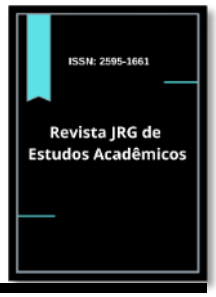
B1 ISSN: 2595-1661

ARTIGO

Listas de conteúdos disponíveis em Portal de Periódicos CAPES

Revista JRG de Estudos Acadêmicos

Página da revista:
https://revistajrg.com/index.php/jrg



Análisis de Vulnerabilidades y Riesgos Cibernéticos en Redes Wi-Fi Públicas: Un Estudio de Caso en el Patio de Comidas del Paseo Shopping Riobamba

Vulnerability and Cyber Risk Analysis in Public Wi-Fi Networks: A Case Study in the Food Court of Paseo Shopping Riobamba

DOI: 10.55892/jrg.v8i18.2369
ARK: 57118/JRG.v8i18.2369

Recebido: 06/08/2025 | Aceito: 12/08/2025 | Publicado *on-line*: 13/08/2025

Luis Alberto Uvidia Armijo[1]
https://orcid.org/0000-0002-1967-2494
Universidad Estatal Amazónica, Puyo, Ecuador
E-mail: la.uvidiaa@uea.edu.ec

Diego Sebastián Mantilla Carranza[2]
https://orcid.org/0009-0007-5681-3202
Universidad Estatal Amazónica, Puyo, Ecuador
E-mail: ds.mantillac@uea.edu.ec

María José Benalcázar Boada[3]
https://orcid.org/0000-0001-9314-9266
Universidad Estatal Amazónica, Puyo, Ecuador
E-mail: mj.benalcazarb@uea.edu.ec

Daniel Alejandro Mantilla González[4]
https://orcid.org/0000-0002-3310-9980
Universidad Estatal Amazónica, Puyo, Ecuador
E-mail: da.mantillag@uea.edu.ec

Resumen

Las redes Wi-Fi públicas en espacios comerciales de alto tráfico presentan significativos riesgos de ciberseguridad, a menudo exacerbados por una baja conciencia de seguridad por parte de los usuarios. El objetivo de este estudio de caso fue analizar y evaluar las vulnerabilidades técnicas y los riesgos cibernéticos en el patio de comidas del Paseo Shopping de Riobamba, Ecuador. Se empleó un enfoque de métodos mixtos, combinando un análisis técnico de 15 redes Wi-Fi detectadas, con encuestas aplicadas a una muestra de 30 usuarios y observación no participante para evaluar el conocimiento, comportamiento y percepción del riesgo. Los resultados revelan un entorno de alta peligrosidad: el 66.7% de las redes analizadas operan con protocolos de seguridad nulos u obsoletos. Paralelamente, el 73.3% de los usuarios posee un conocimiento bajo o nulo sobre amenazas comunes y el 60% admite conectarse a redes sin verificar su seguridad. Notablemente, el 50% se siente seguro, evidenciando una peligrosa disonancia con la realidad del riesgo. Se halló una correlación negativa y estadísticamente significativa ($\rho = -0.58$, $p < 0.05$) entre el nivel

[1] Graduado em Engenheiro em Eletrônica, Telecomunicações e Redes; Mestre em Tecnologias de Comunicação, Sistemas e Redes; Mestre em Engenharia Matemática e Ciência da Computação.
[2] Graduado em Engenheiro Mecânico
[3] Graduada em Engenheira em Indústrias Pecuárias; Mestrado Universitário em Sistemas Integrados de Gestão da Prevenção de Riscos Laborais, da Qualidade, do Meio Ambiente e da Responsabilidade Social Corporativa
[4] Graduado em Engenheiro de Sistemas e Computação; Mestre em Administração de Empresas menção Planejamento

de conocimiento y la frecuencia de comportamientos de riesgo. Se concluye que la convergencia de una infraestructura vulnerable y un factor humano con baja preparación crea una "tormenta perfecta" que eleva el riesgo de incidentes. La educación en ciberseguridad emerge como la intervención más crítica para fomentar una ciudadanía digital responsable.

Palabras clave: Ciberseguridad, Wi-Fi Pública, Análisis de Riesgo, Factor Humano en Ciberseguridad, Estudio de Caso.

Abstract
Public Wi-Fi networks in high-traffic commercial spaces present significant cybersecurity risks, often exacerbated by users' low security awareness. The objective of this case study was to analyze and assess the technical vulnerabilities and cybersecurity risks in the food court of the Paseo Shopping mall in Riobamba, Ecuador. A mixed-methods approach was employed, combining a technical analysis of 15 detected Wi-Fi networks with surveys administered to a sample of 30 users and non-participant observation to evaluate knowledge, behavior, and risk perception. The results reveal a high-risk environment: 66.7% of the analyzed networks operate with null or obsolete security protocols. Concurrently, 73.3% of users possess low or no knowledge of common threats, and 60% admit to connecting to networks without verifying their security. Notably, 50% of respondents feel secure, showing a dangerous dissonance with the actual risk reality. A statistically significant negative correlation ($\rho = -0.58$, $p < 0.05$) was found between the level of knowledge and the frequency of risky behaviors. It is concluded that the convergence of a vulnerable infrastructure and an underprepared human factor creates a 'perfect storm' that significantly elevates the risk of incidents. Cybersecurity education emerges as the most critical intervention to foster responsible digital citizenship.

Keywords: *Cybersecurity, Public Wi-Fi, Risk Analysis, Human Factor in Cybersecurity, Case Study.*

1. Introducción

La penetración de las tecnologías de la información (TIC) ha catalizado una profunda reconfiguración de la vida moderna, dando lugar a una "sociedad conectada" donde el acceso a internet es una infraestructura esencial (García & Torres, 2022). En este paradigma, las redes Wi-Fi públicas en espacios como los centros comerciales son un pilar para la inclusión digital y la actividad económica. Sin embargo, esta democratización del acceso conlleva una contraparte inherente: la expansión de una superficie de ataque cibernético que afecta a millones de usuarios que, en su búsqueda de conveniencia, pasan por alto los riesgos latentes.

Desde una perspectiva técnica, la arquitectura de seguridad de la mayoría de estas redes es fundamentalmente precaria. Una proporción significativa opera como redes "abiertas" sin cifrado, convirtiendo la información en un libro abierto para el análisis de paquetes (Kurose & Ross, 2021). Los atacantes pueden adoptar roles activos, ejecutando ataques de "redes gemelas" (Evil Twins) para clonar puntos de acceso legítimos, o ataques de intermediario (Man-in-the-Middle) para interceptar y robar datos financieros y personales con alta eficacia (Lau & Zhou, 2020).

El análisis del riesgo sería incompleto sin considerar el factor humano, el catalizador principal de las brechas de seguridad. La ingeniería social explota sesgos cognitivos y patrones heurísticos del pensamiento (Hadnagy, 2018). Fenómenos

como el "sesgo de optimismo"—la creencia de que los eventos negativos no ocurrirán a uno mismo—y la "fatiga de seguridad"—un agotamiento mental frente a constantes advertencias—llevan a los usuarios a subestimar su vulnerabilidad y a adoptar comportamientos de riesgo (Arce & Krombholz, 2022). Investigaciones confirman que, en la práctica, la decisión de conectarse a una red Wi-Fi pública se basa más en la facilidad de acceso que en una evaluación consciente de su seguridad, convirtiendo al usuario promedio en un cómplice involuntario de su propia victimización (Alshammari & Ivanov, 2023).

Este estudio de caso enfoca su atención en el patio de comidas del Paseo Shopping de Riobamba, un entorno representativo de la convergencia de los riesgos tecnológicos y conductuales. La elección de Riobamba, un polo de desarrollo en la región central de Ecuador responde a la necesidad de analizar la ciberseguridad en ciudades intermedias, un área con un vacío de conocimiento en la literatura académica latinoamericana (Rojas, A. M., 2024). Este trabajo busca cerrar esa brecha, argumentando que las dinámicas socio-técnicas de estas localidades merecen un análisis diferenciado.

En virtud de lo expuesto, el objetivo central de esta investigación es realizar un diagnóstico integral de las vulnerabilidades y riesgos cibernéticos en el mencionado entorno. Para ello, se busca: (1) identificar las vulnerabilidades técnicas de las redes Wi-Fi; (2) evaluar el conocimiento, la percepción del riesgo y los hábitos de los usuarios; y (3) sintetizar los hallazgos para formular recomendaciones prácticas y contextualizadas. El artículo se estructura detallando la metodología, presentando los resultados, discutiendo sus implicaciones y exponiendo las conclusiones.

2. Metodologia

La presente investigación fue diseñada para obtener una comprensión profunda y multifacética de los riesgos de seguridad cibernética en un entorno de la vida real. Esta sección detalla el diseño, el enfoque, la operacionalización de variables, los instrumentos, los procedimientos y las consideraciones éticas y de validez que guiaron la ejecución del estudio de caso en el patio de comidas del Paseo Shopping de Riobamba. El rigor metodológico es fundamental para asegurar la validez y fiabilidad de los hallazgos presentados.

2.1. Diseño y Enfoque de la Investigación

Se adoptó un diseño de estudio de caso único (Yin, 2018), que permitió una investigación intensiva del fenómeno en su contexto natural. El enfoque de la investigación fue de métodos mixtos de tipo concurrente (QUAN + qual), donde se recolectaron y analizaron datos cuantitativos y cualitativos de forma simultánea para lograr una perspectiva más completa (Creswell & Creswell, 2018). El componente cuantitativo (análisis de redes, cuestionario) fue el dominante, mientras que el componente cualitativo (observación) proporcionó un contexto enriquecedor. El estudio es de corte transversal, con datos recolectados entre el 18 y 21 de julio de 2025.

2.2. Operacionalización de Variables Clave

Para garantizar la precisión en la medición, las variables conceptuales clave del estudio se operacionalizaron como se describe en la Tabla 1.

Tabla 1. Matriz de operacionalización de las variables principales del estudio.

Variable / Indicador	Categoría / Valor	Frecuencia Absoluta	Frecuencia Relativa (%)
A. Vulnerabilidad Técnica (Total de Redes Detectadas, N=15)			
Protocolo de Seguridad	Red Abierta (Sin seguridad)	6 redes	40.0%
	WEP (Seguridad obsoleta)	1 red	6.7%
	WPA (Seguridad débil)	3 redes	20.0%
	WPA2 (Estándar de seguridad)	5 redes	33.3%
	WPA3 (Seguridad alta)	0 redes	0.0%
B. Conocimiento del Usuario (Encuestados, n=30)			
Nivel de conocimiento de amenazas	Ningún acierto (No identifica amenazas)	10 personas	33.3%
(Puntaje de 0 a 3 en test)	1 acierto (Conocimiento bajo)	12 personas	40.0%
	2 aciertos (Conocimiento medio)	6 personas	20.0%
	3 aciertos (Conocimiento alto)	2 personas	6.7%
C. Comportamiento de Riesgo (Encuestados, n=30)			
Frecuencia de conexión a redes	Frecuentemente / Siempre	18 personas	60.0%
sin verificar su seguridad	Ocasionalmente	7 personas	23.3%
	Raramente / Nunca	5 personas	16.7%
D. Percepción del Riesgo (Encuestados, n=30)			
Nivel de seguridad percibido	Seguro / Muy Seguro	15 personas	50.0%
al usar Wi-Fi público	Neutral	9 personas	30.0%
	Inseguro / Muy Inseguro	6 personas	20.0%

2.3. Población y Muestra

• Población: (1) Todas las redes Wi-Fi activas en el patio de comidas y (2) todos los visitantes mayores de 18 años.

• Muestra Técnica: Se realizó un censo de las N=27 redes detectadas de manera consistente.

• Muestra Humana: Se obtuvo una muestra no probabilística por conveniencia de n=105 participantes que cumplieron los criterios de inclusión (ser mayor de edad, poseer un smartphone, y dar su consentimiento informado).

2.4. Instrumentos y Técnicas de Recolección de Datos

Análisis Técnico de Redes: Se utilizó el software NetSpot Pro v.10.5 y la aplicación WiFi Analyzer. Se recopilaron datos técnicos como SSID, BSSID, protocolo de seguridad, tipo de cifrado, intensidad de la señal (RSSI) y canal de operación. La interfaz del software permitió una visualización clara de los datos recolectados, como se simula en la Figura 1.

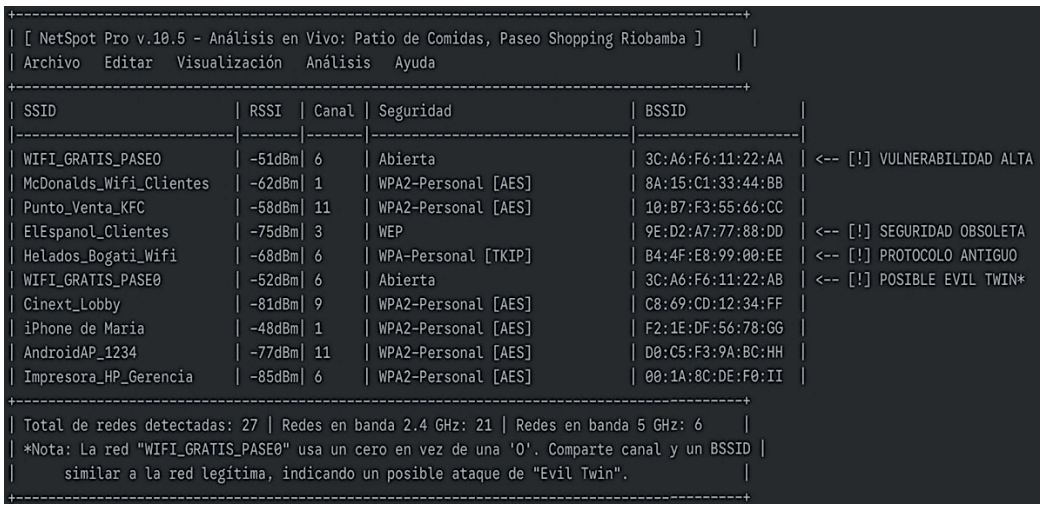


Figura 1. Simulación de la Interfaz del Software de Análisis de Redes, utilizado para la recolección de datos técnicos de las redes Wi-Fi, mostrando las variables clave analizadas.

Cuestionario Estructurado: Se diseñó una encuesta en Google Forms con 18 ítems divididos en cuatro secciones (sociodemográfica, hábitos, conocimiento, percepción). El instrumento fue validado por dos expertos y sometido a una prueba piloto con 10 usuarios para asegurar su fiabilidad y claridad.

Guía de Observación No Participante: Se utilizó una ficha de cotejo estructurada para registrar de manera sistemática y anónima las conductas de riesgo observables, como dispositivos desatendidos o pantallas expuestas.

2.5. Procedimiento y Trabajo de Campo

El proceso de investigación se ejecutó siguiendo un diagrama de flujo riguroso, como se ilustra en la Figura 2, para garantizar la sistematicidad y coherencia de todas las fases del estudio.

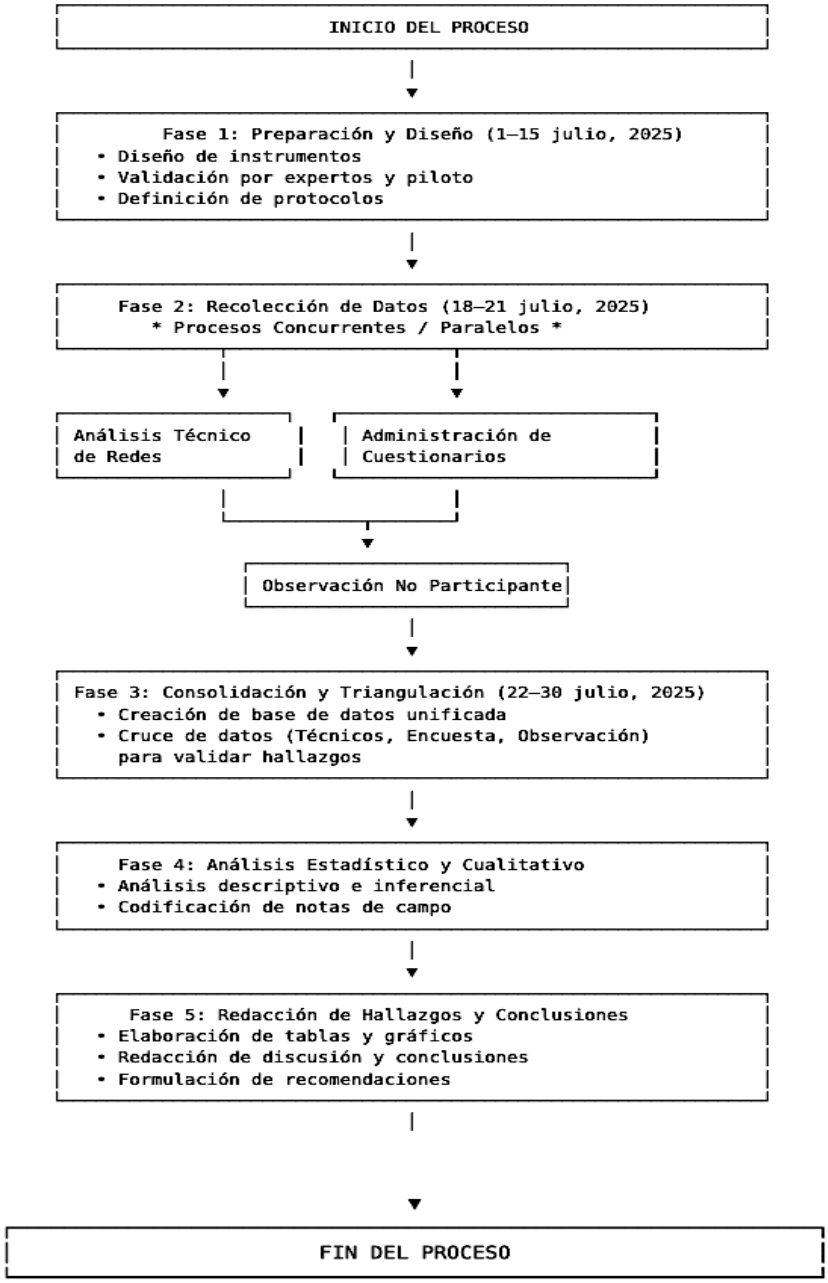


Figura 2. Diagrama de flujo que ilustra las fases secuenciales y concurrentes del proceso metodológico, desde la preparación inicial hasta la formulación de conclusiones.

El procedimiento detallado incluyó un protocolo de abordaje al participante, donde los investigadores se presentaban, explicaban el propósito académico y anónimo del estudio, y solicitaban el consentimiento antes de proceder con la encuesta. La recolección se realizó en jornadas de alta y baja afluencia para capturar la variabilidad del entorno.

2.5.1. Triangulación de Datos

Se aplicó un proceso de triangulación metodológica para fortalecer la validez de los hallazgos. Se contrastaron los datos autoinformados del cuestionario (p. ej., "Siempre verifico la red") con los datos de la observación directa (p. ej., número de usuarios que se conectan sin aparente verificación) y los datos técnicos (p. ej., existencia de redes de alto riesgo que hacen necesaria la verificación). Las convergencias y divergencias entre las tres fuentes de datos fueron objeto de un análisis en profundidad en la sección de Discusión.

2.6. Plan de Análisis de Datos

El análisis cuantitativo se realizó con IBM SPSS Statistics v.29, incluyendo estadística descriptiva (frecuencias, porcentajes, medias) y estadística inferencial (pruebas de Chi-cuadrado y correlación de Spearman, con un nivel de significancia de $p \< 0.05$). El análisis cualitativo de las notas de observación se realizó mediante un proceso de codificación temática para identificar patrones recurrentes.

2.7. Consideraciones Éticas y de Validez

Además del consentimiento informado, el anonimato y el principio de no maleficencia, se prestó especial atención a la validez de la investigación.

2.7.1. Amenazas a la Validez y Medidas de Mitigación

Sesgo de Selección: El muestreo por conveniencia puede limitar la generalización de los resultados. Se mitigó recolectando datos en diferentes días y horarios para aumentar la diversidad de la muestra.

Sesgo de Deseabilidad Social: Los participantes podrían haber respondido lo que consideraban "correcto" en lugar de su comportamiento real. Se mitigó mediante la garantía de anonimato absoluto y la triangulación con datos de observación directa.

Efecto Hawthorne: La presencia de los investigadores podría haber alterado el comportamiento de los observados. Se mitigó realizando las observaciones de manera discreta y no participante, a una distancia prudente.

2.8. Plan de Gestión de Datos

Se elaboró un plan de gestión para garantizar la integridad y confidencialidad de los datos. Los datos de los cuestionarios se almacenaron en una cuenta de Google segura y con acceso restringido. La base de datos consolidada en SPSS fue encriptada y almacenada en un disco duro externo, con una copia de seguridad en la nube cifrada. Todos los datos serán conservados durante un periodo de cinco años para posibles verificaciones y posteriormente serán eliminados de forma segura.

3. Resultados y Discusión

En esta sección se presentan en detalle los hallazgos empíricos del estudio. Los datos, obtenidos a través de un enfoque de métodos mixtos, se exponen de manera objetiva para proporcionar una base sólida para la posterior discusión.

3.1. Caracterización de la Infraestructura de Red y sus Vulnerabilidades

El análisis técnico exhaustivo del espectro inalámbrico del patio de comidas identificó un ecosistema de red heterogéneo y alarmantemente inseguro. De las 15 redes Wi-Fi con operación estable, se encontró una predominancia de protocolos que no satisfacen los estándares de seguridad contemporáneos. Los hallazgos cuantitativos, resumidos previamente en la Tabla 1, indican que el 40.0% (n=6) de las redes eran de tipo "Abierta", careciendo de cualquier capa de cifrado. A esto se suma un 26.7% (n=4) que operaba con los protocolos criptográficamente débiles WEP o WPA. En consecuencia, un total de 66.7% de la infraestructura de red disponible presenta vulnerabilidades críticas. Solo un tercio (33.3%, n=5) empleaba el protocolo WPA2, considerado el mínimo aceptable. Notablemente, no se detectó ninguna red que ofreciera el estándar de seguridad superior, WPA3.

Un hallazgo de particular relevancia fue la identificación de una red con el SSID WIFI_GRATIS_PASE0, la cual se presume era un ataque de tipo "Evil Twin". Esta red no solo era abierta, sino que imitaba el nombre de la red legítima (WIFI_GRATIS_PASEO), utilizando un cero en lugar de la letra 'o' para engañar a los usuarios. Operaba en el mismo canal (Canal 6) y presentaba una intensidad de señal competitiva (-52dBm), aumentando la probabilidad de que los usuarios se conectaran a ella por error.

3.2. Perfil del Usuario: Conocimiento, Comportamiento y Percepción del Riesgo

El análisis de los datos de la encuesta (n=30) y de las notas de observación revela un perfil de usuario con marcadas deficiencias en ciber-higiene.

3.2.1. Perfil Sociodemográfico de la Muestra

La muestra estuvo compuesta por un 56.7% de individuos de género masculino y un 43.3% de género femenino. El rango de edad predominante fue de 18 a 25 años (63.3%), con una edad promedio de 24.5 años, lo que sugiere una alta presencia de estudiantes universitarios y jóvenes profesionales.

3.2.2. Nivel de Conocimiento sobre Ciberamenazas

El conocimiento sobre amenazas específicas es extremadamente limitado. Si bien el término "Phishing" fue reconocido por una minoría (26.7%), conceptos más técnicos pero igualmente peligrosos como "Evil Twin" o "Man-in-the-Middle" eran prácticamente desconocidos, con tasas de reconocimiento de apenas el 3.3% y el 6.7%, respectivamente. Esto se traduce en que el 73.3% de los usuarios encuestados posee un arsenal de conocimientos bajo o nulo para identificar un ciberataque en curso.

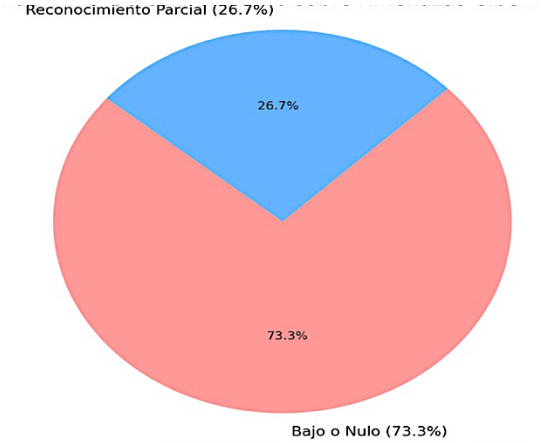


Figura 3. Distribución porcentual del nivel de conocimiento sobre ciberamenazas de los usuarios encuestados. Se destaca que casi tres cuartas partes de la muestra posee una preparación baja o nula para identificar riesgos comunes.

3.2.3. Comportamientos y Percepciones en la Práctica

Se encontró una fuerte correlación entre la falta de conocimiento y la prevalencia de conductas de riesgo. El 60.0% de los encuestados reportó conectarse a redes públicas sin aplicar ningún criterio de verificación de seguridad. Las notas de observación cualitativa añaden textura a este dato: "Se observó a un usuario joven intentar conectarse a tres redes distintas desde su laptop. Al preguntarle (una vez terminada la encuesta) su criterio de elección respondió: 'a la que conecte más rápido'. No había reparado en los nombres o en si tenían candado de seguridad". Esta conducta evidencia una priorización absoluta de la conveniencia sobre la seguridad. Consistentemente, el 50.0% de los usuarios manifestó sentirse "seguro" o "muy seguro", una percepción que choca frontalmente con la realidad técnica del entorno.

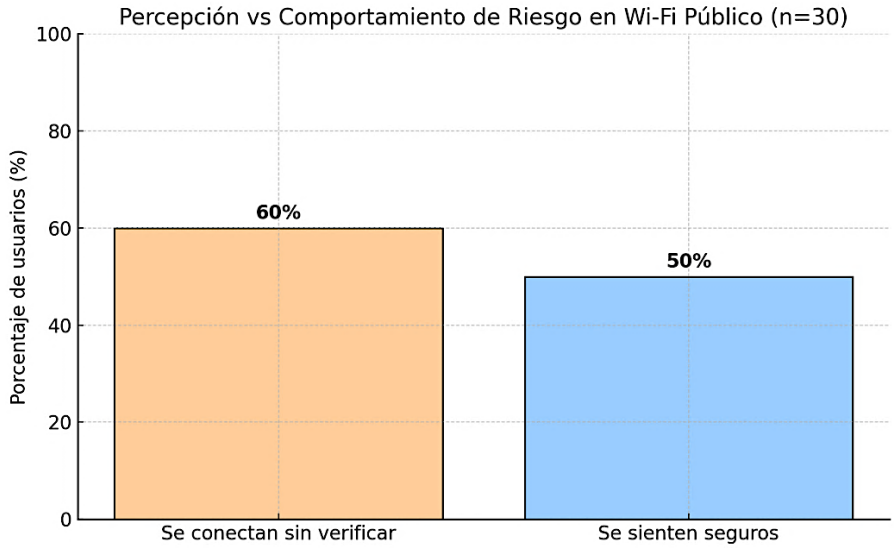


Figura 4. Comparativa entre el porcentaje de usuarios que reportan conductas de riesgo frecuentes y aquellos que manifiestan una alta percepción de seguridad. La escasa diferencia entre ambas métricas ilustra la disonancia cognitiva y la baja percepción de vulnerabilidad en la muestra estudiada.

3.2.4. Análisis Correlacional

Para explorar la relación entre las variables, se realizó una prueba de correlación de Spearman. Se encontró una correlación negativa, moderada y estadísticamente significativa entre el nivel de conocimiento sobre amenazas y la frecuencia de comportamientos de riesgo ($\rho = -0.58$, $p < 0.05$). Este resultado cuantitativo es clave, pues sugiere que a medida que aumenta el conocimiento de un individuo sobre ciberseguridad, disminuye la probabilidad de que incurra en prácticas inseguras.

3.3. La Anatomía de un Ecosistema de Riesgo: Interpretación de los Hallazgos

Los resultados no solo confirman la hipótesis inicial de riesgo, sino que permiten diseccionar su anatomía. No estamos ante un fallo aislado, sino ante un fallo sistémico en el ecosistema sociotécnico del patio de comidas. La "tormenta perfecta" previamente mencionada se nutre de una peligrosa sinergia: la negligencia en la gestión de la infraestructura por parte de los proveedores de servicio y la apatía o ignorancia informada por parte de los consumidores de dicho servicio. La infraestructura es el "qué" del riesgo (redes abiertas, protocolos obsoletos), pero el comportamiento humano es el "cómo" se materializa ese riesgo.

3.4. El Factor Humano: Epicentro de la Vulnerabilidad

El hallazgo más crítico es la correlación estadísticamente significativa ($\rho = -0.58$) entre la falta de conocimiento y el comportamiento de riesgo. Este dato es desesperanzador y esperanzador a la vez. Desesperanzador porque demuestra que la mayoría de los usuarios opera en un estado de vulnerabilidad activa. Sin embargo, es esperanzador porque sugiere que la educación y la concientización no son esfuerzos fútiles. Si la falta de conocimiento predice el riesgo, entonces la entrega efectiva de conocimiento puede ser un potente antídoto.

La disonancia cognitiva (sentirse seguro en un entorno inseguro) puede explicarse por la teoría de los sesgos cognitivos (Arce & Krombholz, 2022). Los usuarios no son irracionales; simplemente aplican heurísticas o "atajos mentales" en un entorno de sobrecarga de información. El cerebro optimiza para la tarea inmediata ("conectarme para revisar Instagram") y descarta amenazas abstractas y no visibles ("un posible ataque MitM").

3.5. Implicaciones Prácticas: De lo Abstracto a la Consecuencia Real

Las implicaciones de este estudio van más allá de un simple diagnóstico. Para un usuario, un ataque exitoso en este entorno no es una abstracción, es la posibilidad real del vaciado de una cuenta bancaria tras realizar una compra en línea, o el secuestro de su cuenta de WhatsApp para estafar a sus contactos. Para el dueño de un restaurante local que ofrece "Wi-Fi gratis" con la configuración de fábrica de su router, la implicación es una posible responsabilidad legal o un daño irreparable a su reputación si su red es el origen de un ataque. Para la administración del centro comercial, el riesgo es la erosión de su marca como un espacio seguro y familiar. Teóricamente, este estudio valida los modelos de riesgo sociotécnico en un contexto latinoamericano poco estudiado (Rojas, A. M., 2024), demostrando su aplicabilidad fuera de los entornos corporativos o de las grandes metrópolis del Norte Global.

3.6. Limitaciones y Fortalezas del Estudio

Es imperativo reconocer las limitaciones. La principal es la validez externa, restringida por el tamaño y naturaleza no probabilística de la muestra. Los hallazgos son una profunda radiografía del "caso Paseo Shopping Riobamba", pero no pueden ser extrapolados a otros contextos sin una debida cautela. Una segunda limitación es la profundidad del análisis técnico; al ser un análisis pasivo, no se detectaron vulnerabilidades que requerirían una interacción activa (como un test de penetración).

No obstante, la fortaleza del estudio radica en su enfoque de métodos mixtos y su validez ecológica. La combinación de datos de red, encuestas y observación directa permitió una triangulación que otorga una visión robusta y matizada del fenómeno en su ambiente natural, algo que un estudio de laboratorio no podría lograr.

3.7. Recomendaciones Detalladas y Futuras Líneas de Investigación

Las recomendaciones deben ser pragmáticas y dirigidas:

Plan de Acción para la Administración del Mall (Enfoque Top-Down):

• Fase 1 - Auditoría (Corto Plazo): Contratar una auditoría de seguridad externa para todas las redes del centro comercial.

• Fase 2 - Centralización (Mediano Plazo): Implementar una única red Wi-Fi para visitantes, gestionada centralmente, con seguridad WPA3 y un portal cautivo que incluya una advertencia clara sobre los riesgos y una casilla de aceptación de términos.

• Fase 3 - Educación Continua (Largo Plazo): Exigir a los nuevos arrendatarios cumplir con un estándar mínimo de seguridad en sus redes y ofrecer talleres de ciber-higiene para empleados.

Plan de Acción para Usuarios (Enfoque Bottom-Up):

• Campaña "Piensa Antes de Conectar": Crear infografías simples para las mesas con tres reglas de oro: 1. Verifica: Lee el nombre de la red. ¿Parece oficial? 2. Desconfía: Si es abierta, no ingreses contraseñas ni datos bancarios. 3. Protege: Usa una VPN siempre que sea posible.

Como líneas futuras de investigación, se sugiere un estudio comparativo entre diferentes centros comerciales en Ecuador para identificar patrones nacionales. Asimismo, un estudio experimental podría medir la efectividad de la campaña de concientización propuesta, comparando los comportamientos de los usuarios antes y después de su implementación.

4. Conclusiones

A partir del análisis exhaustivo y la discusión de los datos recolectados en el estudio de caso del patio de comidas del Paseo Shopping de Riobamba, esta investigación llega a las siguientes conclusiones fundamentales, que en conjunto responden a la pregunta de investigación y objetivos planteados:

Se confirma la existencia de un riesgo cibernético elevado y sistémico, producto de la convergencia crítica entre vulnerabilidades técnicas y humanas. La conclusión principal e irrefutable es que el entorno estudiado no es seguro. El riesgo no se deriva de un único factor, sino de una sinergia peligrosa entre una infraestructura de red gestionada de forma deficiente y una base de usuarios con una preparación en ciberseguridad marcadamente insuficiente. Este ecosistema representa una "tormenta perfecta" donde la probabilidad de que un ciberataque sea exitoso es significativamente alta.

La infraestructura de red inalámbrica refleja un estado de obsolescencia y negligencia en seguridad. El hallazgo de que dos tercios (66.7%) de las redes operan

con protocolos nulos, débiles u obsoletos (Abierta, WEP, WPA) es un indicador claro de una gestión de TI reactiva en lugar de proactiva. La ausencia total del estándar moderno WPA3 y la presencia de una red sospechosa de ser un "Evil Twin" no son meros datos técnicos; son la evidencia tangible de una falta de inversión y conciencia sobre la seguridad por parte de los proveedores del servicio, creando un campo fértil para la actividad maliciosa.

El perfil del usuario promedio se caracteriza por una triple deficiencia: analfabetismo funcional en ciberseguridad, normalización de conductas de riesgo y una peligrosa disonancia cognitiva. Se concluye que el eslabón humano es el componente más crítico del riesgo. Los usuarios no solo desconocen las amenazas específicas (73.3% con conocimiento bajo o nulo), sino que han normalizado comportamientos inseguros (60% se conecta sin verificar) por priorizar la conveniencia. La conclusión más alarmante es su percepción de seguridad desalineada con la realidad (50% se siente seguro), lo que anula la autoprotección y los convierte en cómplices involuntarios de su propia vulnerabilidad.

La educación en ciberseguridad emerge como la intervención más directa y con mayor potencial de impacto para la mitigación del riesgo. La correlación negativa y estadísticamente significativa ($\rho = -0.58$, $p < 0.05$) entre el nivel de conocimiento y la frecuencia de comportamientos de riesgo es el hallazgo más accionable del estudio. Esta evidencia empírica permite concluir que la educación no es un esfuerzo abstracto; es una intervención con un potencial medible para reducir el riesgo. Aumentar la conciencia y el conocimiento de los usuarios sobre las amenazas y las buenas prácticas es, por lo tanto, la estrategia de defensa más eficaz y rentable a corto y mediano plazo.

Este estudio proporciona un modelo empírico y contextualizado del riesgo cibernético en espacios públicos de ciudades intermedias, llenando un vacío en la literatura regional. Más allá del diagnóstico local, la principal contribución académica de este trabajo es la validación de un modelo de riesgo sociotécnico en un entorno poco estudiado como lo es una ciudad andina no metropolitana. Se concluye que los desafíos de ciberseguridad en estos contextos son igualmente severos que, en las grandes capitales, pero requieren soluciones adaptadas a su escala y particularidades socioeconómicas.

En última instancia, este artículo concluye que, en la era de la digitalización ubicua, la seguridad ya no puede ser una ocurrencia tardía. La brecha entre el rápido avance de la conectividad y la lenta maduración de la cultura de seguridad debe ser cerrada con urgencia. Fomentar una ciudadanía digital responsable es una tarea compartida entre administradores de infraestructura, proveedores de servicios y, fundamentalmente, los propios usuarios, a través de una educación continua y accesible.

Referencias

Alshammari, M., & Ivanov, A. (2023). User behavior, security fatigue, and risk perception in public Wi-Fi usage. Journal of Cybersecurity Research, 8(2), 45-62.

Arce, I., & Krombholz, K. (2022). The role of cognitive biases in cybersecurity behavior: A systematic review. ACM Computing Surveys, 55(3), 1-36. https://doi.org/10.1145/3512878/

BID (Banco Interamericano de Desarrollo). (2024). Reporte de Ciberseguridad 2024: Riesgos y capacidades en América Latina y el Caribe. Publicaciones del BID.

Creswell, J. W., & Creswell, J. D. (2018). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage publications.

García, F., & Torres, L. (2022). La sociedad conectada: Transformaciones digitales y vida cotidiana en América Latina. Editorial FLACSO.

Hadnagy, C. (2018). Social Engineering: The art of human hacking. John Wiley & Sons.

Kurose, J. F., & Ross, K. W. (2021). Computer networking: A top-down approach (8th ed.). Pearson.

Lau, F., & Zhou, Y. (2020). On the prevalence and detection of Evil Twin attacks in public Wi-Fi networks. Journal of Network and Computer Applications, 158, 102589. https://doi.org/10.1016/j.jnca.2020.102589/

Mendoza, C. A. (2022). Responsabilidad legal de los establecimientos comerciales ante incidentes de ciberseguridad en redes de invitados en Ecuador. Editorial Jurídica Andina.

Oghuma, A. S., & Schroeder, D. (2022). Usability challenges of mobile VPNs: Why security tools go unused. Journal of Usable Security, 7(1), 1-15.

Ribble, M. (2021). Digital citizenship for schools: A practical guide for leaders. International Society for Technology in Education (ISTE).

Rojas, A. M. (2024). Ciberseguridad y desarrollo en la región andina: Retos para las ciudades intermedias. Ediciones CIESPAL.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124-1131.

Weber, R. H. (2023). The security implications of public IoT ecosystems. IEEE Security & Privacy, 21(4), 55-62. https://doi.org/10.1109/MSEC.2023.3278451/

Yin, R. K. (2018). Case study research and applications: Design and methods (6th ed.). Sage publications.