CIUDAD GLOCAL

v.1, n.2, 2025

Acceptance date: 14/07/2025

https://doi.org/10.65937/ciudadglocal.2025.12.v1.n2

Wi-Fi público en el tejido urbano: Revisión de riesgos de seguridad, percepción de usuarios y estrategias de protección

Public Wi-Fi in the Urban Fabric: Review of Security Risks, User Perception and Protection Strategies

José de Jesús Franco Romero
Estudiante de la Maestría en Ciencia de la Ciudad del Centro Universitario de Tonalá (CUTONALÁ). Universidad de Guadalajara. Correo electrónico: jose.franco1908@alumnos.udg.mx ORCID id: https://orcid.org/0009-0005-5192-5921

Diego Nápoles Franco
Profesor Investigador del Centro Universitario de Ciencias Sociales y Humanidades (CUCSH). Universidad de Guadalajara. Correo electrónico: diego.napoles@academicos.udg.mx ORCID id: https://orcid.org/0000-0002-8637-1325

Aarón Jiménez Govea
Profesor Investigador del Centro Universitario de Tonalá (CUTONALÁ). Universidad de Guadalajara. Correo electrónico: aaron.jimenez@academicos.udg.mx ORCID id: https://orcid.org/0009-0008-1429-1925

Resumen

Este artículo presenta una revisión bibliográfica sobre las redes Wi-Fi públicas como componente integral del tejido urbano y del territorio digital contemporáneo. Se analizan los riesgos de seguridad documentados, el comportamiento de los usuarios frente a estos riesgos, y las estrategias de protección disponibles. La evidencia revisada indica que, a pesar del conocimiento creciente sobre vulnerabilidades, muchos usuarios

continúan utilizando redes Wi-Fi públicas no seguras principalmente debido a la conservación de datos móviles y factores situacionales. Estudios experimentales en diversos contextos urbanos revelan la transmisión de información sensible sin cifrado adecuado, desde credenciales de inicio de sesión hasta datos personales identificables. La literatura también documenta cómo factores demográficos, ambientales y cognitivos influyen en las decisiones de los usuarios, destacando la "heurística de preservación de recursos". Se subraya además la relación del Wi-Fi público con la movilidad urbana y la configuración del territorio digital, mostrando cómo la disponibilidad y seguridad de estas redes impactan la accesibilidad, interacción y equidad en el espacio urbano. Las conclusiones apuntan hacia estrategias multidisciplinarias que combinan soluciones técnicas, educación dirigida y políticas públicas, promoviendo ciudades conectadas de manera segura y equitativa.

Palabras clave: Wi-Fi público, Seguridad cibernética, Tejido urbano, Comportamiento de usuarios, Heurística de preservación de recursos, Infraestructura digital, Movilidad digital, Territorio urbano

Abstract

This article presents a literature review on public Wi-Fi networks as an integral component of the urban fabric and contemporary digital territory. It analyzes documented security risks, user behavior towards these risks, and available protection strategies. The reviewed evidence indicates that, despite growing knowledge about vulnerabilities, many users continue using unsecured public Wi-Fi networks primarily due to mobile data conservation and situational factors. Experimental studies in diverse urban contexts reveal the transmission of sensitive information without adequate encryption, from login credentials to personally identifiable data. The literature also documents how demographic, environmental, and cognitive factors influence user decisions, highlighting the "resource preservation heuristic." Furthermore, the relationship between public Wi-Fi and urban mobility and digital territory configuration is emphasized, showing how the availability and security of these networks impact accessibility, interaction, and equity in urban space. The conclusions point toward multidisciplinary strategies that combine technical solutions, targeted education, and public policies, promoting cities that are connected in a safe and equitable manner.

Keywords: *Public Wi-Fi, Cybersecurity, Urban fabric, User behavior, Resource preservation heuristic, Digital infrastructure, Digital mobility, Urban territory.*

Introducción

Las redes Wi-Fi públicas se han convertido en un componente fundamental de la infraestructura urbana moderna, transformando los espacios públicos y la forma en que los ciudadanos interactúan con su entorno urbano. En la

actualidad, la conectividad inalámbrica se considera un servicio esencial que facilita la movilidad, productividad y acceso a información, contribuyendo significativamente al concepto de ciudades inteligentes (McShane et al., 2016). Sin embargo, el concepto de brecha digital urbana trasciende la tradicional dicotomía rural-urbana, manifestándose de manera compleja en el tejido urbano contemporáneo. Como establece UN-Habitat (2021), "la brecha digital persiste dentro de ciudades bien conectadas, megaciudades y centros regionales", donde globalmente el 28% de los hogares urbanos carecen de conectividad a internet. En América Latina, esta realidad se agrava por las inequidades socioeconómicas: CEPAL (2022) documenta brechas de conectividad de más de 50 puntos porcentuales entre hogares de mayores y menores ingresos, convirtiendo al Wi-Fi público en una alternativa esencial para el acceso digital en contextos vulnerables.

Sin embargo, la accesibilidad y conveniencia que hacen tan populares a las redes Wi-Fi públicas también las vuelven vulnerables a actividades maliciosas, especialmente aquellas dirigidas a interceptar información personal valiosa. Esta paradoja representa un desafío significativo para la planificación urbana moderna: cómo proporcionar conectividad amplia y accesible sin comprometer la seguridad y privacidad de los ciudadanos.

Este artículo busca sintetizar la literatura existente sobre tres aspectos fundamentales de las redes Wi-Fi públicas en entornos urbanos: los riesgos de seguridad documentados, los factores que influyen en el comportamiento de los usuarios frente a estos riesgos, y las estrategias de protección disponibles. La revisión pretende ofrecer una perspectiva integral que sirva tanto a investigadores como a planificadores urbanos, proveedores de servicios y usuarios finales.

Metodología

Esta revisión bibliográfica narrativa se basa en una selección sistemática de 27 estudios académicos publicados entre 2004 y 2023 que abordan aspectos de seguridad, comportamiento de usuarios y estrategias de protección relacionadas con redes Wi-Fi públicas en contextos urbanos, también se revisaron 2 documentos institucionales. La muestra analizada incluye 13 estudios empíricos con datos primarios (48%), 12 estudios conceptuales y teóricos (44%), y 2 fuentes institucionales especializadas (8%). Las fuentes incluyen artículos de revistas académicas, actas de conferencias y reportes técnicos obtenidos de bases de datos como IEEE Xplore, ACM Digital Library, ScienceDirect y Google Scholar.

Esta revisión narrativa busca síntesis interpretativa de literatura multidisciplinar que integra dimensiones técnicas, sociales y territoriales del Wi-Fi público urbano, superando aproximaciones fragmentadas que analizan estos aspectos de manera separada. La revisión revela un vacío significativo de estudios empíricos en contextos latinoamericanos, lo que justifica la necesidad de investigación

contextualizada en la región y valida la pertinencia de enfoques transdisciplinarios para comprender la apropiación social de infraestructuras digitales urbanas.

Criterios de selección

Los criterios de inclusión se centraron en estudios que: (1) examinaran aspectos técnicos de seguridad en redes Wi-Fi públicas; (2) analizaran comportamientos y percepciones de usuarios; (3) propusieran o evaluaran estrategias de protección; y (4) contextualizaran estos elementos en entornos urbanos. Se dio preferencia a estudios empíricos que incluyeran evidencia experimental, encuestas con usuarios reales, o análisis de infraestructura en funcionamiento.

Los criterios de exclusión abarcaron: (1) estudios puramente teóricos sin evidencia empírica o aplicación contextual; (2) investigaciones enfocadas exclusivamente en redes privadas o corporativas sin relevancia para espacios públicos; (3) artículos de divulgación sin metodología científica explícita; y (4) publicaciones duplicadas o versiones preliminares de trabajos ya incluidos.

La ausencia de estudios empíricos específicamente latinoamericanos en la literatura consultada se reconoce como una limitación inherente al estado actual del conocimiento, que simultáneamente justifica la relevancia de investigación futura en estos contextos.

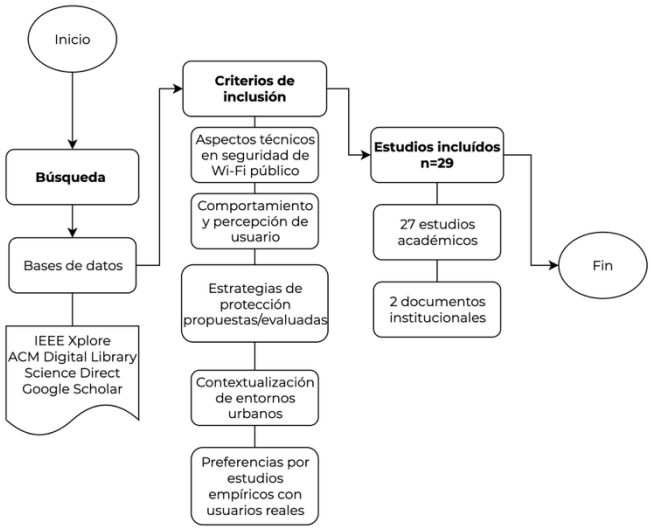

Figura 1.
Metodología del estudio.

Fuente: Elaboración propia.

Enfoque metodológico socio-tecnológico

El análisis integra perspectivas técnicas sobre vulnerabilidades de redes Wi-Fi con marcos de apropiación social de tecnologías urbanas. La síntesis busca articular tres dimensiones: vulnerabilidades manifiestas, distribución territorial, y factores socioculturales que condicionan prácticas ciudadanas (UN-Habitat, 2021). Este enfoque transdisciplinar permite comprender el Wi-Fi público como infraestructura socio-territorial donde convergen aspectos técnicos, comportamentales y urbanos.

Riesgos de seguridad en redes Wi-Fi públicas: Evidencia empírica

Vulnerabilidades técnicas documentadas

La literatura revisada identifica consistentemente vulnerabilidades técnicas significativas en redes Wi-Fi públicas, particularmente en redes abiertas que no requieren autenticación ni proporcionan cifrado. Estas vulnerabilidades permiten diversos tipos de ataques, incluyendo intercepción de datos, ataques de intermediario (man-in-the-middle) y creación de puntos de acceso maliciosos (rogue access points) (Cheng et al., 2013; Szongott et al., 2015). La naturaleza abierta de estas redes, combinada con la transmisión inalámbrica de datos, crea un entorno donde las comunicaciones pueden ser fácilmente interceptadas por actores maliciosos.

Puntos de acceso gemelos maliciosos (Evil Twin)

Szongott et al. (2015) analizan el problema de los puntos de acceso gemelos maliciosos (Evil Twin Access Points), presentando un sistema de reconocimiento basado en contexto que puede desplegarse de manera autónoma y no requiere cambios en la infraestructura. Esta contribución es particularmente relevante para la detección y mitigación de este tipo de amenazas en entornos urbanos. Los Evil Twin son puntos de acceso fraudulentos que imitan a redes Wi-Fi legítimas, engañando a los usuarios para que se conecten a ellos. Una vez conectados, los atacantes pueden interceptar todo el tráfico de red no cifrado, incluyendo potencialmente credenciales de inicio de sesión y datos personales.

Kern (2004) examina las implicaciones legales de la utilización no autorizada de redes Wi-Fi, incluyendo aspectos relacionados con la creación de puntos de acceso falsos y las prácticas conocidas como "war-driving" (búsqueda sistemática de redes Wi-Fi vulnerables). Su análisis destaca cómo la mayoría de las regulaciones existentes no estaban originalmente diseñadas para abordar las complejidades del acceso inalámbrico, creando vacíos legales que pueden ser explotados.

Vulnerabilidades en infraestructura y protocolos

Szewczyk y Macdonald (2017) proporcionan un análisis histórico de la seguridad de los enrutadores de banda ancha, señalando que a pesar de la importancia de estos dispositivos en la seguridad de la red, las consideraciones de seguridad nunca han sido prioritarias en su desarrollo. Su investigación revela que los consumidores a menudo poseen enrutadores con múltiples características orientadas al usuario final, pero plagados de vulnerabilidades que los hacen susceptibles a la explotación. Los autores identifican la configuración predeterminada deficiente, el firmware desactualizado y las interfaces de administración inseguras como problemas comunes que afectan a los enrutadores utilizados en redes públicas.

La seguridad de los protocolos de red también representa un punto crítico de vulnerabilidad. Bonné et al. (2017) descubrieron que un tercio de las redes Wi-Fi a las que se conectan los participantes de su estudio no tienen

ninguna seguridad habilitada, exponiendo a los usuarios a diversos tipos de ataques. Su investigación también reveló que muchos usuarios no son conscientes de las conexiones que sus aplicaciones establecen a través de estas redes inseguras, incrementando el riesgo de filtración de datos.

Problemas en los portales cautivos

Ali et al. (2019) abordan específicamente las vulnerabilidades asociadas con los portales cautivos (captive portals) utilizados en muchas redes Wi-Fi públicas. Estos portales, diseñados para autenticar usuarios y controlar el acceso a la red, a menudo recopilan datos personales y pueden incorporar mecanismos de seguimiento. Su análisis de 67 puntos de acceso Wi-Fi públicos en Montreal, Canadá, reveló que muchos de estos portales recopilaban cantidades significativas de información personal sensible a través de formularios de registro y opciones de inicio de sesión social. Más preocupante aún, los autores identificaron actividades de seguimiento que a veces comenzaban incluso antes de que el usuario aceptara las políticas de privacidad y términos de servicio.

El estudio demuestra que estos portales representan un significativo riesgo de privacidad, tanto por la cantidad de datos recolectados como por las prácticas potencialmente engañosas empleadas durante el proceso de registro. Los riesgos son particularmente elevados porque estos portales a menudo representan un punto de entrada obligatorio para los usuarios que desean acceder a la red, creando así una situación donde se ven forzados a comprometer su privacidad para obtener conectividad. Además, la investigación reveló que muchos usuarios no comprenden completamente el alcance de la información que están proporcionando ni cómo podría ser utilizada, lo que los expone a riesgos adicionales de identificación y seguimiento.

Vulnerabilidades en configuraciones personales

Zhang et al. (2017) analizan los comportamientos de seguridad de la información de los usuarios de smartphones en China, encontrando preocupaciones serias sobre la seguridad en el uso de estos dispositivos. Su estudio identifica que muchos usuarios ignoran la información de seguridad al descargar y usar aplicaciones, habilitando inadecuadamente utilidades adicionales como el compartir archivos o la visibilidad de redes cuando se conectan a Wi-Fi público. Estas configuraciones erróneas de los dispositivos agravan las vulnerabilidades inherentes a las redes Wi-Fi públicas, creando puntos adicionales de exposición.

Ndibwile et al. (2019) señalan que los usuarios en diferentes contextos geográficos y económicos muestran comportamientos variables respecto a las actualizaciones de seguridad de sus dispositivos. Por ejemplo, en Tanzania, donde el costo relativo de los datos móviles es alto, los usuarios tienden a posponer las actualizaciones de seguridad para conservar datos, aumentando así su vulnerabilidad

cuando utilizan redes Wi-Fi públicas. Este comportamiento ilustra cómo los factores económicos pueden amplificar los riesgos técnicos inherentes a estas redes.

La **Tabla 1** sintetiza las principales vulnerabilidades técnicas identificadas en la literatura revisada, organizadas según su naturaleza, riesgo asociado y contexto de exposición en entornos urbanos

Tabla 1.
Vulnerabilidades técnicas documentadas en redes Wi-Fi públicas.

Tipo de Vulnerabilidad	Descripción Técnica	Riesgo Principal	Contexto de Exposición
Evil Twin Access Points	Puntos de acceso fraudulentos que imitan redes Wi-Fi legítimas mediante la duplicación de nombres de red (SSID)	Interceptación de todo el tráfico no cifrado, con credenciales y datos personales	Espacios públicos urbanos con alta densidad de redes Wi-Fi
Redes abiertas sin cifrado	Redes que no requieren autenticación ni proporcionan cifrado de datos	Intercepción pasiva de comunicaciones y ataques man-in-the-middle	33% de las redes utilizadas por usuarios según estudios empíricos
Vulnerabilidades en enrutadores	Configuraciones predeterminadas deficientes, firmware desactualizado e interfaces de administración inseguras	Compromiso de toda la infraestructura de red y acceso no autorizado a configuraciones	Enrutadores de banda ancha utilizados en establecimientos públicos
Portales cautivos maliciosos	Sistemas de autenticación que recopilan datos personales excesivos y emplean mecanismos de seguimiento	Violación de privacidad y recolección no autorizada de información personal sensible	67 puntos de acceso analizados en Montreal, Canadá
Configuraciones erróneas de dispositivos	Habilitación inadecuada de compartir archivos, visibilidad de redes y posponer actualizaciones de seguridad	Exposición adicional de datos personales y vulnerabilidades no parcheadas	Usuarios de smartphones en contextos con datos móviles costosos
Vacíos legales regulatorios	Ausencia de marcos legales específicos para abordar el acceso inalámbrico no autorizado	Impunidad para actividades maliciosas como war-driving y creación de redes falsas	Jurisdicciones con regulaciones desactualizadas sobre tecnologías inalámbricas

Fuente: Elaboración propia a partir de Szongott et al. (2015); Cheng et al. (2013); Bonné et al. (2017); Szewczyk y Macdonald (2017); Ali et al. (2019); Zhang et al. (2017); Ndibwile et al. (2019) y Kern (2004).

Como se observa en la síntesis anterior, las vulnerabilidades documentadas abarcan desde aspectos técnicos de infraestructura hasta comportamientos de usuarios, evidenciando la naturaleza multidimensional de los riesgos en redes Wi-Fi públicas.

Evolución de las amenazas

Sangeen et al. (2023) han documentado una evolución preocupante en la sofisticación de los ataques dirigidos a usuarios de redes Wi-Fi públicas. Su

investigación destaca que, a pesar de las mejoras en algunas áreas de la seguridad de redes, los atacantes han desarrollado técnicas más avanzadas para comprometer las comunicaciones. Esto incluye ataques que pueden eludir algunas medidas de seguridad comunes y técnicas de ingeniería social diseñadas específicamente para el contexto de Wi-Fi público. Los autores enfatizan la necesidad de aumentar la conciencia sobre estos peligros, ya que muchos usuarios siguen sin comprender plenamente las implicaciones de seguridad de utilizar redes no seguras.

Lugovic et al. (2019) analizaron las prácticas de protocolo de seguridad de redes Wi-Fi en destinos turísticos, encontrando significativas variaciones en los estándares de seguridad implementados. Su estudio en la ciudad de Zadar, Croacia, reveló que muchos puntos de acceso en áreas turísticas priorizaban la facilidad de acceso sobre la seguridad, creando concentraciones de vulnerabilidades en zonas frecuentadas por visitantes temporales que podrían no estar familiarizados con los riesgos locales.

Esta diversidad de vulnerabilidades técnicas documentadas subraya la complejidad del panorama de amenazas asociado con las redes Wi-Fi públicas. Más allá de las vulnerabilidades inherentes a la tecnología en sí, factores como la configuración inadecuada, la falta de conciencia del usuario, y las variaciones en las prácticas de implementación contribuyen a crear un entorno donde los datos personales y la privacidad pueden estar significativamente comprometidos.

Comportamiento y percepción de los usuarios

Conciencia sobre riesgos

La literatura muestra una evolución en la conciencia de los usuarios sobre los riesgos de seguridad en redes Wi-Fi públicas. Swanson et al. (2010) observaron que los usuarios de Wi-Fi público participaban en una forma de "seguridad ingenua" y no creían que los riesgos se materializarían en su caso, a pesar de ser conscientes de ellos de manera abstracta.

La investigación de Maimon et al. (2020) encontró que personas con mayor conciencia situacional (atención a su entorno) tenían menor probabilidad de acceder a redes maliciosas y mayor tendencia a adoptar comportamientos de autoprotección. Sin embargo, la conciencia situacional no eliminaba completamente los comportamientos riesgosos.

Estudios más recientes como el de Sangeen et al. (2023) han enfatizado la necesidad de aumentar la conciencia sobre los peligros de usar redes Wi-Fi públicas no seguras, destacando que muchos usuarios siguen sin comprender plenamente las implicaciones de seguridad.

Factores que influyen en la decisión de uso

Heurística de preservación de recursos

Un hallazgo potencial en múltiples estudios es el papel de la "heurística de

preservación de recursos" - el deseo de conservar datos móviles - como un factor determinante en la decisión de utilizar redes Wi-Fi públicas no seguras.

Sombatruang et al. (2016, 2019) introdujeron y expandieron este concepto, demostrando que la restricción de datos móviles instigaba una actitud de toma de riesgos, llevando a decisiones de utilizar Wi-Fi público potencialmente no seguro. Esta heurística era particularmente pronunciada cuando los usuarios llegaban aproximadamente al 30% de su asignación de datos mensuales.

Esta heurística de preservación de recursos adquiere particular relevancia en el contexto latinoamericano, donde CEPAL (2022) identifica disparidades significativas en conectividad que constituyen factores de exclusión social. En algunos países de la región, las diferencias en acceso a internet entre hogares de distintos niveles de ingresos pueden superar los 50 puntos porcentuales, configurando un escenario donde las redes Wi-Fi públicas emergen como infraestructuras críticas para el acceso digital de poblaciones con recursos limitados (UN-Habitat, 2021). Este contexto transforma el comportamiento de preservación de datos móviles de una simple preferencia económica a una estrategia de supervivencia digital urbana.

Sombatruang et al. (2016, 2019) descubrieron que el agotamiento de los datos móviles impulsaba significativamente a los participantes a usar redes Wi-Fi no seguras, especialmente cuando su asignación restante llegaba aproximadamente al 30%. El nivel de batería, sin embargo, no jugaba un papel significativo. Los riesgos percibidos del Wi-Fi no seguro tampoco afectaban la toma de decisiones.

Asimismo, estudios económicos y psicológicos más amplios sustentan esta idea. Lv et al. (2014) mostraron que la escasez dirige la atención limitada de una persona hacia los recursos escasos y descuida otras dimensiones, lo que puede llevar a comportamientos irracionales. De manera similar, Diekert y Brekke (2022) exploran cómo los grupos disciplinan el uso de recursos bajo escasez, ofreciendo perspectivas sobre comportamiento colectivo que podrían aplicarse a entornos de redes.

Además, varios estudios han identificado correlaciones entre factores demográficos y la probabilidad de utilizar redes Wi-Fi públicas no seguras. Sombatruang et al. (2018) encontraron que las participantes femeninas y aquellas con educación secundaria eran más propensas a usar Wi-Fi público.

Ndibwile et al. (2019) realizaron un estudio comparativo de la percepción y preferencia de seguridad de usuarios de smartphones en Japón y Tanzania, encontrando que la privacidad de datos es igualmente importante para la mayoría de los participantes (70%) en ambos países. Sin embargo, los participantes en Japón eran ligeramente más propensos a leer los términos y condiciones al conectarse al Wi-Fi público (36% frente al 27%).

También, Ferreira et al. (2014) presentaron un análisis socio-técnico de seguridad de los puntos de acceso Wi-Fi, destacando cómo elementos contextuales influyen en las decisiones de los usuarios y pueden comprometer la seguridad.

Bonné et al. (2017) evaluaron hasta qué punto la postura de privacidad de los usuarios de dispositivos móviles se corresponde con su comportamiento real, monitoreando las redes Wi-Fi a las que se conectaban los dispositivos de los participantes durante un período de 30 días. Descubrieron que, en general, los participantes desconocían una parte significativa de las conexiones realizadas por las aplicaciones en sus dispositivos, un problema que se agrava por el hecho de que un tercio de las redes Wi-Fi a las que se conectan los participantes no tienen ninguna seguridad habilitada.

Lugovic et al. (2019) investigaron las preferencias de seguridad actuales de las redes informáticas inalámbricas en destinos turísticos, específicamente en la ciudad de Zadar, Croacia, para llamar la atención sobre la conciencia de seguridad del Wi-Fi y exponer el comportamiento de seguridad a nivel del enrutador.

Estrategias de protección y mitigación

Soluciones técnicas

La literatura identifica varias soluciones técnicas para mitigar los riesgos de seguridad en redes Wi-Fi públicas:

Tabla 2.
Soluciones técnicas para mitigar riesgos de seguridad en redes Wi-Fi públicas.

Solución técnica	Descripción	Referencia
Redes Privadas Virtuales (VPN)	Crean un túnel cifrado para proteger el tráfico de datos en redes públicas, garantizando la confidencialidad de la comunicación.	McShane et al. (2016)
HTTPS y SSL/TLS	Protocolos de cifrado que aseguran la transferencia de datos; aplicados también al cifrado de video en tiempo real para multimedia.	Dilkash et al. (2018)
Configuración adecuada de dispositivos	La correcta configuración de enrutadores y dispositivos fortalece la seguridad, reduciendo vulnerabilidades a ataques externos.	Szewczyk & Macdonald (2017)

Nota: La tabla resume las principales soluciones técnicas identificadas en la literatura para fortalecer la seguridad en redes Wi-Fi públicas.

Fuente: Elaboración propia.

Concienciación y educación de usuarios

Varios estudios destacan la importancia de la educación y concienciación de los usuarios. Ndibwile et al. (2018) estudiaron las preferencias de los usuarios para diferentes notificaciones de seguridad rediseñadas para mejorar el cumplimiento de las actualizaciones. Su diseño de notificación novedoso que integraba actualizaciones de seguridad con otros servicios de información gratuitos parecía prometedor para aumentar la conciencia de seguridad y el cumplimiento de las actualizaciones.

En otro estudio, Ndibwile et al. (2018) exploraron los factores que influyen en las decisiones de seguridad de smartphones en países en desarrollo y desarrollados,

identificando diferencias significativas en las actitudes y comportamientos. Esto sugiere la necesidad de enfoques educativos adaptados a diferentes contextos culturales y económicos.

De Santo, A., & Gaspoz, C. (2015) investigaron la influencia de la alfabetización en riesgos de privacidad de los usuarios en la intención de instalar una aplicación móvil. Utilizando mínimos cuadrados parciales (PLS), encontraron que más que la alfabetización en riesgos de privacidad es la alfabetización en comportamiento de afrontamiento la que influye en la decisión del usuario de instalar una aplicación móvil.

Responsabilidad de proveedores y políticas

Varios estudios destacan el papel que pueden desempeñar los proveedores de redes y los reguladores como se aprecia en la tabla siguiente:

Tabla 3.
Rol de proveedores y reguladores en la seguridad de redes Wi-Fi públicas.

Aspecto identificado	Descripción
Cifrado implementado por proveedores	Los proveedores de servicios deben garantizar medidas de seguridad, incluyendo el cifrado adecuado, para proteger la privacidad de los usuarios.
Certificación y estándares	Se requieren marcos legales y normativos claros que regulen el uso de conexiones no cifradas en redes Wi-Fi públicas.
Responsabilidad de desarrolladores de apps	Los desarrolladores deben aplicar mejores prácticas de seguridad para evitar vulnerabilidades en el uso de aplicaciones móviles.
Rol de operadores de telecomunicaciones	Los operadores deben participar en la educación de usuarios para fomentar la atención a factores de seguridad al descargar aplicaciones.

Nota: La tabla sintetiza el papel de distintos actores —proveedores, reguladores, desarrolladores y operadores— en el fortalecimiento de la seguridad de redes Wi-Fi públicas.

Fuente: Elaboración propia a partir de Lotfy et al. (2021); Kern (2004); Zhang et al. (2017) y Rensburg et al. (2018).

Discusión e implicaciones para la planificación urbana

Equilibrio entre accesibilidad y seguridad

Un tema recurrente en la literatura es la tensión entre proporcionar acceso fácil y conveniente a Internet a través de Wi-Fi público y garantizar la seguridad de los usuarios. Este equilibrio es particularmente relevante para los planificadores urbanos que buscan mejorar la conectividad como parte de iniciativas de ciudades inteligentes.

La investigación sugiere que simplemente advertir a los usuarios que eviten el Wi-Fi público no es una estrategia efectiva. Maimon et al. (2020) encontraron que, aunque la mayoría de los usuarios de Wi-Fi evitan acceder a sitios bancarios usando redes Wi-Fi públicas establecidas, todavía usan estas redes para acceder a redes sociales, correo electrónico y otros sitios web que manejan información sensible.

En cambio, un enfoque más práctico implica la implementación de soluciones técnicas (como VPN y cifrado generalizado), combinadas con educación dirigida a los usuarios y

políticas que incentiven a los proveedores a mejorar la seguridad de sus redes.

La literatura revisada subraya la creciente importancia del Wi-Fi público como un componente de la infraestructura urbana moderna. McShane et al. (2016) destacan la práctica segura del Wi-Fi público, evaluando y gestionando los riesgos de seguridad de datos. Su informe resalta los desafíos compartidos para los usuarios de Wi-Fi público, empleadores, proveedores de redes Wi-Fi públicas y responsables políticos para promover la seguridad del Wi-Fi público, al tiempo que mantienen los beneficios de accesibilidad que ofrece esta tecnología de comunicación.

Estas observaciones, junto con la creciente inversión de gobiernos estatales y municipales en redes Wi-Fi públicas, indican que el Wi-Fi público está pasando de ser una comodidad a ser considerado un servicio esencial. Esto tiene implicaciones significativas para la planificación urbana, ya que la provisión de conectividad confiable y segura se convierte en un componente fundamental del diseño urbano.

La evidencia de que usuarios con planes de datos móviles más pequeños son más propensos a utilizar Wi-Fi público no seguro plantea importantes consideraciones de equidad. Las consideraciones de equidad se intensifican cuando se analiza el contexto regional. UN-Habitat (2021) enfatiza que la evaluación de la brecha digital requiere una comprensión tridimensional que incorpore: conectividad (acceso a infraestructura utilizable), alfabetización digital (capacidad de usar tecnologías para comunicar información), y acceso a dispositivos (acceso sostenible y asequible). En el contexto del Wi-Fi público urbano, estas dimensiones adquieren características particulares donde la infraestructura pública compensa parcialmente las limitaciones socioeconómicas de acceso individual.

Además, el fortalecimiento de la ciberseguridad se ha convertido en un elemento central de la política digital en América Latina (CEPAL, 2022), donde solo 13 de los 33 países de la región contaban con una estrategia de ciberseguridad en 2020. Esta situación evidencia que la construcción social del riesgo cibernético en espacios públicos constituye una dimensión fundamental para comprender las prácticas ciudadanas de conectividad, especialmente entre poblaciones que dependen críticamente de infraestructuras digitales públicas para su inclusión digital. Los hallazgos de Sombatruang et al. (2019) sobre la influencia de los factores que impulsan a los usuarios a usar Wi-Fi no seguro sugieren que las personas con recursos limitados pueden estar más expuestas a riesgos de seguridad cibernética.

Soon et al. (2024) examinan el gasto en alimentos de los deciles más pobres, destacando la vulnerabilidad esperada y la indulgencia contraintuitiva. Aunque este estudio no se centra directamente en el Wi-Fi, ofrece perspectivas sobre cómo la escasez económica influye en las decisiones de gasto, potencialmente aplicables a las decisiones relacionadas con el uso de datos móviles versus Wi-Fi público.

Folta et al. (2022) investigan la elección de alimentos con escasez económica y abundancia de tiempo, encontrando que las personas con ingresos muy limitados, pero con relativa abundancia de tiempo pueden experimentar una condición de "preescasez", con un hiperfoco en un recurso escaso que podría llevar a un efecto túnel a medida que aumentan las restricciones. Este marco podría aplicarse al contexto del Wi-Fi público, donde los usuarios con recursos financieros limitados podrían centrarse intensamente en conservar datos, incluso a costa de la seguridad.

Esto subraya la importancia de considerar el acceso seguro a Internet como un problema de equidad en la planificación urbana. Las políticas que solo se centran en advertir sobre los riesgos sin proporcionar alternativas asequibles podrían inadvertidamente perjudicar a los grupos más vulnerables.

Vinculación con problemáticas urbanas locales y derecho a la ciudad

Los hallazgos sobre vulnerabilidades y comportamientos de usuarios de Wi-Fi público se vinculan directamente con problemáticas urbanas contemporáneas en ciudades mexicanas y latinoamericanas. La falta de seguridad en redes públicas puede generar inequidades en el acceso a información y servicios digitales, afectando especialmente a ciudadanos con recursos limitados. Esto tiene implicaciones sobre el derecho a la ciudad, ya que el acceso a espacios públicos conectados se convierte en un elemento central de la participación social, el disfrute del espacio urbano y la inclusión digital.

El análisis muestra que las decisiones de los usuarios, impulsadas por la heurística de preservación de recursos, reflejan desigualdades en el acceso a datos móviles y a conectividad segura. En este sentido, garantizar un Wi-Fi público seguro no es solo un problema tecnológico, sino también un componente de equidad urbana, al facilitar que todos los ciudadanos puedan ejercer su derecho a informarse, comunicarse y moverse en la ciudad de manera digital.

Esta problemática adquiere características particulares en el contexto latinoamericano, donde las condiciones socioeconómicas y la dinámica urbana generan patrones específicos de exposición a riesgos de seguridad en redes Wi-Fi públicas. Si bien la literatura revisada proporciona evidencia robusta sobre vulnerabilidades técnicas y comportamientos de usuarios en contextos internacionales, es importante contextualizar estos hallazgos en América Latina, y particularmente en México, donde la dinámica urbana y socioeconómica genera condiciones particulares de exposición a estos riesgos.

Aunque no existen estudios académicos sistemáticos que documenten vulnerabilidades de Wi-Fi público en contextos urbanos latinoamericanos, reportes periodísticos y comunicados de empresas de ciberseguridad sugieren la presencia de patrones similares a los documentados

en la literatura internacional. El Sol de México (2024) reporta la identificación de puntos de acceso fraudulentos (Evil Twin) en espacios concurridos de la Ciudad de México como el Metro, plazas comerciales y zonas turísticas. Por su parte, una encuesta de Kaspersky (2023) indica que el 18% de los usuarios latinoamericanos se conecta a redes Wi-Fi públicas sin verificar su seguridad, sugiriendo comportamientos de riesgo consistentes con la heurística de preservación de recursos documentada en contextos asiáticos (Sombatruang et al., 2019). Estos indicios preliminares, aunque provenientes de fuentes no académicas, refuerzan la necesidad de investigación empírica rigurosa que caracterice sistemáticamente las vulnerabilidades técnicas, los comportamientos ciudadanos y los factores socioculturales específicos que condicionan el uso de Wi-Fi público en ciudades latinoamericanas como Guadalajara.

Estos portales reflejan un riesgo significativo de violación de privacidad que se agrava cuando los usuarios aceptan condiciones sin leerlas, replicando patrones observados en estudios internacionales (Ali et al., 2019).

En cuanto a la equidad de acceso y comportamiento de usuarios, se observa que en ciudades latinoamericanas los factores socioeconómicos juegan un papel determinante. Usuarios con planes de datos móviles limitados son más propensos a conectarse a Wi-Fi público inseguro, replicando la heurística de preservación de recursos identificada en estudios internacionales (Sombatruang et al., 2019). Esto evidencia la necesidad de políticas locales que integren medidas de seguridad con accesibilidad económica, evitando que los grupos más vulnerables queden expuestos de manera desproporcionada a riesgos cibernéticos.

Finalmente, las experiencias latinoamericanas destacan la importancia de acciones regulatorias y educativas, dado que muchos países presentan vacíos legales en materia de seguridad de redes públicas, lo que dificulta sancionar la creación de redes falsas o el uso indebido de datos personales (Kern, 2004). Iniciativas municipales y estatales en México, como la implementación de Wi-Fi gratuito en espacios públicos, han comenzado a incorporar prácticas de seguridad, pero persiste la necesidad de estandarizar protocolos y concienciar a los usuarios sobre su uso seguro.

En conjunto, estas evidencias sugieren que, aunque los riesgos y comportamientos observados en Latinoamérica son consistentes con hallazgos internacionales, los contextos socioeconómicos y regulatorios locales generan particularidades que requieren estrategias adaptadas, combinando educación, soluciones técnicas y políticas públicas que aseguren tanto la accesibilidad como la seguridad en el uso de Wi-Fi público en entornos urbanos. Estos hallazgos regionales validan la pertinencia del enfoque socio-tecnológico para analizar la apropiación social de infraestructuras digitales urbanas en donde la intersección entre necesidades de conectividad y condiciones socioeconómicas locales

requiere comprensión contextualizada de las prácticas ciudadanas específicas.

Movilidad digital y territorio urbano

El Wi-Fi público configura un territorio digital sobre el espacio físico urbano, transformando la manera en que los ciudadanos interactúan con la ciudad y sus servicios. La disponibilidad y seguridad de la conectividad impactan directamente la movilidad digital, es decir, la capacidad de acceder a información y servicios mientras se desplazan por la ciudad. Por ejemplo, usuarios que dependen de transporte público o se desplazan por áreas densamente urbanizadas pueden enfrentar riesgos de seguridad y limitaciones de acceso si las redes no son confiables.

Este enfoque evidencia que el Wi-Fi público debe conceptualizarse como infraestructura urbana esencial, al igual que el transporte, la iluminación o la red vial, integrando planificación tecnológica y urbana para fortalecer la seguridad, la equidad y la inclusión digital. La implementación de redes seguras y accesibles puede convertirse en una estrategia clave para promover ciudades inteligentes y participativas, donde la movilidad física y digital se complementen.

Marco conceptual: Wi-Fi público como infraestructura socio-territorial

Esta revisión propone conceptualizar el Wi-Fi público como infraestructura socio-territorial urbana que trasciende la dimensión puramente tecnológica. Este marco se fundamenta en la comprensión de que las dinámicas de apropiación social de tecnologías digitales urbanas reflejan procesos complejos de negociación entre necesidad de conectividad y percepción de riesgo (UN-Habitat, 2021).

Marco tri-dimensional integrado:

a) Dimensión técnica: Vulnerabilidades documentadas y estrategias de mitigación, donde la caracterización técnica de vulnerabilidades constituye la base material para comprender la construcción social del riesgo cibernético en espacios públicos (UN-Habitat, 2021).

b) Dimensión social: Comportamientos ciudadanos condicionados por factores socioeconómicos, reconociendo que la transformación digital depende de la interacción con factores económicos, sociales e institucionales (CEPAL, 2022) y que aproximadamente el 30% de la población adulta latinoamericana mayor de 15 años tenía habilidades digitales básicas en 2020.

c) Dimensión territorial: Distribución espacial que impacta equidad y movilidad urbana, donde la materialidad digital condiciona las prácticas sociales urbanas (UN-Habitat, 2021), y la configuración técnica de redes funciona como determinante de prácticas sociales específicas.

d) Contribución teórica: Este enfoque supera la tradicional separación entre estudios técnicos de ciberseguridad y análisis sociales de usuarios, integrando las tres dimensiones del desarrollo digital identificadas por CEPAL (2022): economía conectada, economía digital y economía digitalizada, aplicadas al contexto de infraestructuras digitales públicas urbanas.

Conclusiones

Esta revisión de la literatura sobre Wi-Fi público en el tejido urbano revela que las vulnerabilidades como desafío urbano integral persisten de manera significativa. A pesar del conocimiento creciente sobre los riesgos, las vulnerabilidades de seguridad en redes Wi-Fi públicas siguen siendo prevalentes (Sombatruang et al., 2018; Ali et al., 2019; Sangeen et al., 2023), representando no solo riesgos tecnológicos sino desafíos que afectan el derecho a la ciudad y la equidad digital, con exposición diferenciada según condiciones socioeconómicas.

Los factores comportamentales y la apropiación social de estas infraestructuras digitales demuestran que el comportamiento de usuarios está influenciado por la heurística de preservación de recursos (Sombatruang et al., 2019), factores demográficos (Ndibwile et al., 2019), y elementos contextuales (Bonné et al., 2017). En Latinoamérica, la movilidad digital depende críticamente de redes Wi-Fi seguras, especialmente para usuarios con recursos limitados, quienes enfrentan una tensión constante entre la necesidad de conectividad y la exposición a riesgos de seguridad.

La evidencia analizada subraya que el Wi-Fi público se consolida como infraestructura socio-territorial esencial en la configuración urbana contemporánea (McShane et al., 2016; Maimon et al., 2020). Esta infraestructura requiere una conceptualización que trascienda lo puramente tecnológico, vinculándose estrechamente con la planificación territorial, la movilidad urbana y la configuración del espacio público. Las estrategias efectivas para abordar esta complejidad deben combinar soluciones técnicas como VPN y HTTPS (McShane et al., 2016), educación contextualizada de usuarios (Ndibwile et al., 2018), y políticas regulatorias para proveedores (Lotfy et al., 2021), superando aproximaciones puramente tecnológicas hacia enfoques socio-tecnológicos integrales.

Las consideraciones de equidad digital y las particularidades del contexto latinoamericano revelan que los usuarios con recursos limitados enfrentan mayor exposición a riesgos cibernéticos. La evidencia regional documenta patrones similares a los internacionales, pero con particularidades socioeconómicas y regulatorias que requieren estrategias adaptadas e intervenciones contextualizadas que reconozcan el Wi-Fi público como una necesidad social esencial para la inclusión digital.

Para planificadores urbanos, estas conclusiones sugieren tratar el Wi-Fi

público como infraestructura esencial con enfoque de equidad territorial. Para proveedores, existe oportunidad de diferenciación mediante mejores prácticas de seguridad. Para usuarios, se requieren medidas proactivas complementadas con alfabetización digital contextualizada.

Futuras investigaciones deberían explorar aspectos socioeconómicos desde marcos de apropiación social de tecnologías urbanas y desarrollar intervenciones específicas para contextos latinoamericanos, contribuyendo a ciudades más seguras, equitativas y digitalmente inclusivas. La evidencia valida la pertinencia de enfoques transdisciplinarios que integren estudios socio-tecnológicos con sistemas ciber-físicos urbanos para comprender la intersección entre tecnología, sociedad y territorio.

Glosario técnico

Captive portal (Portal cautivo): Sistema de autenticación utilizado en redes Wi-Fi públicas que solicita información del usuario (como correo electrónico o registro en redes sociales) antes de permitir el acceso a Internet. Puede representar riesgos de privacidad y seguimiento de datos (Ali et al., 2019).

Evil Twin Access Point (Punto de acceso gemelo malicioso): Punto de acceso inalámbrico fraudulento que imita la red legítima mediante la duplicación del SSID. Permite interceptar todo el tráfico de datos no cifrado, incluyendo credenciales y datos personales (Szongott et al., 2015).

Heurística de preservación de recursos: Comportamiento de los usuarios que priorizan la conservación de datos móviles limitados, motivando el uso de redes Wi-Fi públicas potencialmente inseguras (Sombatruang et al., 2016, 2019).

Infraestructura urbana digital: Conjunto de tecnologías que conforman la conectividad en espacios urbanos, incluyendo Wi-Fi público, sensores urbanos y plataformas digitales, consideradas esenciales para la movilidad, interacción ciudadana y servicios urbanos (McShane et al., 2016).

Red Wi-Fi pública: Red inalámbrica abierta o de fácil acceso disponible en espacios urbanos, transporte público o establecimientos comerciales, caracterizada por su facilidad de acceso y vulnerabilidades técnicas (Cheng et al., 2013; Bonné et al., 2017).

Seguridad de red: Conjunto de prácticas, protocolos y configuraciones técnicas destinadas a proteger la información transmitida en redes inalámbricas contra accesos no autorizados, ataques de intermediario y compromisos de privacidad (Szewczyk y Macdonald, 2017).

Territorio urbano: Espacio físico de la ciudad donde convergen infraestructuras digitales como redes Wi-Fi públicas. La disponibilidad y seguridad de estas redes influyen en cómo los ciudadanos acceden a servicios e interactúan con el espacio público.

Vulnerabilidad técnica: Debilidad en hardware, software o configuración de red que puede ser explotada para comprometer la seguridad y privacidad de los usuarios. Incluye configuraciones erróneas de dispositivos, firmware desactualizado y protocolos inseguros (Zhang et al., 2017; Ndibwile et al., 2019).

VPN (Virtual Private Network / Red Privada Virtual): Tecnología que crea un canal cifrado para proteger la transmisión de datos en redes inseguras, asegurando confidencialidad e integridad de la información (McShane et al., 2016).

Equidad digital: Condición en la que todos los ciudadanos tienen acceso seguro, confiable y asequible a servicios digitales y conectividad, independientemente de factores socioeconómicos o geográficos (Sombatruang et al., 2019; Folta et al., 2022).

Movilidad digital: Capacidad de acceder a información y servicios digitales mientras las personas se desplazan por la ciudad. Depende de la disponibilidad y seguridad de redes Wi-Fi públicas que permitan conectividad continua en diferentes espacios urbanos.

Portales maliciosos: Variantes de captive portals que recopilan datos personales de manera excesiva o engañosa, y pueden usar mecanismos de seguimiento sin consentimiento explícito (Ali et al., 2019).

Redes abiertas sin cifrado: Redes Wi-Fi que permiten conexión sin autenticación y sin cifrado de datos, exponiendo a los usuarios a interceptación pasiva, ataques man-in-the-middle y robo de credenciales (Cheng et al., 2013; Bonné et al., 2017).

Vacíos legales regulatorios: Ausencia o desactualización de marcos legales que regulen el acceso inalámbrico y la protección de datos en redes públicas, permitiendo que actividades maliciosas queden impunes (Kern, 2004).

Configuraciones erróneas de dispositivos: Ajustes inapropiados en smartphones y laptops, como compartir archivos, visibilidad de redes y posponer

Referencias

Ali, S., Osman, T., Mannan, M., & Youssef, A. (2019). On privacy risks of public WiFi captive portals. En C. Pérez-Solà, G. Navarro-Arribas, A. Biryukov, & J. Garcia-Alfaro (Eds.), Data privacy management, cryptocurrencies and blockchain technology (pp. 80-98). Springer. https://doi.org/10.1007/978-3-030-31500-9_6

Bonné, B., Rovelo, G., Quax, P., & Lamotte, W. (2017). Insecure network, unknown connection: Understanding Wi-Fi privacy assumptions of mobile device users. Information, 8(3), 76. https://doi.org/10.3390/info8030076

Cheng, N., Oscar Wang, X., Cheng, W., Mohapatra, P., & Seneviratne, A. (2013). Characterizing privacy leakage of public WiFi networks for users on travel. 2013 Proceedings IEEE INFOCOM, 2769-2777. https://doi.org/10.1109/INFCOM.2013.6567086

Comisión Económica para América Latina y el Caribe. (2022). A digital path for sustainable development in Latin America and the Caribbean (LC/CMSI.8/3). Naciones Unidas.

De Santo, A., & Gaspoz, C. (2015). Influence of users' privacy risks literacy on the intention to install a mobile application. En A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis (Eds.), New contributions in information systems and technologies (pp. 329-341). Springer. https://doi.org/10.1007/978-3-319-16486-1_33

Diekert, F., & Brekke, K. A. (2022). Groups discipline resource use under scarcity. Theory and Decision, 92(1), 75-103. https://doi.org/10.1007/s11238-021-09813-4

Ferreira, A., Huynen, J.-L., Koenig, V., & Lenzini, G. (2014). Socio-technical security analysis of wireless hotspots. En T. Tryfonas & I. Askoxylakis (Eds.), Human aspects of information security, privacy, and trust (pp. 306-317). Springer. https://doi.org/10.1007/978-3-319-07620-1_27

Folta, S. C., Anyanwu, O., Pustz, J., Oslund, J., Penkert, L. P., & Wilson, N. (2022). Food choice with economic scarcity and time abundance: A qualitative study. Health Education & Behavior, 49(1), 150-158. https://doi.org/10.1177/10901981211045926

Janse Van Rensburg, W., Thomson, K.-L., & Futcher, L. (2018). Factors influencing smartphone application downloads. En L. Drevin & M. Theocharidou (Eds.), Information security education – towards a cybersecure society (pp. 81-92). Springer. https://doi.org/10.1007/978-3-319-99734-6_7

Kern, B. D. (2004). Whacking, joyriding and war-driving: Roaming use of Wi-Fi and the law. Santa Clara High Technology Law Journal, 21(1), 101-178. https://digitalcommons.law.scu.edu/chtlj/vol21/iss1/3

Lotfy, A. Y., Zaki, A. M., Abd-El-Hafeez, T., & Mahmoud, T. M. (2021). Privacy issues of public Wi-Fi networks. En A. E. Hassanien, A. Haqiq, P. J. Tonellato, L. Bellatreche, S. Goundar, A. T. Azar, E. Sabir, & D. Bouzidi (Eds.), Proceedings of the International Conference on Artificial Intelligence and Computer Vision (AICV2021) (pp. 656-665). Springer. https://doi.org/10.1007/978-3-030-76346-6_58

Lugovic, S., Mrsic, L., & Korona, L. Z. (2019). Public WiFi security network protocol practices in tourist destination. En C. Esposito, J. Hong, & K.-K. R. Choo (Eds.), Pervasive systems, algorithms and networks (pp. 321-332). Springer. https://doi.org/10.1007/978-3-030-30143-9_27

Lv, X., Wang, X., & Fu, X. (2014). Why poverty impedes decision performance? Three psychological explanations. Advances in Psychological Science, 22(11), 1823. https://doi.org/10.3724/SP.J.1042.2014.01823

Maimon, D., Howell, C. J., Jacques, S., & Perkins, R. C. (2020). Situational awareness and public Wi-Fi users' self-protective behaviors. Security Journal, 35,

154-174. https://doi.org/10.1057/s41284-020-00270-2

McShane, I., Gregory, M. A., & Wilson, C. (2016). Practicing safe public Wi-Fi: Assessing and managing data-security risks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2895216

Ndibwile, J. D., Luhanga, E. T., Fall, D., Miyamoto, D., & Kadobayashi, Y. (2018). A comparative study of smartphone-user security perception and preference towards redesigned security notifications. Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities, 1-6. https://doi.org/10.1145/3283458.3283486

Ndibwile, J. D., Luhanga, E., Fall, D., & Kadobayashi, Y. (2019). A demographic perspective of smartphone security and its redesigned notifications. J. Inf. Process., 27, 773-786. https://doi.org/10.2197/ipsjjip.27.773

Ndibwile, J. D., Luhanga, E. T., Fall, D., Miyamoto, D., & Kadobayashi, Y. (2018). Smart4Gap: Factors that influence smartphone security decisions in developing and developed countries. Proceedings of the 2018 10th International Conference on Information Management and Engineering, 5-15. https://doi.org/10.1145/3285957.3285980

Sangeen, M., Bhatti, N. A., Kifayat, K., Alsadhan, A. A., & Wang, H. (2023). Blind-trust: Raising awareness of the dangers of using unsecured public Wi-Fi networks. Computer Communications, 209, 359-367. https://doi.org/10.1016/j.comcom.2023.07.011

Sombatruang, N., Kadobayashi, Y., Sasse, M. A., Baddeley, M., & Miyamoto, D. (2018). The continued risks of unsecured public Wi-Fi and why users keep using it: Evidence from Japan. 2018 16th Annual Conference on Privacy, Security and Trust (PST), 1-11. https://doi.org/10.1109/PST.2018.8514208

Sombatruang, N., Onwuzurike, L., Sasse, M. A., & Baddeley, M. (2019). Factors influencing users to use unsecured wi-fi networks: Evidence in the wild. Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks, 203-213. https://doi.org/10.1145/3317549.3323412

Sombatruang, N., Sasse, M. A., & Baddeley, M. (2016). Why do people use unsecure public wi-fi?: An investigation of behaviour and factors driving decisions. Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, 61-72. https://doi.org/10.1145/3046055.3046058

Soon, J.-J., Abdul Adzis, A., Applanaidu, S. D., & Zainal Abidin, N. (2024). Food expenditure of the poorest deciles: Expected vulnerability and counterintuitive indulgence? Journal of the Asia Pacific Economy, 29(3), 1239-1256. https://doi.org/10.1080/13547860.2023.2166718

Swanson, C., Urner, R., & Lank, E. (2010). Naïve security in a Wi-Fi world. En M. Nishigaki, A. Jøsang, Y. Murayama, & S. Marsh (Eds.), Trust management IV (pp.

32-47). Springer. https://doi.org/10.1007/978-3-642-13446-3_3

Szewczyk, P., & Macdonald, R. (2017). Broadband router security: History, challenges and future implications. The Journal of Digital Forensics, Security and Law. https://doi.org/10.15394/jdfsl.2017.1444

Szongott, C., Brenner, M., & Smith, M. (2015). METDS - a self-contained, context-based detection system for evil twin access points. En R. Böhme & T. Okamoto (Eds.), Financial cryptography and data security (pp. 370-386). Springer. https://doi.org/10.1007/978-3-662-47854-7_22

UN-Habitat. (2021). Assessing the digital divide: Understanding internet connectivity and digital literacy in cities and communities. United Nations Human Settlements Programme.

Zhang, X. J., Li, Z., & Deng, H. (2017). Information security behaviors of smartphone users in China: An empirical analysis. The Electronic Library, 35(6), 1177-1190. https://doi.org/10.1108/EL-09-2016-0183