas entre los usuarios en general. Esta percepción colectiva resulta contradictoria al contrastarla con los datos del estudio: mientras el 55,15 % identifica correctamente el robo de datos como principal amenaza y un 47,42 % ha buscado capacitación por iniciativa propia, persisten prácticas inseguras como no verificar redes (36,08 %).

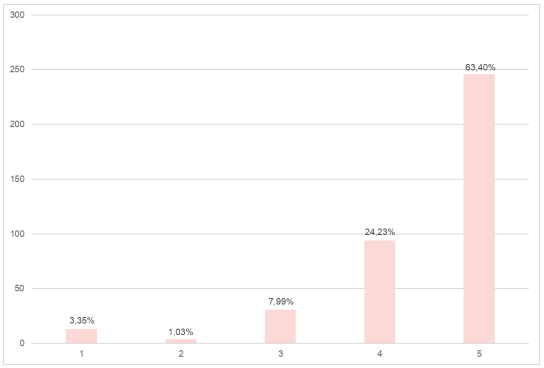

Figura 14. Educación sobre ciberseguridad

La Figura 14 muestra una clara tendencia hacia los valores altos, con la mayoría de respuestas concentradas en los niveles 4 y 5. Esto indica una aprobación abrumadora entre los encuestados sobre la necesidad urgente de promover educación en ciberseguridad para redes públicas. Los niveles intermedios y bajos aparecen como minoritarios, reforzando que la demanda de capacitación es casi unánime en esta población.

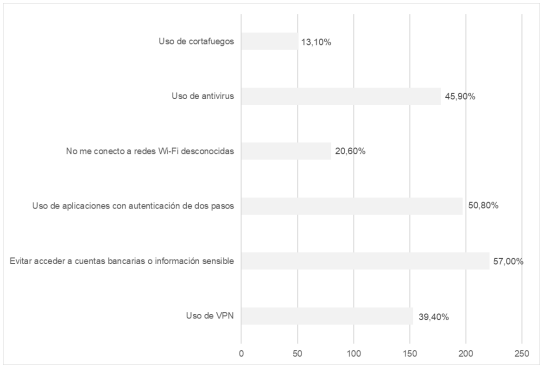

Figura 15. Medidas de seguridad

La Figura 15 revela que las medidas de seguridad más practicadas son evitar acceder a cuentas bancarias/información sensible y el uso de aplicaciones con autenticación de dos pasos, seguidas del uso de antivirus. Estas prácticas reflejan una estrategia defensiva centrada en proteger datos críticos y reforzar accesos, aunque dependen más de la precaución del usuario que de herramientas avanzadas. Llama la atención el bajo uso de VPNs (a pesar de ser una recomendación clave en ciberseguridad) y de cortafuegos, lo que sugiere desconocimiento o percepciones de complejidad.

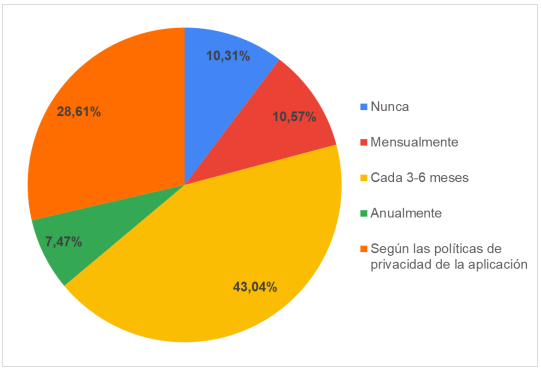

Figura 16. Prevención de riesgos

La Figura 16 muestra que la mayoría de los encuestados (43,04 %) cambian sus contraseñas cada 3-6 meses, una práctica moderadamente segura que equilibra frecuencia y practicidad. Sin embargo, un 28,61 % solo las actualiza según las políticas de las plataformas, lo que sugiere dependencia de terceros para gestionar su seguridad. Preocupa que un 10,31 % admita nunca cambiar sus contraseñas y otro 7,47 % lo haga anualmente, grupos vulnerables a ataques prolongados. Aunque el 10,57 % que las renueva mensualmente sigue buenas prácticas, su minoría refleja que la mayoría prioriza la conveniencia sobre la seguridad óptima.

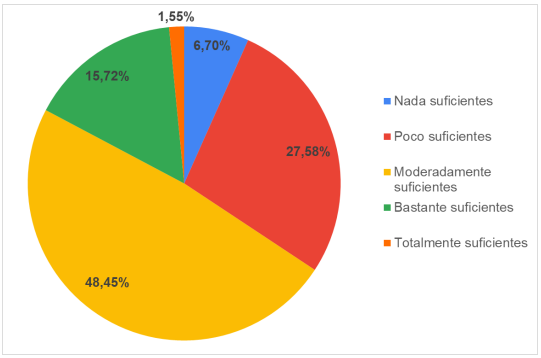

Figura 17. Medidas de seguridad aplicadas

La Figura 17 revela una autopercepción moderada sobre la eficacia de las medidas de seguridad: casi la mitad de los encuestados (48,45 %) considera que sus prácticas son ”moderadamente suficientes”, lo que refleja una postura realista pero no del todo confiada. Un 27,58 % las califica como ”poco suficientesz un 6,70 % como ”nada suficientes”, sumando un 34,28 % que reconoce explícitamente sus carencias de protección. En contraste, solo un 1,55 % las considera ”totalmente suficientesz un 15,72 % ”bastante suficientes”, lo que confirma que la mayoría duda de la firmeza de sus acciones.

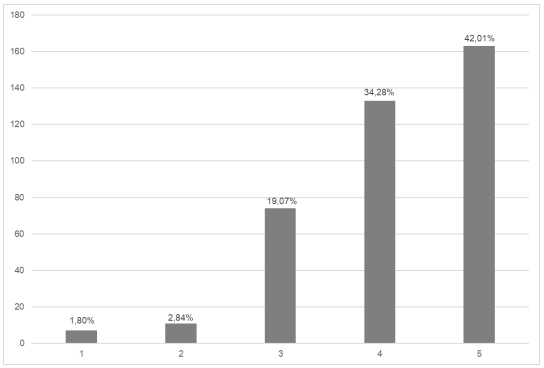

Figura 18. Responsabilidad sobre su propia seguridad

La Figura 18 muestra una clara tendencia hacia los valores altos, con la mayoría de respuestas concentradas en los niveles 4 y 5 , lo que sugiere que la mayoría de los encuestados asume que la seguridad en redes públicas es una responsabilidad individual. Esta percepción se alinea con otros hallazgos del estudio: aunque los usuarios critican sus propias medidas de seguridad (48,45 % las considera solo ”moderadamente suficientes”), depositan en sí mismos la obligación de protegerse.

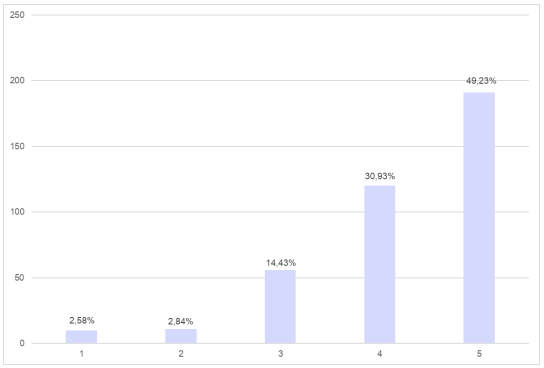

Figura 19. Protección de los administradores

La Figura 19 revela un fuerte consenso hacia los valores altos, con respuestas masivamente concentradas en los niveles 4 y 5 , lo que indica que más del 80 % de los encuestados exige que los administradores de redes Wi-Fi públicas asuman la responsabilidad de proteger los datos de los usuarios. Esta demanda de corresponsabilidad institucional contrasta con otro hallazgo clave del estudio: el 76,29 % también cree que los usuarios deben ser responsables individualmente, evidenciando una visión dual donde ambos actores tienen roles complementarios.

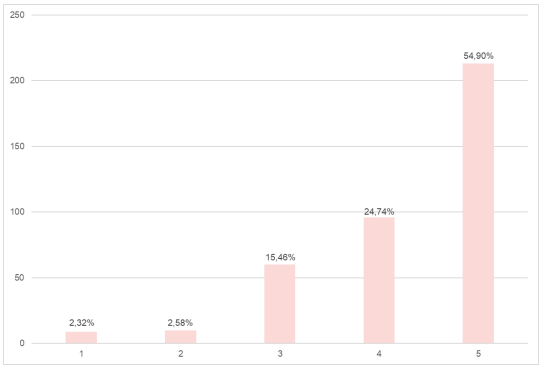

Figura 20. Conocimiento sobre las políticas de seguridad

La Figura 20 refleja la percepción de los encuestados sobre la responsabilidad de los administradores de redes Wi-Fi públicas en la protección de los datos de los usuarios. Se observa que la mayoría otorga una alta importancia a este aspecto, con un 49,2 % que seleccionó el nivel 5 y un 30,9 % que eligió el nivel 4. En conjunto, el 80,1 % de los participantes (niveles 4 y 5) considera fundamental que se garantice la seguridad de la información. En contraste, solo un 2,6 % otorgó el nivel más bajo (1), lo que indica que son pocos quienes restan importancia a esta responsabilidad.

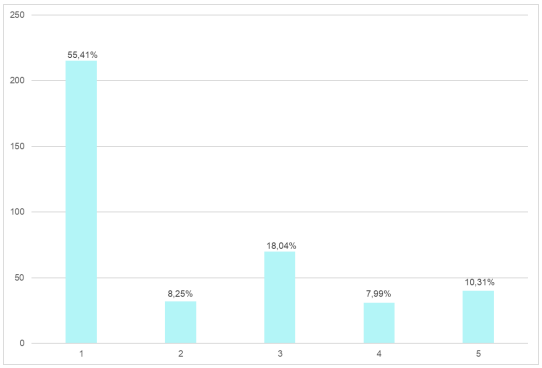

Figura 21. Grado ético sobre el uso indebido de estas redes

La Figura 21 revela una condena mayoritaria del uso anónimo de redes Wi-Fi públicas para actividades ilegales, con respuestas masivamente concentradas en los niveles 1 y 2, lo que indica un fuerte rechazo ético a prácticas como piratería o descargas no autorizadas. Esta postura se alinea con el principio de no maleficencia identificado en el marco teórico del estudio, donde los usuarios valoran la integridad de las redes. Los niveles altos (4-5) son marginales, sugiriendo que solo una minoría mínima justifica estas acciones.

VI. Discusión

Los resultados de este estudio nos muestran un panorama claro sobre cómo los jóvenes, principalmente estudiantes universitarios, usan las redes Wi-Fi públicas. Casi la mitad de los encuestados tiene entre 18 y 21 años (Figura 1), y la mayoría son estudiantes universitarios (Figura 3 y Figura 4).

Esto coincide con los lugares donde más se conectan: los campus universitarios y centros comerciales (Figura 7).

Estos jóvenes usan mucho sus teléfonos para conectarse a estas redes (Figura 5) y lo hacen casi todos los días (Figura 6). Esto significa que las redes Wi-Fi públicas son muy importantes en su vida diaria, especialmente para redes sociales, navegar por internet y para estudiar o trabajar (Figura 8).

Sin embargo, hay un problema importante: la mayoría no revisa si las redes a las que se conecta son seguras (Figura 9). Muchos saben que el robo de datos personales es el mayor riesgo (Figura 11), pero no toman las medidas necesarias para protegerse. Esto se debe, en parte, a que muchos no han recibido capacitación sobre cómo usar estas redes de forma segura (Figura 12).

Aunque muchos creen saber sobre seguridad en internet (Figura 10), sus acciones no lo demuestran. La mayoría usa medidas básicas como evitar dar información importante y usar la verificación en dos pasos (Figura 15). Cambian sus contraseñas cada 3 a 6 meses (Figura 16), lo que no es suficiente para estar completamente seguros. Además, muchos sienten que sus medidas de seguridad son solo "moderadamente suficientes"(Figura 17).

En cuanto a quién es responsable de la seguridad, la mayoría piensa que tanto los usuarios como los administradores de las redes tienen un papel importante (Figura 18 y Figura 19). También creen que es fundamental que los administradores informen sobre las políticas de seguridad (Figura 20).

Finalmente, la mayoría está en contra de usar las redes Wi-Fi públicas para actividades ilegales (Figura 21). Esto muestra que, aunque no siempre se protegen bien, tienen una buena conciencia sobre lo que está bien y lo que está mal en internet.

VII. Conclusiones

El estudio revela una clara discrepancia entre las expectativas de seguridad y las prácticas reales de los usuarios de redes Wi-Fi públicas en Quevedo. Aunque el 85 % exige transparencia en las políticas de seguridad antes de conectarse y el 80 % responsabiliza a los administradores de garantizar la protección, solo el 16,5 % verifica activamente la autenticidad de las redes. Además, un 34 % admite que sus medidas de seguridad son insuficientes, lo que los hace vulnerables a ataques como MITM y Evil Twin [11], [20].

La mayoría de los usuarios son jóvenes universitarios que dependen en gran medida de estas conexiones. Si bien el 55 % identifica el robo de datos como el principal riesgo y el 48,5 % considera sus precauciones "moderadamente suficientes", persisten prácticas vulnerables. Estas incluyen el bajo uso de VPNs, la renovación poco frecuente de contraseñas (10,3 % nunca las cambia) y la alta dependencia diaria de redes públicas (65.4 %).

Un problema crítico es la falta de educación en ciberseguridad. Muchos usuarios nunca han recibido capacitación sobre cómo protegerse en redes Wi-Fi públicas. Aunque algunos implementan medidas como VPNs o autenticación de dos factores, estas acciones son insuficientes para mitigar todos los riesgos [7], [16].

Reducir estos peligros requiere un enfoque multifacético. Los usuarios deben comprender los riesgos y adoptar medidas preventivas simples, como evitar redes sospechosas, desactivar la opción de compartir datos y utilizar herramientas como VPNs para proteger su información [10], [28]. La educación y la concienciación son fundamentales, ya que la tecnología por sí sola no es suficiente [30].

Los resultados también destacan que la seguridad en redes Wi-Fi públicas se percibe como una responsabilidad compartida. Aunque los usuarios deben tomar precauciones individuales, también esperan que los administradores mejoren la seguridad y sean transparentes sobre sus políticas [26]. Para lograr un equilibrio, se necesitan normativas más estrictas y la promoción de buenas prácticas en la administración de redes [27].

La combinación de educación, tecnología y normativas es clave para mejorar la seguridad en redes públicas. Se recomienda que universidades y administradores de redes implementen campañas de información, cursos de formación y mejoras en la infraestructura de seguridad. Esto reducirá la exposición a ataques y fomentará un uso más seguro y responsable de estas conexiones [9], [25].

VIII. Trabajos Futuros

Este estudio permitió identificar la percepción de los usuarios sobre la seguridad en redes Wi-Fi públicas en Quevedo, pero hay varios aspectos que podrían explorarse con mayor profundidad.

En futuros trabajos, sería interesante ampliar el estudio a otras ciudades para comparar los resultados y ver si los hábitos y conocimientos sobre seguridad varían según la región.

Además, se podría llevar a cabo una investigación enfocada en evaluar la efectividad de las campañas de educación en ciberseguridad. Por ejemplo, se podría implementar un programa de capacitación en universidades y medir si los estudiantes mejoran sus prácticas de seguridad después de recibir información sobre los riesgos y las mejores formas de protegerse.

Otro enfoque relevante sería analizar la seguridad real de las redes Wi-Fi públicas mediante pruebas técnicas que detecten vulnerabilidades en la configuración de los puntos de acceso. Esto ayudaría a comprobar si las redes que los usuarios consideran seguras realmente cumplen con estándares adecuados de protección.

Estos son algunos posible trabajos futuros que podrían llevarse a cabo tomando esta investigación como base.

Referencias

[1] K. Sinchana, C. Sinchana, H. L. Gururaj, and B. R. S. Kumar, "Performance evaluation and analysis of various network security tools," *2019 International Conference on Communication and Electronics Systems (ICCES)*, pp. 644–650, 7 2019, DOI: 10.7717/peerj-cs.1185.

[2] R. Alueendo, N. Suresh, V. Hashiyana, and E. Bagarukayo, "A systematic review: Vulnerability assessment of wi-fi in educational institution," in *2020 IST-Africa Conference (IST-Africa)*. IEEE, 2020, pp. 1–6.

[3] N. Pimple, T. Salunke, U. Pawar, and J. Sangoi, "Wireless security—an approach towards secured wi-fi connectivity," in *2020 6th international conference on advanced computing and communication systems (ICACCS)*. IEEE, 2020, pp. 872–876, DOI: 10.1109/ICACCS48705.2020.9074350.

[4] K. s Arikumar, A. D. Kumar, S. B. Prathiba, K. Tamilarasi, R. S. Moorthy, and M. M. Iqbal, "Enhancing the security of wpa2/psk authentication protocol in wi-fi networks," *Procedia Computer Science*, vol. 215, pp. 413–421, 2022, DOI: 10.1016/j.procs.2022.12.043.

[5] A. Carballal, J. P. Galego-Carro, N. Rodriguez-Fernandez, and C. Fernandez-Lozano, "Wi-fi handshake: analysis of password patterns in wi-fi networks," *PeerJ Computer Science*, vol. 8, p. e1185, 12 2022, DOI: 10.7717/peerj-cs.1185.

[6] M. Abdulkader, "Why do people use public wi-fi? : An investigation of risk-taking behaviour and factors lead to decisions," pp. iv, 33, 2023.

[7] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for wi-fi and wpa3," *Electronics*, vol. 7, p. 284, 10 2018, DOI: 10.3390/electronics7110284.

[8] A. V. Anastasia, S. V. Zareshin, I. S. Rumyantseva, and V. G. Ivanenko, "Proceedings of the 2017 ieee north west russia section young researchers in electrical and electronic engineering conference (2017 eiconrusnw) : February 1-3, 2017, st. petersburg, russia," *2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, 2017, DOI: 10.1109/EIConRus.2017.7910505.

[9] D. Gao, H. Lin, Z. Li, F. Qian, Q. A. Chen, Z. Qian, W. Liu, L. Gong, and Y. Liu, "A nationwide census on wifi security threats: prevalence, riskiness, and the economics," in *Proceedings of the 27th Annual International Conference on Mobile Computing and Networking*, 2021, pp. 242–255, DOI: 10.1109/10.1145/3447993.3448620.

[10] H. S. Choi, D. Carpenter, and M. S. Ko, "Risk taking behaviors using public wi-fi™," *Information Systems Frontiers*, vol. 24, pp. 965–982, 6 2022.

[11] M. Asaduzzaman, M. S. Majib, and M. M. Rahman, "Wi-fi frame classification and feature selection analysis in detecting evil twin attack," in *2020 IEEE Region 10 Symposium (TENSYMP)*. IEEE, 2020, pp. 1704–1707, DOI: 10.1109/TENSYMP50017.2020.9231042.

[12] S. Friedl and G. Pernul, "Forensic analysis of an iot arp spoofing attack," in *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2024, pp. 1–7, DOI: 10.1109/ISDFS60797.2024.10527302.

[13] V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur, and M. Amoon, "Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion," *Electronics*, vol. 12, no. 20, p. 4299, 2023, DOI: 10.3390/electronics12204299.

[14] R. K. Ayeni, A. A. Adebiyi, J. O. Okesola, and E. Igbekele, "Phishing attacks and detection techniques: A systematic review," in *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG)*. IEEE, 2024, pp. 1–17, DOI: 10.1109/SEB4SDG60871.2024.10630203.

[15] Z. S. Karam, R. H. Ali, and B. O. Al-Nashy, "Exploring emerging strategies for countering computer malware attacks: A comprehensive survey of tools and techniques." *International Journal of Computational & Electronic Aspects in Engineering (IJCEAE)*, vol. 4, no. 2, 2023, DOI: 10.26706/ijceae.4.2.20239750.

[16] J. James, "Analysis of security features and vulnerabilities in public/open wi-fi," *Journal of Information Systems Applied Research*, vol. 14, pp. 4–13, 2021. [Online]. Available: https://conisar.org

[17] P. Shrivastava, M. S. Jamal, and K. Kataoka, "Evilscout: Detection and mitigation of evil twin attack in sdn enabled wifi," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 89–102, 2020, DOI: 10.1109/TNSM.2020.2972774.

[18] R. Lakhani and R. C. Sachan, "Securing wireless networks against emerging threats: An overview of protocols and solutions," *Journal of Science & Technology*, vol. 5, no. 4, pp. 10–55 662, 2024, DOI: 10.55662/JST.2024.5406.

[19] M. Thankappan, H. Rifà-Pous, and C. Garrigues, "Multi-channel man-in-the-middle attacks against protected wi-fi networks: A state of the art review," *Expert Systems with Applications*, vol. 210, p. 118401, 2022, DOI: 10.1016/j.eswa.2022.118401.

[20] M. Mahyoub, A. Matrawy, K. Isleem, and O. Ibitoye, "Cybersecurity challenge analysis of work-from-anywhere (wfa) and recommendations guided by a user study," 9 2024. [Online]. Available: http://arxiv.org/abs/2409.07567

[21] Z. Xu, J. Li, Y. Pan, M. Li, and L. Lazos, "Harvesting physical-layer randomness in millimeter wave bands," *IEEE Transactions on Mobile Computing*, 2024, DOI: 10.1109/TMC.2024.3499876.

[22] H. Fereidouni, O. Fadeitcheva, and M. Zalai, "Iot and man-in-the-middle attacks," *arXiv preprint arXiv:2308.02479*, 2023, DOI: 10.48550/arXiv.2308.02479.

[23] M. A. Al-Shareeda and S. Manickam, "Man-in-the-middle attacks in mobile ad hoc networks (manets): Analysis and evaluation," *Symmetry*, vol. 14, p. 1543, 7 2022.

[24] M. A. Yurdagul and H. T. Sencar, "Blekeeper: Response time behavior based man-in-the-middle attack detection," in *2021 IEEE Security and Privacy Workshops (SPW)*. IEEE, 2021, pp. 214–220, DOI: 10.1109/SPW53761.2021.00035.

[25] D. Kozhuharova, A. Kirov, and Z. Al-Shargabi, "Ethics in cybersecurity. what are the challenges we need to be aware of and how to handle them?" in *Cybersecurity of Digital Service Chains: Challenges, Methodologies, and Tools*. Springer International Publishing Cham, 2022, pp. 202–221, DOI: 10.1007/978-3-031-04036-8_9.

[26] P. Formosa, M. Wilson, and D. Richards, "A principlist framework for cybersecurity ethics," *Computers & Security*, vol. 109, p. 102382, 2021, DOI: 10.1016/j.cose.2021.102382.

[27] F. Tronnier, S. Pape, S. Löbner, and K. Rannenberg, "A discussion on ethical cybersecurity issues in digital service chains," in *Cybersecurity of digital service chains: challenges, methodologies, and tools*. Springer, 2022, pp. 222–256, DOI: 10.1007/978-3-031-04036-8_10.

[28] S. O. Oruma and S. Petrovic, "Security threats to 5g networks for social robots in public spaces: a survey," *IEEE Access*, vol. 11, pp. 63 205–63 237, 2023, DOI: 10.1109/ACCESS.2023.3288338.

[29] I. Bongiovanni, D. M. Herold, and S. J. Wilde, "Protecting the play: An integrative review of cybersecurity in and for sports events," *Computers & Security*, p. 104064, 2024, DOI: 10.1016/j.cose.2024.104064.

[30] A. David, T. Yigitcanlar, R. Y. M. Li, J. M. Corchado, P. H. Cheong, K. Mossberger, and R. Mehmood, "Understanding local government digital technology adoption strategies: A prisma review," *Sustainability*, vol. 15, no. 12, p. 9645, 2023, DOI: 10.3390/su15129645.

[31] A. Van Twist, E. Ruijer, and A. Meijer, "Smart cities & citizen discontent: A systematic review of the literature," *Government Information Quarterly*, vol. 40, no. 2, p. 101799, 2023, DOI: 10.1016/j.giq.2022.101799.

[32] S. L. Lohr, *Sampling*. Chapman and Hall/CRC, 10 2021.

[33] A. Adelia, M. Miftahurrahmah, N. Nurpathonah, Y. Zaindanu, and M. T. Ihsan, "The role of google form as an assessment tool in elt: Critical review of the literature," *ETDC: Indonesian Journal of Research and Educational Review*, vol. 1, no. 1, pp. 58–66, 2021, DOI: 10.51574/ijrer.v1i1.49.

IX. Anexos

IX-A. Encuesta

Información demográfica	
1	¿Cuál es su rango de edad?
2	¿Con qué género se identifica?
3	¿Cuál es su nivel educativo más alto alcanzado?
4	¿Cuál es su ocupación principal?
5	¿Con qué tipo de dispositivo suele conectarse a redes Wi-Fi públicas?
Frecuencia de uso de redes Wi-Fi públicas	
6	¿Con qué frecuencia utiliza redes Wi-Fi públicas?
7	¿En qué lugares suele conectarse a redes Wi-Fi públicas?
8	¿Utiliza redes Wi-Fi públicas principalmente para...? (Seleccione todas las opciones que correspondan)
9	¿Suele verificar si la red Wi-Fi pública a la que se conecta es auténtica (por ejemplo, preguntar al personal del lugar)?
Conocimiento sobre Riesgos Asociados	
10	En una escala del 1 al 5, ¿qué tan informado se considera sobre los riesgos de seguridad en redes Wi-Fi públicas? (Donde 1 es nada informado y 5 es muy informado)
11	¿Qué considera el mayor riesgo de utilizar redes Wi-Fi públicas?
12	¿Ha recibido información o capacitación sobre el uso seguro de redes Wi-Fi públicas?
13	¿Cree que la mayoría de los usuarios de redes Wi-Fi públicas desconocen los riesgos asociados?
14	Se debe promover la educación sobre ciberseguridad en redes de acceso público
Medidas de seguridad aplicadas	
15	¿Qué medidas de seguridad implementa al usar redes Wi-Fi públicas? (Seleccione todas las opciones que correspondan)
16	¿Con qué frecuencia cambia las contraseñas de sus cuentas personales para prevenir riesgos asociados a redes públicas?
17	¿Cree que las medidas de seguridad que aplica actualmente son...?
Percepción ética	
18	Los usuarios deben ser responsables de su propia seguridad al usar redes públicas.
19	Los administradores de redes Wi-Fi públicas deben garantizar la protección de los datos de los usuarios.
20	Debe ser obligatorio informar a los usuarios sobre las políticas de seguridad de una red Wi-Fi pública antes de su uso.
21	¿En qué grado ético considera el utilizar redes Wi-Fi públicas de manera anónima para actividades no permitidas (como descargas ilegales, piratería)?

Tabla II
Encuesta