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

***Abstract*— 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.**

I. Introducción

En la era de la interconectividad, las redes Wi-Fi públicas desempeñan un papel fundamental al facilitar el acceso a Internet en espacios urbanos y académicos. Sin embargo, la creciente dependencia de estas redes abiertas también expone a los usuarios a riesgos significativos debido a vulnerabilidades en los protocolos de seguridad, la falta de autenticación robusta y la posible explotación de datos personales [1]. Estos riesgos cobran especial relevancia en entornos como universidades y espacios comerciales, donde una gran cantidad de personas se conectan diariamente sin contar con medidas de seguridad adecuadas [2].

La evolución de los estándares Wi-Fi ha estado marcada por esfuerzos constantes para mejorar la seguridad de las conexiones. Inicialmente, el protocolo *Wired Equivalent Privacy (WEP)* fue diseñado para ofrecer una protección básica, pero rápidamente se demostró vulnerable a ataques que comprometían su cifrado [3]. Esto impulsó el desarrollo de *Wi-Fi Protected Access (WPA)* como una solución temporal hasta la implementación de *Wi-Fi Protected Access 2 (WPA2)*, el cual introdujo mejoras como el *handshake* de cuatro pasos para la autenticación de clientes y puntos de acceso [4]. No obstante, WPA2 también presentó debilidades, como los ataques *Key Reinstallation Attack (KRACK)*, que permiten la interceptación y manipulación de datos transmitidos [5].

Para abordar estas vulnerabilidades, se lanzó *Wi-Fi Protected Access 3 (WPA3)*, incorporando mecanismos de autenticación más robustos y mitigando amenazas como los ataques KRACK, *Man-in-the-Middle (MITM)* y los ataques de Diccionario Offline, los cuales buscan descifrar claves precompartidas *(PSK, Pre-Shared Key)* [6]. Además, el estándar *Wi-Fi CERTIFIED Enhanced Open*, basado en WPA3, ha sido propuesto como una solución para mejorar la seguridad en redes públicas mediante el cifrado individual de conexiones [7].

A pesar de estos avances, estudios han demostrado que muchas redes públicas continúan operando sin cifrado adecuado, exponiendo a millones de usuarios a posibles ataques cibernéticos [8]. En particular, un estudio realizado en Moscú reveló que el 25 % de las redes públicas carecen de cifrado adecuado, mientras que otro 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 mejorar la seguridad en redes públicas, promoviendo el uso de protocolos avanzados y la concienciación sobre riesgos cibernéticos [6].

En Ecuador, espacios como centros comerciales, parques públicos y universidades, ofrecen redes Wi-Fi públicas para sus usuarios. Si bien estas

infraestructuras son esenciales para la conectividad, la falta de medidas de seguridad adecuadas podría facilitar la interceptación de datos sensibles y aumentar el riesgo de ataques cibernéticos [1].
Dado este panorama, el presente estudio se llevará a cabo en la ciudad de Quevedo, provincia de Los Ríos, Ecuador, específicamente en tres lugares clave: el Campus Central de la UTEQ, el Campus La María de la UTEQ y el Centro Comercial Paseo Shopping (`https://www.elpaseoshopping.com/quevedo`).
El objetivo es analizar la percepción de los usuarios sobre los riesgos asociados al uso de redes Wi-Fi públicas y evaluar las implicaciones éticas de las prácticas de seguridad adoptadas. A través de este análisis, 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 este apartado se presenta una revisión de la literatura actual sobre los riesgos de seguridad en redes Wi-Fi públicas y la percepción de seguridad en las mismas.

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].
Este tipo de ataque es peligroso en redes Wi-Fi públicas debido a la falta de fuertes mecanismos de autenticación y encriptación [12]. 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. 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. Para disminuir estos ataques, se recomienda evitar redes Wi-Fi públicas desconocidas, utilizar conexiones cifradas como VPNs y preferir redes con autenticación basada en certificados digitales [13].
En entornos académicos, como señalan Mahyoub et al. [14], 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 [15] [16].
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 [17] [18].

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

- **Confianza en Redes Wi-Fi públicas:** Oruma y Petrovic [19] destacan que la confianza de los usuarios en redes públicas proviene de la percepción de que lugares como cafeterías y aeropuertos implementan medidas de seguridad adecuadas. Sin embargo, Bongiovanni et al. [20] advierten que esta confianza no siempre está justificada, ya que las redes en eventos masivos y espacios públicos suelen

carecer de cifrado robusto, exponiéndolas a ataques como MITM o DNS spoofing. Por otra parte, la necesidad de acceso inmediato a Internet frecuentemente supera las preocupaciones de seguridad, lo que lleva a los usuarios a conectarse a redes abiertas sin tomar precauciones adicionales [21]. En consecuencia, la percepción de confianza en redes públicas no siempre se basa en información objetiva, sino en factores contextuales y emocionales.

- **Factores Emocionales:** Diversos estudios han analizado cómo las emociones influyen en la percepción de seguridad en redes Wi-Fi públicas. Según Van Twist et al. [22], los usuarios pueden experimentar ansiedad al realizar transacciones financieras o ingresar credenciales personales en redes abiertas, conscientes del riesgo de robo de datos. Bongiovanni et al. [20] refuerzan esta idea al señalar que en eventos deportivos y espectáculos masivos, la preocupación por la ciberseguridad es alta, particularmente entre aquellos que han sido víctimas de ataques previos. En contraste, Oruma y Petrovic [19] argumentan que una parte significativa de los usuarios presenta optimismo irrealista, minimizando los riesgos bajo la creencia de que llos no les sucederáËste fenómeno es respaldado por David et al. [21], quienes encontraron que los jóvenes y personas con menor educación en ciberseguridad tienden a adoptar comportamientos más riesgosos en redes públicas.
- **Conveniencia o Seguridad:** El equilibrio entre conveniencia y seguridad sigue siendo un desafío en el uso de redes Wi-Fi públicas. Van Twist et al. [22] sostienen que, aunque los usuarios son conscientes de los riesgos, la accesibilidad gratuita a Internet es prioritaria en entornos urbanos. Además, David et al. [21] destacan que la falta de alternativas seguras refuerza esta elección, ya que no siempre es viable utilizar datos móviles o conexiones privadas en espacios públicos. Ahora bien, Oruma y Petrovic [19] indican que en ciudades con políticas de autenticación en redes públicas, la percepción de seguridad puede ser mayor. Sin embargo, Bongiovanni et al. [20] cuestionan la efectividad de estas medidas, señalando que incluso redes con autenticación pueden ser vulneradas mediante ataques avanzados, lo que demuestra que la seguridad percibida no siempre refleja la seguridad real.
- **Falta de Conocimiento:** El desconocimiento sobre ciberseguridad es un factor determinante en la percepción de seguridad de los usuarios. David et al. [21] destacan que muchas personas ignoran la existencia de ataques como evil twin attacks o el sniffing de paquetes, confiando en indicadores superficiales como la presencia de un candado en la barra de direcciones. Por otro lado, Oruma y Petrovic [19] sugieren que la educación en ciberseguridad es clave para reducir estos riesgos, aunque su impacto depende de la voluntad del usuario para adoptar prácticas más seguras. Sin embargo, Van Twist et al. [22] plantean que la educación en ciberseguridad, aunque necesaria, no es suficiente para modificar el comportamiento de los usuarios. Incluso personas con conocimientos avanzados pueden incurrir en prácticas riesgosas por comodidad o simple desinterés. En esta línea, Bongiovanni et al. [20] argumentan que, más allá de la concienciación, es esencial implementar regulaciones más estrictas y mecanismos de seguridad que protejan a los usuarios de manera automática.

II-C. Principios éticos relacionados con la ciberseguridad

La integración de consideraciones éticas en el ámbito de la ciberseguridad es esencial para proteger tanto la información como los derechos y el bienestar de los usuarios. Este aspecto adquiere relevancia en el contexto de las redes Wi-Fi públicas, las cuales forman parte de un entorno digital en el que convergen productos tecnológicos y cadenas de servicios digitales [23]. Dichos productos y servicios se ofrecen a través de estas redes, lo que implica que cualquier vulnerabilidad o falta de ética en su desarrollo o implementación repercute directamente en la seguridad y la protección de los

usuarios.

Formosa et al. [24] propusieron un marco ético basado en cinco principios fundamentales: beneficencia, no maleficencia, autonomía, justicia y explicabilidad. Según estos autores, dichos principios pueden llegar a entrar en conflicto y, por ello, deben ser equilibrados de manera cuidadosa en función del contexto en el que se apliquen. Desde una perspectiva no técnica, Kozhuharova et al. [23] subrayaron la importancia de integrar estos principios en el diseño y desarrollo de productos tecnológicos, para evitar causar daños o efectos negativos a los usuarios. Por su parte, Tronnier et al. [25] aplicaron el marco propuesto por Formosa et al. para examinar los dilemas éticos en las cadenas de servicios digitales, evaluando cómo se ve afectado cada uno de los cinco principios a lo largo de los distintos procesos.

En este contexto, se sintetizan los elementos clave del marco ético:

- **Beneficencia y No Maleficencia:** Las tecnologías de ciberseguridad deben utilizarse para favorecer el bienestar de los usuarios y prevenir daños intencionales [23], [24]. Este principio es crucial en las redes Wi-Fi públicas, donde la exposición a riesgos cibernéticos es alta y la protección de la información es vital.
- **Autonomía:** Se debe garantizar que los usuarios dispongan de la información necesaria para tomar decisiones informadas sobre el uso de servicios tecnológicos. La autonomía implica que las personas puedan evaluar el impacto de estos productos y servicios en sus vidas [24], [25].
- **Justicia:** Es fundamental asegurar la equidad y la accesibilidad en el uso de tecnologías y servicios digitales, evitando sesgos y discriminaciones. Esto implica que los servicios ofrecidos a través de redes Wi-Fi públicas deben beneficiar a todos los usuarios sin exclusiones [24], [25].
- **Explicabilidad:** Las políticas, prácticas y tecnologías en ciberseguridad deben ser claras y comprensibles, permitiendo una rendición de cuentas adecuada y fomentando la transparencia en su implementación [24].
- **Privacidad:** Aunque no se plantea como un principio independiente, la protección de la información personal se integra de forma transversal en el análisis de los cinco principios, permitiendo abordar de manera integral la salvaguarda de la privacidad [24].

Se reconoció además que estos principios pueden entrar en conflicto y, por ello, su aplicación práctica requiere un equilibrio sensible al contexto. Formosa et al. [24] destacaron que no existen soluciones exclusivamente técnicas para resolver los dilemas éticos, puesto que ignorar estas consideraciones no elimina los problemas inherentes. Tronnier et al. [25] evidenciaron que los problemas éticos en las cadenas de servicios digitales afectan de manera diferenciada a cada principio, lo que demanda medidas compensatorias específicas. En consecuencia, Kozhuharova et al. [23] recomendaron la implementación de estrategias organizativas y tecnológicas —como la elaboración de una lista de requisitos éticos— para garantizar la protección de los derechos y libertades de los usuarios en el desarrollo y aplicación de nuevas tecnologías.

La revisión realizada evidencia que se han abordado principalmente las vulnerabilidades técnicas de las redes Wi-Fi públicas, la falta de concienciación de los usuarios frente a las amenazas y los principios éticos relacionados con la ciberseguridad. Sin embargo, no profundizan en los aspectos éticos relacionados con la percepción de seguridad de los usuarios en redes Wi-Fi públicas, particularmente en entornos académicos.

Por lo tanto, esta investigación se enfoca en realizar un análisis ético sobre las percepciones de los usuarios de las redes Wi-Fi públicas. A través de una encuesta estructurada, se recogieron datos que permiten identificar las prácticas habituales de los usuarios, su conocimiento sobre las vulnerabilidades de estas redes y las implicaciones éticas relacionadas con su uso.

III. Estudio Propuesto

El presente estudio es un análisis enfocado en la percepción de los usuarios sobre los riesgos y aspectos éticos asociados al uso de redes Wi-Fi públicas. Este estudio se fundamenta en la recopilación de datos mediante encuestas aplicadas a los usuarios.

Los objetivos específicos del análisis son los siguientes:

- Evaluar el grado de información que poseen los usuarios acerca de los riesgos de seguridad al conectarse a redes Wi-Fi públicas.
- Identificar las percepciones de los usuarios respecto a la seguridad de estas redes y las medidas que consideran adecuadas para proteger sus datos personales.
- Presentar un análisis basado en los datos recopilados, ofreciendo una perspectiva clara sobre el conocimiento y las prácticas actuales de los usuarios al conectarse a redes Wi-Fi públicas.

IV. Materiales y métodos

El presente estudio adoptó un enfoque exploratorio con el objetivo de recopilar 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**: Se realizó un análisis de literatura científica y estudios previos relacionados con la seguridad y la percepción ética en el uso de redes Wi-Fi públicas. Esta fase permitió fundamentar el diseño del cuestionario.
2. **Diseño del instrumento de recolección de datos**: A partir de la información obtenida en la revisión del estado del arte, se elaboró un cuestionario estructurado, organizado en las siguientes áreas temáticas:
   - Información demográfica.
   - Frecuencia de uso de redes Wi-Fi públicas.
   - Conocimiento sobre los riesgos asociados.
   - Medidas de seguridad aplicadas.
   - Percepción ética.
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 empleó la fórmula para poblaciones finitas propuesta por Lohr [26]:

$$n = \frac{U_o \cdot P \cdot Q \cdot Z^2}{(U_o - 1) \cdot e^2 + P \cdot Q \cdot Z^2} \quad (1)$$

Donde:

- ***Tamaño de la muestra*** ***(n):*** Son las encuestas mínimas realizadas.
- ***Población objetivo*** ***($U_o = 206,008$):*** Se tomó como referencia la población de la ciudad de Quevedo según el Instituto Nacional de Estadística y Censos (INEC) en su informe del año 2022 [27]. Esta cifra representa el universo total de individuos dentro del área geográfica de estudio.
- ***Proporción de aceptación*** ***($P = 0{,}9$ y proporción de rechazo $Q = 0{,}1$):*** Se asumió que el 90 % de la población encuestada podría tener conocimiento o una percepción sobre los riesgos y aspectos éticos del uso de redes Wi-Fi públicas, mientras que el 10 % restante no. Teniendo en cuenta la relación $P + Q = 1$.
- ***Nivel de confianza del 95 %*** $Z = 1{,}96$***:*** El nivel de confianza representa la probabilidad de que la muestra seleccionada refleje con precisión las características de la población total. Se eligió un 95 % de confianza, un estándar común en estudios de encuestas y análisis de percepción, ya que ofrece un equilibrio entre precisión y margen de error [26]. En una distribución normal, este nivel de confianza corresponde a un valor crítico $Z = 1{,}96$, lo que significa que el intervalo de confianza abarca aproximadamente 1.96 desviaciones estándar en ambos sentidos de la media, cubriendo así el 95 % de los posibles valores muestrales.
- ***Margen de error*** $e = 0{,}05$***:*** Se esta-

bleció un margen de error del 5 %, lo que indica que los resultados obtenidos en la muestra pueden diferir en hasta ±5 puntos porcentuales de los valores reales en la población. Este valor es ampliamente utilizado en estudios de encuestas y percepción, ya que proporciona un equilibrio entre precisión y tamaño muestral, evitando una muestra excesivamente grande que podría ser innecesaria o poco práctica [26].

$$n = \frac{(206008) \cdot (0{,}9) \cdot (0{,}1) \cdot (1{,}96)^2}{(206008 - 1) \cdot (0{,}05)^2 + (0{,}9) \cdot (0{,}1) \cdot (1{,}96)^2} \tag{2}$$

4. **Aplicación del cuestionario**: Una vez determinado el tamaño de la muestra, el cuestionario fue distribuido a través de la plataforma Google Forms, lo que permitió llegar a una mayor cantidad de participantes de manera eficiente. Se garantizó la confidencialidad y el anonimato de las respuestas, en cumplimiento con los principios éticos de la investigación.
5. **Procesamiento y análisis de datos**: Finalizada la fase de recolección de datos, las respuestas obtenidas fueron organizadas y analizadas utilizando las herramientas de Google Forms, que permitieron generar resúmenes estadísticos en forma de gráficos de barras y diagramas circulares [28], para facilitar la interpretación de los resultados.

V. Resultados

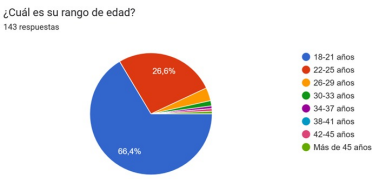

Fig. 1: Rango de edad de los encuestados

La mayoría de los encuestados se encontraba en el rango de 18 a 21 años (66.4 %), seguido del grupo de 22 a 25 años (26.6 %). Los demás grupos etarios representaron menos del 5 % de la muestra, con una presencia mínima de personas mayores de 30 años (Figura 1). Esto indica que la población estudiada está mayoritariamente compuesta por jóvenes, quienes suelen tener un uso intensivo de dispositivos móviles y una mayor exposición a redes Wi-Fi públicas.

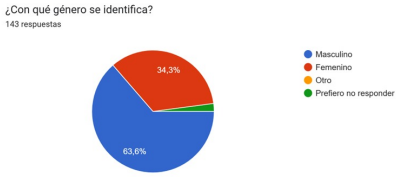

Fig. 2: Género de los encuestados

Del total de encuestados, 63.6 % se identificó como masculino y 34.3 % como femenino, mientras que un 2.1 % prefirió no responder (Figura 2). Esta distribución de género no muestra una diferencia significativa en el acceso a redes Wi-Fi públicas, lo que sugiere que el uso de estas redes es generalizado en ambos grupos.

Fig. 3: Nivel educativo de los encuestados

El 65.7 % de los encuestados indicó que su nivel educativo más alto es educación superior incompleta, seguido de secundaria completa (16.8 %) y educación superior completa (11.2 %) (Figura 3). El acceso a redes Wi-Fi públicas, en este contexto, parece estar estrechamente vinculado a la educación superior, ya que la mayoría de los encuestados son estudiantes universitarios.

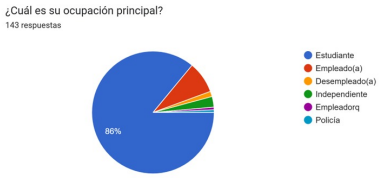

Fig. 4: Ocupación principal de los encuestados

El 86.0 % de los encuestados indicó que su ocupación principal es ser estudiante, seguido de empleados (8.4 %) (Figura 4). Este dato refuerza la idea de que los entornos académicos constituyen uno de los espacios donde más se accede a redes Wi-Fi públicas.

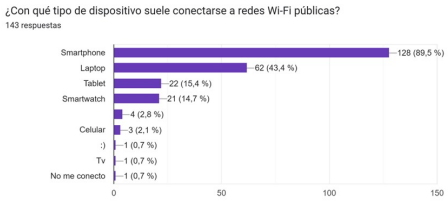

Fig. 5: Tipo de dispositivo usado

El 89.5 % de los encuestados utiliza smartphones (Figura 5) como principal dispositivo de conexión, lo que sugiere una vulnerabilidad mayor exposición a amenazas, como el Evil Twin y el MITM, en comparación con equipos de escritorio.

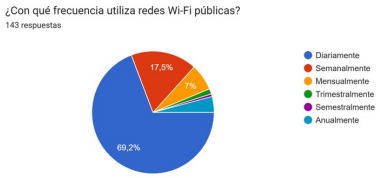

Fig. 6: Frecuencia de uso de redes Wi-Fi públicas

El 69.2 % de los participantes respondió que utiliza redes Wi-Fi públicas diariamente, mientras que un 17.5 % lo hace semanalmente (Figura 6). Estos resultados reflejan una alta dependencia de estas redes para actividades cotidianas.

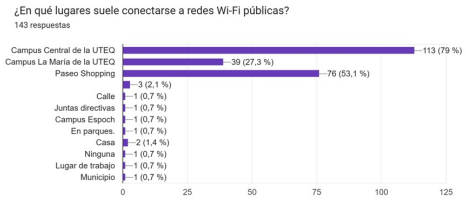

Fig. 7: Lugares de conexión

Los lugares más frecuentes donde los encuestados acceden a redes Wi-Fi públicas fueron el Campus Central de la UTEQ (79.0 %), seguido del Paseo Shopping (53.1 %) y el Campus La María de la UTEQ (27.3 %) (Figura 7). Esto sugiere que los entornos educativos y comerciales son los principales puntos de acceso.

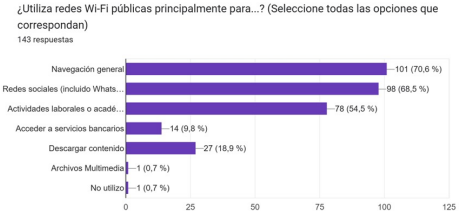

Fig. 8: Uso de las redes Wi-Fi

Las actividades más comunes realizadas en redes Wi-Fi públicas fueron navegación general (70.6 %), uso de redes sociales (68.5 %) y actividades laborales o académicas (54.5 %) (Figura 8). En contraste, solo un 9.8 % utilizó estas redes para acceder a servicios bancarios, lo que sugiere que los usuarios reconocen el riesgo de ingresar información financiera en redes abiertas.

Fig. 9: Verificación de redes auténticas

El 18.2 % de los encuestados indicó que siempre verifica la autenticidad de la red, mientras que un 27.3 % lo hace con frecuencia. Sin embargo, un 32.9 % rara vez toma esta precaución y un 21.7 % nunca lo hace (Figura 9). Esto indica que una parte significativa de los usuarios se conecta a redes Wi-Fi públicas sin verificar su legitimidad.

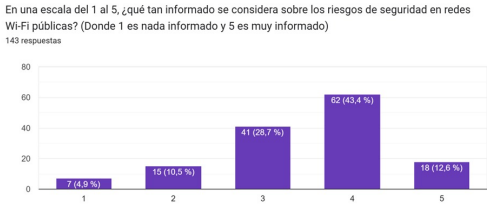

Fig. 10: Nivel de conocimiento sobre seguridad

El 43.4 % de los encuestados afirmó estar algo informado, mientras que solo el 12.6 % se considera muy informado. En contraste, un 15.4 % indicó que tiene poco o ningún conocimiento sobre estos riesgos (Figura 10).

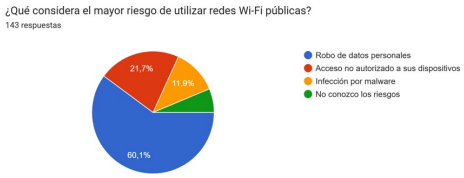

Fig. 11: Mayor riesgo de uso

El 60.1 % de los encuestados señaló que el mayor riesgo es el robo de datos personales, seguido del acceso no autorizado a dispositivos (21.7 %) y la infección por malware (11.9 %) (Figura 11).

Fig. 12: Nivel de capacitación

El 15.4 % indicó haber recibido información en su lugar de trabajo o estudio, mientras que el 43.4 % lo hizo por iniciativa propia. Sin embargo, un 41.3 % nunca ha recibido capacitación, lo que sugiere una brecha en la educación sobre seguridad digital (Figura 12).

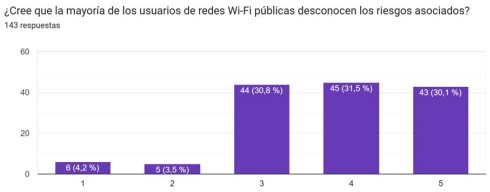

Fig. 13: Percepción de los encuestados

El 61.6 % de los encuestados estuvo de acuerdo o totalmente de acuerdo con que la mayoría de los usuarios desconocen los riesgos, lo que refuerza la necesidad de educación en ciberseguridad (Figura 13).

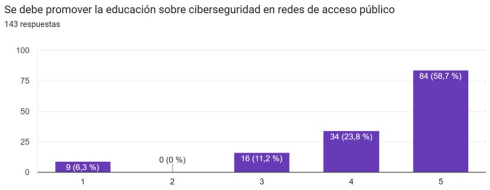

Fig. 14: Educación sobre ciberseguridad

El 82.5 % de los encuestados estuvo de acuerdo o totalmente de acuerdo con que se debe promover la educación en ciberseguridad (Figura 14).

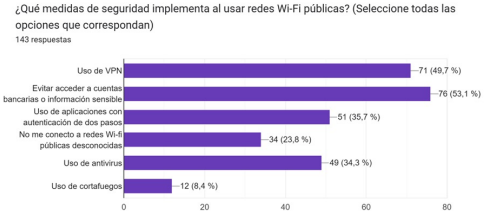

Fig. 15: Medidas de seguridad

Las principales medidas de seguridad adoptadas fueron evitar acceder a cuentas bancarias (53.1 %), uso de VPNs (49.7 %) y autenticación de dos factores (35.7 %) (Figura 15).

Fig. 16: Prevención de riesgos

El 41.3 % de los encuestados cambia sus contraseñas cada 3 a 6 meses, mientras que un 14.0 % nunca las cambia (Figura 16).

Fig. 17: Medidas de seguridad aplicadas

La mayoría de los encuestados (56.6 %) creen que las medidas de seguridad que usan son moderadamente suficientes, seguidos de un 25.2 % que las considera poco suficientes (Figura 17).

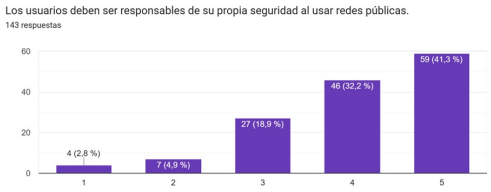

Fig. 18: Responsabilidad sobre su propia seguridad

El 73.5 % estuvo de acuerdo o totalmente de acuerdo con esta afirmación (Figura 18).

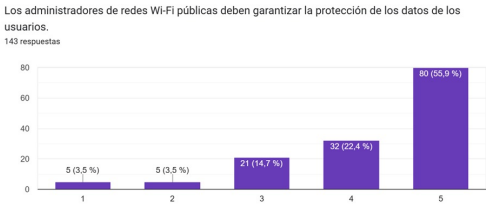

Fig. 19: Protección de los administradores

El 78.3 % de los encuestados manifestó estar de acuerdo o totalmente de acuerdo con esta afirmación (Figura 19).

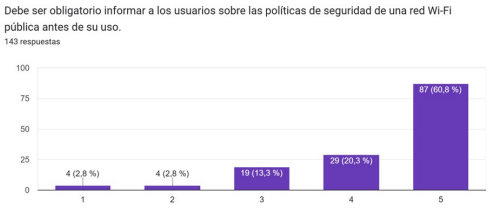

Fig. 20: Conocimiento sobre las políticas de seguridad

El 81.1 % de los encuestados estuvo de acuerdo o totalmente de acuerdo con esta afirmación (Figura 20).

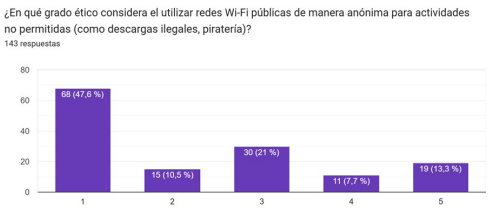

Fig. 21: Grado ético sobre el uso indebido de estas redes

El 47.6 % lo consideró muy poco ético, mientras que solo un 13.3 % lo consideró ético (Figura 21).

VI. Discusión

Los hallazgos de este estudio evidenciaron que la muestra, compuesta mayoritariamente por jóvenes

(66.4 % entre 18 y 21 años, Figura 1), corresponde a una población con alta exposición a tecnologías móviles, lo cual se refleja en el predominio del smartphone como dispositivo de acceso (89.5 %, Figura 5). La alta frecuencia de uso diario de redes Wi-Fi públicas (69.2 %, Figura 6) indica que estos espacios digitales se han vuelto esenciales para actividades cotidianas, especialmente en entornos académicos y comerciales, como lo demuestran los lugares de conexión (Campus Central de la UTEQ, 79.0 %; Paseo Shopping, 53.1 %, Figura 7).

A pesar de la elevada dependencia de estas redes, se observa una preocupante brecha en las prácticas de seguridad. Solo un 18.2 % de los encuestados verificaba siempre la autenticidad de la red (Figura 9), lo cual los hace susceptibles a ataques MITM y Evil Twin. Asimismo, aunque el 60.1 % identificó el robo de datos personales como el principal riesgo (Figura 11), la percepción del nivel de conocimiento sobre seguridad fue moderada, con solo un 12.6 % considerándose muy informados (Figura 10). Esta discontinuidad entre la conciencia del riesgo y la adopción de medidas preventivas sugiere la necesidad de intensificar los esfuerzos en educación y capacitación en ciberseguridad.

En cuanto a las medidas de seguridad implementadas, los resultados muestran que la mayoría de los usuarios optó por estrategias básicas como evitar ingresar información sensible (53.1 %) y utilizar VPNs (49.7 %), aunque se reconoce que estas prácticas son calificadas como moderadamente suficientes por el 56.6 % de la muestra (Figura 15 y Figura 17). La frecuencia de cambio de contraseñas, siendo que un 41.3 % lo realiza cada 3 a 6 meses, refleja también una aproximación rutinaria, pero insuficiente para disminuir en su totalidad estos riesgos.

La dimensión ética abordada en la encuesta revela una percepción dual de responsabilidad. Por un lado, el 73.5 % de los encuestados considera que los usuarios deben ser responsables de su propia seguridad (Figura 18), y por otro lado, un 78.3 % opina que los administradores de redes Wi-Fi públicas deben garantizar la protección de los datos (Figura 19). Además, el consenso sobre la necesidad de informar a los usuarios acerca de las políticas de seguridad (81.1 %, Figura 20) refuerza la importancia de adoptar métodos que combinen medidas técnicas y éticas.

VII. Conclusiones

El estudio mostró que la mayoría de los usuarios de redes Wi-Fi públicas en Quevedo son jóvenes universitarios que dependen mucho de estas conexiones, pero no están bien informados sobre sus riesgos. Aunque muchos reconocen que el robo de datos personales es una amenaza, son muy pocos los que verifican si las redes a las que se conectan son seguras, lo que los hace vulnerables a ataques como MITM y Evil Twin [11], [14].

Si bien algunos toman medidas como usar VPNs o activar la autenticación en dos pasos, estas acciones no son suficientes para evitar todos los riesgos [7], [12]. Un problema importante es la falta de educación sobre ciberseguridad, ya que muchos nunca han recibido capacitación sobre cómo protegerse en redes Wi-Fi públicas. Reducir estos peligros requiere que los usuarios comprendan los riesgos y adopten medidas simples, como evitar redes sospechosas, desactivar la opción de compartir datos y usar herramientas como VPNs para proteger su información [10], [19]. La educación y la concienciación juegan un papel clave en la seguridad digital, ya que la tecnología por sí sola no basta [21].

Los resultados también reflejan que la seguridad en redes Wi-Fi públicas es vista como una responsabilidad compartida. Aunque cada persona debe tomar precauciones, también se espera que los administradores de redes mejoren la seguridad y sean más claros sobre sus políticas [24]. Para lograr un equilibrio, es importante que existan normativas más estrictas y que se promuevan buenas prácticas en la administración de redes [25].

La combinación de educación, tecnología y normativas permite 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. De esta forma, se reducirá la exposición de los usuarios a ataques y se fomentará un uso más seguro y responsable de

estas conexiones [9], [23].

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.

References

[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] 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

[13] 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.

[14] 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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

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

[27] Instituto Nacional de Estadística y Censos (INEC), "Censo Ecuador," 2025, consultado el 12 de febrero de 2025. [Online]. Available: https://geo.cepal.org/censo-ecuador/

[28] 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)?

TABLE I: Encuesta