UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SUBSISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Análisis de los mecanismos de prevención y mitigación de ataques contra la autenticación y el cifrado en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 para el fortalecimiento de la seguridad de acceso.

AUTOR:

Ing. Huilcapi Subía Darío Fernando

Trabajo de Titulación previo a la obtención del Grado Académico de

MAGÍSTER EN TELECOMUNICACIONES

TUTOR:

Ph.D. Bohórquez Escobar Celso Bayardo

Guayaquil, 14 de julio del 2026

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SUBSISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

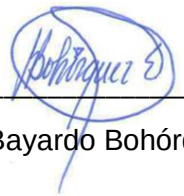
CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el **Ing. Darío Fernando Huilcapi Subía** como requerimiento parcial para la obtención del Grado Académico de **MAGÍSTER EN TELECOMUNICACIONES**

TUTOR

Ph.D. Celso Bayardo Bohórquez Escobar

DIRECTOR DEL PROGRAMA



Ph.D. Celso Bayardo Bohórquez Escobar

Guayaquil, 14 de julio del 2026

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SUBSISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, Darío Fernando Huilcapi Subía

DECLARO QUE:

El trabajo de titulación **"Análisis de los mecanismos de prevención y mitigación de ataques contra la autenticación y el cifrado en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 para el fortalecimiento de la seguridad de acceso."**, previa a la obtención del grado Académico de Magíster, ha sido desarrollado en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del trabajo de titulación del Grado Académico en mención.

Guayaquil, 14 de julio del 2026

EL AUTOR

Ing. Darío Fernando Huilcapi Subía

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SUBSISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Darío Fernando Huilcapi Subía**

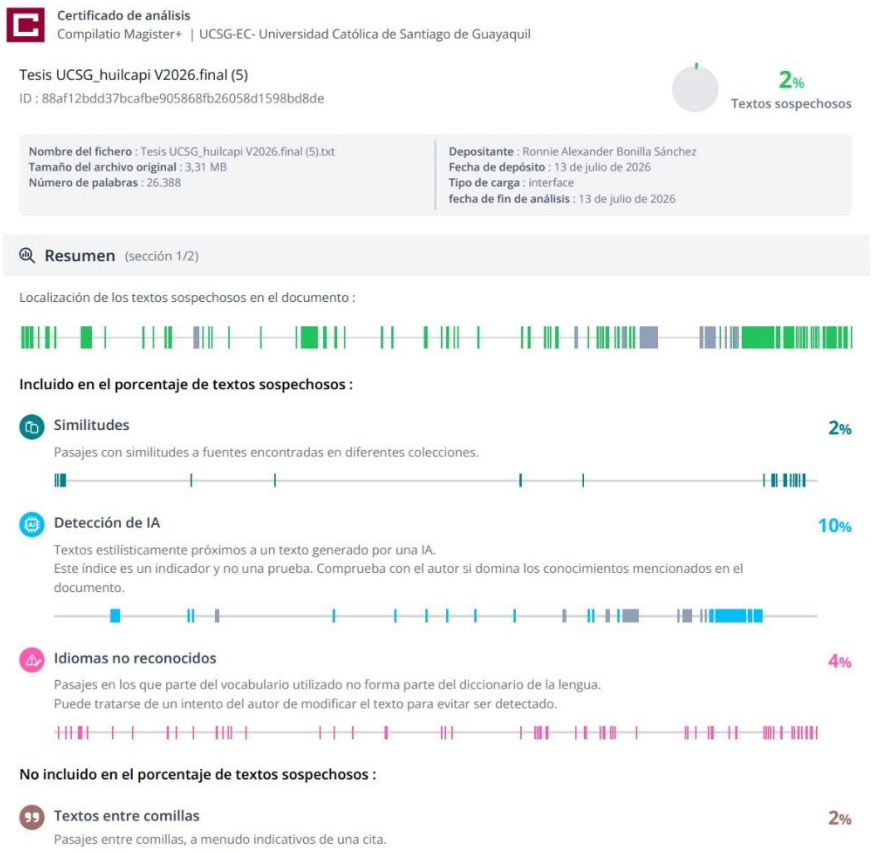
Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del trabajo de titulación de Maestría titulado: **"Análisis de los mecanismos de prevención y mitigación de ataques contra la autenticación y el cifrado en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 para el fortalecimiento de la seguridad de acceso."**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 14 días del mes de julio del año 2026

EL AUTOR

Ing. Darío Fernando Huilcapi Subía

INFORME DE COMPILATIO



Certificado de análisis
Compilatio Magister+ | UCSG-EC- Universidad Católica de Santiago de Guayaquil

Tesis UCSG_huilcapi V2026.final (5)
ID : 88af12bdd37bcafbe905868fb26058d1598bd8de

2%
Textos sospechosos

Nombre del fichero : Tesis UCSG_huilcapi V2026.final (5).txt
Tamaño del archivo original : 3,31 MB
Número de palabras : 26.388

Depositante : Ronnie Alexander Bonilla Sánchez
Fecha de depósito : 13 de julio de 2026
Tipo de carga : interface
fecha de fin de análisis : 13 de julio de 2026

Resumen (sección 1/2)

Localización de los textos sospechosos en el documento :

Incluido en el porcentaje de textos sospechosos :

Similitudes 2%
Pasajes con similitudes a fuentes encontradas en diferentes colecciones.

Detección de IA 10%
Textos estilísticamente próximos a un texto generado por una IA.
Este índice es un indicador y no una prueba. Comprueba con el autor si domina los conocimientos mencionados en el documento.

Idiomas no reconocidos 4%
Pasajes en los que parte del vocabulario utilizado no forma parte del diccionario de la lengua.
Puede tratarse de un intento del autor de modificar el texto para evitar ser detectado.

No incluido en el porcentaje de textos sospechosos :

Textos entre comillas 2%
Pasajes entre comillas, a menudo indicativos de una cita.

Reporte Compilatio del trabajo de titulación de la Maestría en Telecomunicaciones denominado: **"Análisis de los mecanismos de prevención y mitigación de ataques contra la autenticación y el cifrado en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 para el fortalecimiento de la seguridad de acceso"**, del Ing. Darío Fernando Huilcapi Subía, de la IV promoción, se encuentra al 2% de coincidencias.

Atentamente,

Ing. Bayardo Bohórquez Escobar, Ph.D
Docente-Tutor

Agradecimiento

Agradezco, en primer lugar, a Dios, por la vida, la salud y la fortaleza para llegar hasta aquí. A mis padres, por su amor, sus enseñanzas y los valores que me hicieron mejor ser humano. A mi familia, en especial a mi esposa, por su apoyo, su comprensión y su compañía constante; a mis hermanos, por su ejemplo y cercanía; y a mis sobrinos, por la alegría que le suman a mi vida.

A mis hijos, que, aunque los menciono al final ocupan el primer lugar en mi corazón, porque son la razón por la que me levanto cada día con ganas de seguir luchando, aprendiendo y trabajando para darles un presente digno y un futuro cada vez mejor.

Mi gratitud también a todas las personas que, de manera directa o indirecta, aportaron algo a este camino: un consejo, un ejemplo, una palabra de aliento o una broma que hizo más llevaderos los días difíciles. En especial, a mis compañeros de trabajo y amigos.

Por último, un agradecimiento especial al Ph.D. Celso Bayardo Bohórquez Escobar y a todo su equipo, que dieron su tiempo, su conocimiento y un acompañamiento incondicional, haciendo grandes esfuerzos para ayudarnos a superar las dificultades y alcanzar esta meta académica.

Dedicatoria

Dedico este trabajo, ante todo, a mi mamá y a mi esposa. La primera me dio la vida, me enseñó a caminar con los pies en la tierra y me regaló la mejor vida que un hijo puede soñar; la segunda me enseñó a vivirla con amor, propósito y esperanza.

A ti, mamita de mi vida, porque no hay un solo día en que no te piense ni te extrañe. Por ti prometí terminar este camino de la manera más honorable posible, tal como me enseñaste a enfrentar cada desafío. En cada logro y en cada meta alcanzada siempre estás tú, y sé que en esta tampoco vas a faltar, porque vives para siempre en mi memoria, en mis valores y en mi corazón.

A mi esposa, una verdadera guerrera, porque con valentía y optimismo me demuestra cada día cómo enfrentar la adversidad, me recuerda que nunca hay que dejar de luchar y me enseña a confiar plenamente en Dios, incluso en los momentos más difíciles.

A mis hijos, por llenar los espacios vacíos de mi corazón, por darme motivos para sonreír y por hacer de cada día una razón para seguir adelante.

A mi papá, por cada sacrificio que hizo para que hoy podamos disfrutar de una vida feliz. Su amor, su esfuerzo y su entrega dejaron en mí un ejemplo que llevaré siempre, y por el que estaré eternamente agradecido.

A mis hermanos, por estar ahí, por tenderme la mano y ayudarme cada vez que los he necesitado.

Y a todas las personas que, con su cariño, su ejemplo, su compañía o una palabra dicha en el momento justo, hacen que esta vida sea hermosa.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SUBSISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

Ph.D. Celso Bayardo Bohórquez Escobar

TUTOR

f. _____

Mgtr. Nestor Armando Zamora Cedeño

REVISOR

f. _____

Mgtr. Ronnie Alexander Bonilla Sánchez

REVISOR

f. _____

Ph.D. Celso Bayardo Bohórquez Escobar

DIRECTOR DEL PROGRAMA (e)

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

Las redes Wi-Fi permiten la conexión universal de dispositivos inalámbricos en diferentes ámbitos, pero su evolución no eliminó las amenazas de autenticación, cifrado y control de acceso. El problema abarca diferentes aspectos que afecta a factores como credencias débiles, protocolos heredados, tramas de administración desprotegidas, firmware desactualizado, segmentación deficiente e identidad de acceso limitada. El presente estudio analiza estrategias actuales para prevención y mitigación de amenaza en las redes WiFi, para recomendar alternativas que fortalezcan la seguridad de acceso. La metodología de investigación empleó un enfoque descriptivo y explicativo, además de un diseño documental, utilizando el método PRISMA para la revisión sistemática que se complementó con un análisis documental, técnico y comparativo. Se obtuvieron 53 fuentes bibliográficas que caracterizan tanto las amenazas, como las vulnerabilidades, además de los mecanismos y condiciones adecuados para su implementación. Posteriormente los resultados sugieren que WPA2, WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS y PMF cumplen funciones distintas y pero que a su vez complementarias permitiendo inferir que ningún control aplicable aislado permitiría cubrir la variedad de escenarios susceptibles de riesgos. Se comprendió y determinó que las diversas generaciones de redes Wi-Fi no son la causa principal por la cual están expuestas a vulnerabilidades y amenazas, sino que son un conjunto de factores como la compatibilidad, la configuración, la gestión de credenciales, la actualización, la segmentación y un monitoreo sostenido que permiten contar con un esquema relativamente seguro. El aporte del estudio consiste en establecer una gama de estrategias que confronta las amenazas y debilidades desembocando en mecanismos de prevención, mitigación y fortalecimiento estructural. Se concluye que una arquitectura de defensa en profundidad, con autenticación robusta, cifrado vigente, protección de tramas, control de identidad, hardening y supervisión, reduce la superficie de exposición y mejora la seguridad operativa.

Palabras clave: seguridad WLAN, IEEE 802.11, WPA3, autenticación inalámbrica, cifrado, control de acceso, revisión sistemática PRISMA, Wi-Fi 6.

ABSTRACT

Wi-Fi networks enable the universal connection of wireless devices in different environments, but their evolution did not eliminate authentication, encryption, and access control threats. The problem covers different aspects that affect factors such as weak credentials, legacy protocols, unprotected management frames, outdated firmware, poor segmentation, and limited access identity. The present study analyzes current strategies for the prevention and mitigation of threats in Wi-Fi networks, in order to recommend alternatives that strengthen access security. The research methodology employed a descriptive and explanatory approach, in addition to a documentary design, using the PRISMA method for the systematic review, which was complemented with documentary, technical, and comparative analysis. Fifty-three bibliographic sources were obtained that characterize both threats and vulnerabilities, in addition to the mechanisms and conditions appropriate for their implementation. Subsequently, the results suggest that WPA2, WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS, and PMF perform different and but at the same time complementary functions, allowing the inference that no isolated applicable control would make it possible to cover the variety of scenarios susceptible to risks. It was understood and determined that the different generations of Wi-Fi networks are not the main cause for which they are exposed to vulnerabilities and threats, but rather that they are a set of factors such as compatibility, configuration, credential management, updating, segmentation, and sustained monitoring that make it possible to have a relatively secure scheme. The contribution of the study consists of establishing a range of strategies that confronts threats and weaknesses, leading to prevention, mitigation, and structural strengthening mechanisms.

Keywords: access control, encryption, IEEE 802.11, PRISMA systematic review, wireless authentication, Wi-Fi 6, WLAN security, WPA3.

INTRODUCCIÓN

Las redes wifi predominan en la actualidad por ser por excelencia de fácil acceso y de simple conexión, el incremento y masificación de los dispositivos en el hogar, en las empresas y la tendencia de convertir todo equipo a los Smart crea un campo de desarrollo amplio para wifi, no concebimos una empresa, un hospital o un centro educativo sin este servicio.

Pero con ello también aparecen diferentes problemas que no solo comprometen la seguridad de la información sino la estabilidad de los procesos y reputación empresarial, estos problemas no solo son responsabilidad de los dueños o administradores de red sino es un acuerdo implícito donde el usuario debe ser cauto y velar x la seguridad de su equipo porque puede convertirse en el inicio del vector de ataque.

Aunque si bien es cierto, los cambios generacionales impulsan mejoras en los servicios, algoritmos y demás mecanismos de control, de nada sirve si se desconocen o no se los aplican por conveniencia en el uso de versiones antigua, por ello se considera que se debe estudiar no solo un mecanismo aislado, sino el conjunto de estrategias de autenticación, cifrado, control y protección de tramas, y guías de configuración segura para aportar con estrategias, mecanismos y servicios relevantes como AES-CCMP, SAE, OWE, PMF, 802.1X, EAP-TLS. (Halbouni et al., 2023b).

El problema científico radica en que persisten amenazas como desautenticación, abuso de tramas de administración, rogue AP, evil twin, Man-in-the-Middle, captura de handshakes, ataques de diccionario, fuerza bruta, downgrade y explotación de credenciales débiles. Estudios recientes evidencian que los ataques de downgrade continúan siendo relevantes en sistemas Wi-Fi de nueva generación, lo que exige mecanismos de detección, prevención y mitigación más sistemáticos (Tareef et al., 2025).

El estudio analizará los principales mecanismos de prevención y mitigación de ataques de autenticación y cifrado en redes inalámbricas Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7, mediante una investigación de tipo descriptiva y de naturaleza explicativa, para proponer alternativas que fortalezcan la seguridad

de acceso en entornos IEEE 802.11 actuales.

Capítulo 1: Descripción del proyecto de intervención

1.1. Antecedentes de la investigación

Conforme evolucionan las comunicaciones digitales la necesidad de acceso a contenidos y conectividad entre instalaciones y dispositivos se convierte en una necesidad indispensable para los diferentes sectores residenciales, comerciales y productivos de una sociedad como es la medicina, la educación, la industria entre otros. Además, el consumo de contenido multimedia, el internet de las cosas y del todo ha llevado a la generación Y (migrantes digitales) y Z (nativos digitales) a demandar redes de alta velocidad y que sean de fácil acceso manteniendo la transparencia en la comunicación garantizando la integridad y disponibilidad, es por ello que las redes inalámbricas han permitido la evolución de la portabilidad de los dispositivos de comunicaciones por lo cual estas han tenido un desarrollo vertiginoso.

La principal tecnología de acceso a WLAN es aquella que utiliza el conjunto de estándares IEEE 802.11, por su facilidad de implementación, costos accesibles, facilidad de administración y sobretodo el uso de espectro no regulado siendo esto también una desventaja ya que puede dar cabida a la saturación de canales por una mala administración en la planificación del espectro. El efecto de la saturación es más crítico cuando se utiliza wireless como accedo de última milla ya que con ello se incrementa la posibilidad de encontrar en su camino redes que trabajen a la misma frecuencia.

Los principales ISP que operan en la ciudad de Guayaquil ofrecen a sus clientes residenciales Router Access Point como medio de acceso para conectarse a la red WLAN que los transportará a internet, es precisamente en este proceso donde se producen diversas vulnerabilidades debido a la fragilidad de los mecanismos de autenticación y encriptación que utilizan estas empresas proveedoras de servicios de internet.

Este problema no es exclusivo de la WLAN domésticas, aplicaciones empresariales pueden sufrir las mismas vulnerabilidades y ataques de acceso a la red dejando expuesta la información que por ellas se trafique y ocasionando pérdidas en los negocios.

De acuerdo con la Tabla 1, en el último reporte de incidentes basados en la clasificación general presentado por (MyCert, 2026) (departamento dentro de seguridad cibernética Malasia), muestra que en el primer semestre del 2026 el principal riesgo a la seguridad es ocasionado por la intrusión a los sistemas, seguido de los códigos maliciosos y la vulnerabilidades no parchadas; esto pone en evidencia que es necesario estrategias de autenticación, encriptación además de la socialización y concientización de los mecanismos de seguridad para acceso a la red inalámbrica con el usuario final.

Tabla 1

Reported Incidents based on General Incident Classification Statistics 2026

Incidente	Ene.	Feb.	Mar.	Abr.	May.	Jun.	Jul.	Ago.	Sep.	Oct.	Nov.	Dic.	Total
Intrusion Attempt	26	21	35	33	28	0	0	0	0	0	0	0	143
Vulnerabilities Report	8	6	12	4	4	0	0	0	0	0	0	0	34
Spam	8	14	9	11	7	0	0	0	0	0	0	0	49
Intrusion	21	17	25	25	13	0	0	0	0	0	0	0	101
Fraud	574	636	619	759	675	0	0	0	0	0	0	0	3,263
Content Related	36	43	45	67	61	0	0	0	0	0	0	0	252
Denial of Service	2	1	2	0	0	0	0	0	0	0	0	0	5
Malicious Codes	12	9	7	12	11	0	0	0	0	0	0	0	51
Total	**687**	**747**	**754**	**911**	**799**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**3,898**

Nota. Adaptado de *Reported Incidents based on General Incident Classification Statistics 2026*, por Malaysia Computer Emergency Response Team (MyCERT), 2026, CyberSecurity Malaysia. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=17e4d4cf-1ce2-4ceb-85d2-6cdf484b9faa

1.2. Planteamiento del problema

Los administradores de red y personal técnico solo utilizarán algoritmos de encriptación por defecto, pero no utilizan buenas prácticas para definir las políticas de seguridad de la red inalámbrica por desconocimiento o por falta de preocupación, esto provoca grandes pérdidas a las compañías y compromete la seguridad de la información de los usuarios domésticos y empresariales, debido a la fragilidad de los protocolos de encriptación comúnmente utilizados.

Uno de los factores más alarmantes es el desconocimiento en los usuarios finales y de los administradores de redes caseras, acerca de las vulnerabilidades existentes y malas prácticas de seguridad en las que incurren cotidianamente, lo que los lleva a desconfiar solo en aquellos factores inseguros que conocen como por ejemplo compartir la contraseña de su Wireless. En un análisis a gran escala sobre contraseñas Wi-Fi, Veroni et al. (2022) evidencian que los usuarios tienden a subestimar la importancia de las contraseñas de redes privadas en relación con su seguridad y privacidad, lo que incrementa la exposición frente a accesos no autorizados y ataques dirigidos a mecanismos de autenticación inalámbrica.

Cuando el préstamo de la clave no es algo consentido el evento inmediato que puede ocurrir es tratar de conseguirla por otros mecanismos aplicando herramientas de penetración. En la actualidad de acuerdo con Bispham et al. (2021) el 25% de los usuarios de redes inalámbricas 802.11 no cambia su contraseña predeterminada de sus equipos router ap, así mismo se destaca que el 23% de los encuestados menciona que hubo acceso no autorizados a su red wifi sin su consentimiento, de los cuales el 49% lo hizo sin utilizar contraseña válida y el 37% usó la contraseña que tenía configurada en el equipo Access point.

No obstante, el problema no se centra únicamente en las debilidades de la administración de las contraseñas, sino que es mucho más profundo y escala a la configuración integral de los mecanismos de autenticación, cifrado y control de acceso. En las redes Wifi modernas existen problemas en debilidades de los algoritmos de cifrado WPA2 y WPA3, además de la coexistencia, el uso incorrecto de protocolos y modos de transición, así como la ausencia de PMF (Marcos de Gestión Protegidos) y de la falta de validación de certificados en entornos 802.1X/EAP-TLS, esto facilita ataques de desautenticación, rogue AP, evil twin, Man-in-the-Middle, captura de handshakes, ataques de diccionario, downgrade y accesos no autorizados, Fortinet (2026) advierte que los atacantes están automatizando el reconocimiento, reduciendo el tiempo entre la divulgación y explotación de

vulnerabilidades, y utilizando inteligencia artificial y herramientas mercantilizadas para acelerar el acceso inicial y la explotación.

1.3. Justificación

Las redes inalámbricas son susceptibles y están expuestas a los ataques debido a su naturaleza sin fronteras y su omnipresencia. De acuerdo con WE ARE SOCIAL (2022) en lo que va del 2022 se considera que el número de usuarios de internet ya superan la mitad de la población global y con ello el medio de acceso más utilizado son las redes inalámbricas 802.11.

Diversos estudios recientes señalan que el crecimiento del tráfico en redes Wi-Fi está estrechamente relacionado con la expansión de dispositivos IoT y con el aumento de superficies de ataque en entornos domésticos y empresariales, lo que exige reforzar las medidas de seguridad en redes inalámbricas(Rasool et al., 2025). Esto evidencia una tendencia de crecimiento que hasta la fecha se puede notar al observar la creciente demanda de dispositivos que se suman a la gama de lo inalámbrico. Este escenario definitivamente eleva el nivel de las medidas de seguridad que deben tenerse en cuenta, especialmente en la reducción de la intrusión en redes inalámbricas.

Para el 2026 las amenazas crecieron exponencialmente de la misma forma que se masificó el uso de la tecnología inalámbrica para las actividades cotidianas empresariales y del hogar, agregándole a esto el consumo del servicio a través del internet de las cosas IoT que permitieron incorporar termostatos, persianas, cámaras de seguridad y demás electrodomésticos a la red wifi.

Por lo expuesto anteriormente es necesario hacer énfasis en la seguridad de acceso de autenticación y encriptación, ya sea para evitar pérdidas económicas, de información sensible y personal, hasta evitar daños en las configuraciones y equipos de la red, debido a que las técnicas y mecanismos cambian y se mejoran con el tiempo, por ello es necesario estar a la vanguardia y hacer uso de las políticas y mecanismos de mitigación más idóneas y actualizados.

La estadística muestra que los patrones utilizados para los ataques cambian generacionalmente. “Desde 1997 hasta 2003 la mayoría de los incidentes registrados se debieron a casos de spam y virus, pero a partir de 2004 al 2014 hay una enorme inclinación en el intento de intrusión e intrusión del ataque a la red, propiamente a partir de ese año al 2022 se ha intensificado el ransonware, la suplantación de identidad y phishing con todas sus variantes Esto evidencia las limitaciones de Ecuador en materia de ciberseguridad, reflejadas en su ubicación dentro de los puestos inferiores del índice regional y en la persistencia de brechas institucionales y técnicas frente a las amenazas digitales (Sayago-Heredia, 2022).

El impacto económico que generan las amenazas cibernéticas no solo se miden como pérdidas monetarias sino como la acumulación de factores que afectan a la pérdida del valor empresarial, reputacional y continuidad operativa; esto se amplificó posterior a la pandemia COVID-19 debido a la masificación, integración, despliegue y migración de servicios a entornos online, la acelerada transformación digital puso en evidencia las vulnerabilidades de los servicios empresariales permitiendo que sean blanco de ataques de phishing, ransonware, malware, y clonación de identidades que interrumpen los servicios (Alawida et al., 2022).

En los últimos 5 años el panorama no ha cambiado y por lo contraria, las técnicas aplicadas se han perfeccionado e incrementado por ello (Cybersecurity Ventures, 2022) afirma que la estimación de costos globales totales por delitos de ciberseguridad podría alcanzar los 10.5 billones de dólares para el 2025, además de que los costos estimados anualmente aumentaron desde el 2018 en un total del 50%

Sumado a esto, la tendencia es que con el pasar de los años las técnicas utilizadas para los ataques disminuyen en complejidad y aumentan en impacto, lo que conlleva a que cualquier persona con un conocimiento mínimo pueda utilizar el sin fin de manuales de fácil alcance y estrenarse como atacante de la red dejándonos expuesto en caso de no utilizar las medidas adecuadas para protegernos. Por eso, proteger los servicios con estrategias de seguridad de la información se vuelve un elemento fundamental para la

autenticación, el cifrado, el control de acceso, la gestión de configuraciones y la mitigación de amenazas en las redes sin cables (Saeed et al., 2023).

En otro ámbito, las aplicaciones actuales se ven comprometidas por una inadecuada configuración o una política de seguridad no establecida, además todas aquellas aplicaciones futuras como wifi offload se pueden ver afectadas ante los riesgos de seguridad, por ello es importante identificar cada uno de ellos y comprender las tecnologías disponibles para controlarlo y mitigarlos.

Son tantas las vulnerabilidades como los ataques y casos documentados que existen donde la mayoría de ellos se resume en el eslabón más débil que es el usuario, su desconocimiento y los protocolos de acceso usados por defecto con pocas medidas de prevención, por lo cual es sumamente importante aportar con alternativas rápidas y sencillas para que el común de las personas pueda aplicarla a sus Access Point.

1.4. Objetivos

1.4.1. Objetivo general

Analizar los principales mecanismos de prevención y mitigación de ataques de autenticación y cifrado en redes inalámbricas Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7, mediante una investigación de tipo descriptiva y de naturaleza explicativa, para proponer alternativas que fortalezcan la seguridad de acceso en entornos IEEE 802.11 actuales.

1.4.2. Objetivos específicos

- Identificar los principales mecanismos de autenticación, cifrado y vulnerabilidades presentes en redes inalámbricas Wi-Fi modernas mediante una revisión sistemática de literatura basada en el método PRISMA para determinar las amenazas y debilidades de seguridad más relevantes en entornos inalámbricos.
- Analizar las políticas de seguridad, mecanismos de control de acceso y buenas prácticas aplicadas en redes inalámbricas Wi-Fi modernas mediante el estudio comparativo de protocolos y configuraciones de

seguridad, para identificar estrategias efectivas de prevención y mitigación frente a ataques de autenticación y cifrado.

- Proponer alternativas de fortalecimiento de seguridad para redes inalámbricas Wi-Fi modernas mediante el análisis de vulnerabilidades, mecanismos de protección y recomendaciones técnicas basadas en estándares IEEE 802.11, para reducir riesgos asociados a accesos no autorizados y ataques sobre redes inalámbricas modernas.

1.5. Hipótesis

La integración de mecanismos actualizados de prevención y mitigación, basados en autenticación robusta, cifrado seguro, protección de tramas de administración, control de acceso, gestión segura de credenciales, actualización de firmware, endurecimiento de configuraciones y buenas prácticas alineadas con IEEE 802.11 y los perfiles de seguridad WPA2/WPA3, contribuye al fortalecimiento de la seguridad de acceso en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7, al reducir la exposición frente a ataques contra autenticación, debilidades asociadas al cifrado, accesos no autorizados, downgrade, rogue AP, Man-in-the-Middle y configuraciones inseguras.

Variable independiente: mecanismos de prevención y mitigación de ataques contra autenticación y cifrado en redes IEEE 802.11.

Variable dependiente: fortalecimiento de la seguridad de acceso en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7.

Unidad de análisis: redes inalámbricas modernas basadas en IEEE 802.11, considerando entornos Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 y sus configuraciones de seguridad asociadas.

1.6. Metodología de la investigación

El diseño de la investigación nos guiará en el proceso de desarrollo de la investigación enmarcándonos en una planificación de los pasos necesarios para el cumplimiento de los objetivos, es importante porque disminuye el sesgo del investigador y mantiene la integridad de la información cuando sea recolectada.

Según Trochim et al. (2015), el diseño de la investigación “es el pegamento que mantiene el proyecto de investigación cohesionado. Un diseño es utilizado para estructurar la investigación, para mostrar cómo todas las partes principales del proyecto de investigación funcionan en conjunto con el objetivo de responder a las preguntas centrales de la investigación.”

Existen múltiples tipos de investigación, pero la mayoría de ellas responden a dos principales categorías como son los experimentales y los descriptivos.

1.6.1. Tipos de Investigación aplicada

Debido a las múltiples corrientes filosóficas, posturas epistemológicas y escuelas filosóficas existen un sin número de métodos, técnicas e instrumentos con los que el investigador debe enfrentarse al momento de elegir qué camino tomar en su investigación. Por ello es importante conocer los distintos tipos de estudios de investigación, entre ellos tenemos:

Tomado de Burbano (2015)

Por el ámbito en el que se efectúan

- De campo
- Experimentales

Por su Objetivo

- Exploratorio
- Descriptivos
    - Estudios de opinión y actitud
    - Estudios para predecir comportamiento
    - Estudio de las personas que habitan en un lugar

Por el periodo en el que se ejecutan

- Transversales
- Longitudinales
- Pilotos o previos
- Finales o definitivos

El presente estudio se desarrollará bajo un enfoque de investigación descriptivo y explicativo, debido a que busca analizar los principales

mecanismos de autenticación, cifrado, vulnerabilidades y estrategias de mitigación presentes en redes inalámbricas Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7, con el propósito de comprender las debilidades de seguridad más relevantes en entornos IEEE 802.11 actuales y proponer alternativas de fortalecimiento de la seguridad de acceso.

La investigación descriptiva/explicativa permitirá identificar y caracterizar los protocolos de autenticación, mecanismos de cifrado, amenazas, riesgos y configuraciones de seguridad aplicadas en redes inalámbricas modernas. Por ello, se describirán las principales vulnerabilidades asociadas a protocolos de seguridad inalámbrica como WPA2, WPA3 y mecanismos de autenticación basados en IEEE 802.11i.

El diseño es no experimental de tipo documental. No se manipulan variables ni se interviene en entornos reales de producción; el trabajo recae sobre el análisis técnico y comparativo de literatura científica, estándares IEEE 802.11, documentación técnica, reportes de ciberseguridad y estudios especializados en seguridad inalámbrica.

El método principal que se utilizará para la revisión sistemática es el método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), con la cual se identifican, seleccionan, clasifican y analizan estudios sobre mecanismos de autenticación, cifrado y mitigación de ataques en redes Wi-Fi modernas. La búsqueda se realiza en bases de datos científicas indexadas: IEEE Xplore, Scopus, ScienceDirect y SpringerLink.

Entonces podemos inferir que el estudio se centrarará en un análisis documental de las debilidades de las redes wifi, basándose en un revisión sistemática de fuentes de origen confiable y se propondrá un análisis comparativo de los mecanismos que comúnmente pueden afectar a la autenticación de usuarios y dispositivos, así como los mecanismos de cifrado vigentes y actuales, para complementar todo en el análisis técnico de las vulnerabilidades que se identifiquen versus las amenazas que comúnmente afectan a estas redes en la actualidad centrándonos solo en los estándares 5, 6 y 7 de Wi-Fi.

Capítulo 2: Fundamentación Teórica

2.1 Generalidades de las Redes Inalámbricas 802.11

Una red inalámbrica WLAN proporciona los mismos servicios y beneficios que las LAN tradicionales eliminando las limitaciones derivadas del uso del cable de cobre como medio de comunicación y manteniendo las características de las redes basadas en estándar Ethernet. Las redes de área local inicialmente se desarrollaron para coberturas medidas en metros, pero el desarrollo de la tecnología ha permitido llegar a varios kilómetros con los mismos beneficios, con base en esto, la IEEE 802.11 se ha consolidado como uno de los estándares más utilizados y maduros para comunicaciones inalámbricas dentro de redes de área local, debido a su evolución constante en capacidad, eficiencia, velocidad de transmisión y soporte para nuevos entornos de conectividad (Qureshi & Asghar, 2023a).

Las redes inalámbricas hacen uso del espectro de frecuencias de 2.4 Ghz y 5 Ghz, donde la primera de ellas es más utilizada para acceso del usuario, y la segunda para infraestructuras de comunicación punto a punto y punto multipunto en topologías bridge.

Las WLAN ofrecen beneficios relevantes para usuarios residenciales, organizaciones empresariales y proveedores de acceso inalámbrico, entre ellos movilidad, flexibilidad de despliegue, reducción de costos de infraestructura, arquitectura abierta y posibilidad de ampliar la cobertura de servicios de red. No obstante, estas ventajas deben acompañarse de una adecuada planificación técnica, administración centralizada, actualización de configuraciones y políticas de seguridad que permitan reducir riesgos asociados al acceso inalámbrico (Qureshi & Asghar, 2023b).

Los entornos favorables para implementar una wireless lan son aquellos que requieren las mismas velocidades de una Lan Ethernet, también cuando la reconfiguración física cambia a menudo y estos entornos tienden a crecer velozmente, se recomienda cuando las instalaciones son alquiladas y no está permitido remodelar la infraestructura.

2.2 Evolución de las Lan Inalámbricas 802.11

El estándar 802.11 fue definido en la norma IEEE que inicialmente se

basaba en un estándar propietario y de uso empresarial que inicio en el año 1990 y fue ratificado en 1992 con una tasa de transmisión de entre 1 y 2 Mbps, pero no fue hasta el año 1997 que se consideró de uso libre utilizando frecuencias de 2.4 Ghz siendo utilizado para el networking de área local.

A finales de 1999 e inicios del 2000 la IEEE lanza los estándares 802.11b y 802.11a, cada uno con características diferentes, el primero se basaba en modulaciones QPSK alcanzando velocidades de hasta 11 mbps en frecuencias de 2.4 Ghz y el segundo empezó a utilizar QAM con velocidades de 54 mbps en frecuencias de 5 Ghz lo que no lo hacía compatible con los predecesores. Posteriormente en junio del 2003 se ratificó un tercer estándar siendo este el 802.11g que de igual forma que el “b” utilizaba el espectro de los 2.4 Ghz, transmitiendo a velocidades de 54 Mbps utilizando modulación QAM y OFDM para la tasa de transmisión y uso de canal.

Luego del estándar “g”, en enero del 2004, la IEEE nombró un comité para el desarrollo de un nuevo estándar que utilice velocidades de hasta 600 Mbps utilizando modulaciones de tipo OFDM, MIMO, y 64QAM, no fue hasta el 2007 que se conoció a 802.11n que incorporó grandes mejoras sobretodo en la cobertura, diversidad de frecuencia y capacidad de alto reconocimiento multiruta, además se incorporó la característica de dual band donde permitía trabajar con 2.4 Ghz y 5Ghz.

Finalmente, entre los años 2011 a 2013 fue desarrollado una nueva versión del estándar 802.11 denominándolo “ac”, conocidos por algunos como wifi gigabit o wifi 5g por su velocidad de hasta 433 Mbps en flujo de información y llegando teóricamente hasta 3.5 Gbps. Con ancho de canal de 160 Mhz y utilizando 256QAM.

Posteriormente, el estándar IEEE 802.11ax, conocido comercialmente como Wi-Fi 6 y Wi-Fi 6E cuando opera en la banda de 6 GHz, incorporó mejoras orientadas a entornos de alta densidad mediante OFDMA, MU-MIMO, 1024-QAM, Target Wake Time y reutilización espacial, optimizando la eficiencia espectral, la latencia y el consumo energético. Más recientemente, IEEE 802.11be, denominado Wi-Fi 7, amplía estas capacidades con el enfoque Extremely High Throughput, operación en bandas de 2,4, 5 y 6 GHz,

mejoras sobre OFDMA y soporte para aplicaciones sensibles a la latencia, con modos orientados a alcanzar al menos 30 Gbps de rendimiento máximo (Qadri et al., 2022).

Tabla 2

Evolución de las redes 802.11

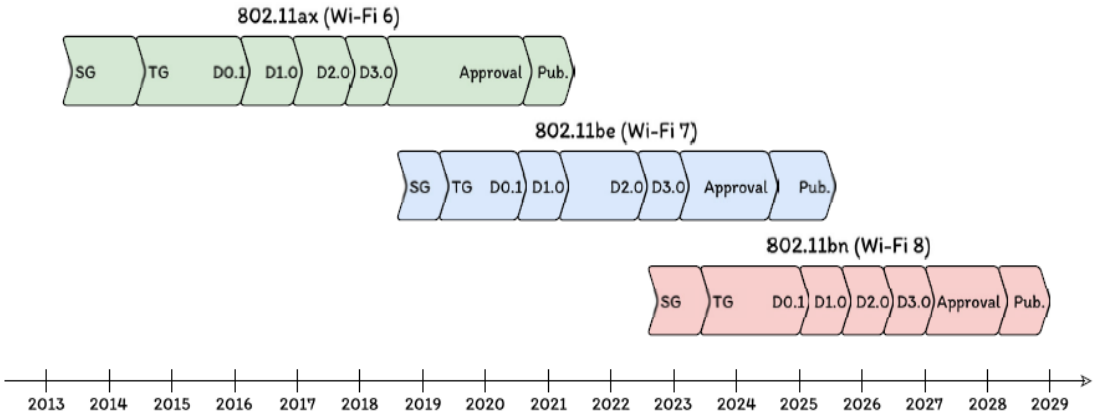
Estándar IEEE	Denominación	Bandas y canales	Características técnicas principales
802.11n	Wi-Fi 4	2,4 GHz y 5 GHz; canales de 20 y 40 MHz	OFDM, MIMO, 64-QAM, hasta cuatro flujos espaciales y tasa máxima teórica de 600 Mbps; incorpora agregación A-MSDU/A-MPDU.La cobertura supera los estándares anteriore
802.11ac	Wi-Fi 5	5 GHz; canales de 20, 40, 80 y 160 MHz	Modulación 256-QAM, beamforming explícito y MU-MIMO limitado al enlace descendente; Adite 8 flujos espaciales en el equipo con tasas de hasta 6.9 Gbps teórico
802.11ax	Wi-Fi 6 / Wi-Fi 6E	2,4 GHz y 5 GHz; Wi-Fi 6E amplía operación a 6 GHz; canales hasta 160 MHz	OFDMA y MU-MIMO en ambos sentidos del enlace, 1024-QAM, BSS Coloring, Target Wake Time y reutilización espacial. Su ganancia se concentra en eficiencia y latencia bajo alta densidad de usuarios.
802.11be	Wi-Fi 7	2,4 GHz, 5 GHz y 6 GHz; canales de hasta 320 MHz	Extremely High Throughput con modulación 4096-QAM, Multi-Link Operation, Multi-RU, puncturing de canal y hasta 16 flujos espaciales. Apunta a cargas de alta demanda que exigen capacidad agregada y latencia acotada.

Nota. Elaboración propia basada en la imagen obtenida de IEEE 802.11n e IEEE 802.11ac y en artículos de (Mozaffariahrar et al., 2022; Qadri et al., 2022).

Sin importar el estándar que se utilice las vulnerabilidades inalámbricas en los protocolos de encriptación y autenticación se mantienen dado las características de WEP Y WPA, aunque se realizan mejoras de seguridad, el principal hueco de seguridad se da por el lado del usuario.

Figura 1

Cronograma de desarrollo de las modificaciones estándar



Nota. Tomado de “A Tutorial on Wi-Fi 8: The Journey to Ultra High Reliability” (p. 172), por (Karamyshev et al., 2025), Problems of Information Transmission, 61(2), 164–210. Licencia CC BY 4.0.

La Figura 1 presenta la línea de tiempo de desarrollo de las enmiendas IEEE 802.11ax, IEEE 802.11be e IEEE 802.11bn, asociadas respectivamente con Wi-Fi 6, Wi-Fi 7 y Wi-Fi 8. En ella se observa la evolución progresiva de cada generación, desde la conformación del grupo de estudio y grupo de trabajo, hasta las etapas de borradores, aprobación y publicación. Esta representación permite evidenciar que Wi-Fi 6 y Wi-Fi 7 corresponden a tecnologías ya consolidadas, mientras que Wi-Fi 8 se encuentra en proceso de estandarización, orientado a mejorar la confiabilidad, latencia, eficiencia y desempeño de las redes WLAN futuras.

2.3 Topologías de las Redes Inalámbricas 802.11

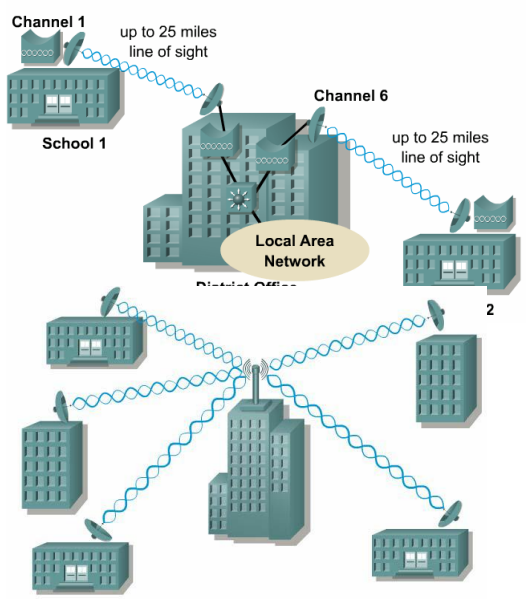
Cuando pensamos en seguridad de acceso es fundamental conocer las arquitecturas y topologías con las que el usuario final se enfrenta ya que el atacante hará un previo estudio para saber si se debe atacar, un AP, un repetidor, un WGB, o penetrar el Wireless controller, además de conocer si existen sistemas redundantes y de standby que también deben ser asegurados y fortalecidos para evitar la intrusión, por ello se estudian varias cualidades de las topologías Wireless lan.

2.3.1. Categorías de las Wireless Lan

Wi-Fi 7, basado en el estándar IEEE 802.11be, representa una de las generaciones más recientes de tecnologías de red inalámbrica orientadas a incrementar la capacidad, eficiencia y rendimiento de las comunicaciones WLAN. Esta generación se fundamenta en el enfoque Extremely High Throughput y contempla mejoras como mayor ancho de canal, modulación de orden superior, operación multi-enlace, gestión avanzada de calidad de servicio y mecanismos orientados a reducir la latencia en aplicaciones de alta demanda, como video 4K/8K, realidad aumentada, realidad virtual, IoT industrial y colaboración en tiempo real (Chen et al., 2022).

Figura 2

Categorización de las redes 802.11



Nota. Adaptado de *Fundamentals of Wireless LANs*, por (Cisco Systems, 2009), p. 96.

De acuerdo con la Figura 2, las topologías ofrecidas por las redes de este tipo son las LANs inalámbricas en el interior de un edificio u hogar y las Bridging inalámbrico de edificio a edificio

2.3.2. Redes Wireless Workgroup Bridge (WGB)

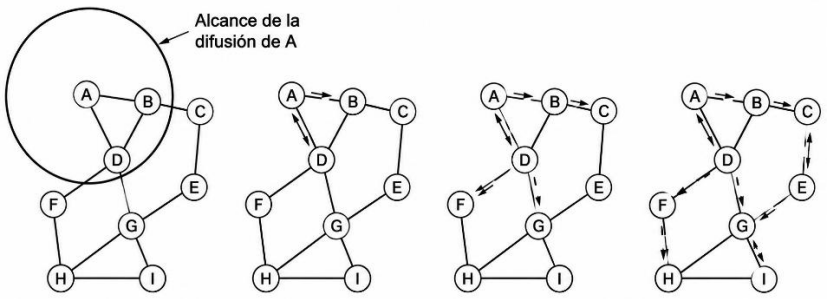
Los puentes de grupo de trabajo o *Workgroup Bridge* (WGB) permiten extender la conectividad de una red inalámbrica hacia dispositivos cableados que no cuentan con adaptador Wi-Fi. En esta modalidad, un punto de acceso configurado como WGB se asocia a otro punto de acceso como si fuera un cliente inalámbrico y proporciona conectividad a los dispositivos conectados a su puerto Ethernet. De esta manera, los equipos cableados pueden acceder a la WLAN a través del enlace inalámbrico establecido entre el WGB y el punto de acceso raíz, lo que resulta útil en escenarios donde no es factible instalar cableado físico, en extensiones de red para dispositivos separados físicamente o en aplicaciones móviles e industriales (Cisco Systems, 2023).

2.3.3. WLAN ad hoc

También conocida como peer to peer, es la configuración más sencilla y simple, tan solo basta con tener un adaptador en el equipo es posible configurarlo y comunicar equipos entre sí. Esta topología puede ser usada fácilmente en una pequeña oficina o incluso en el hogar para compartir archivos. El problema más grave es la cobertura y depende de la cantidad de equipos para escalar y extenderse, además de requerir algoritmos complejos de enrutamiento. En esta área se han desarrollado múltiples investigaciones a fin de proveer servicios estables cuando no se cuenta con un equipo intermediario administrador de las conexiones y sesiones, donde el fin que persigue es proveer disponibilidad a nivel de redes wifi en móviles para ayuda en casos de desastres y no se cuenta con una infraestructura inmediata.

Figura 3

Celdas Ad Hoc



Nota. Tomado de Redes de computadoras (5.ª ed., p. 335), por Tanenbaum et al., 2012), Pearson

La Figura 3 aporta sustento teórico al concepto de WLAN ad hoc, al representar cómo los nodos de una red inalámbrica pueden comunicarse sin depender de un punto de acceso o equipo centralizado. En este tipo de arquitectura, cada estación actúa como participante de la red y, cuando el destino no se encuentra dentro del alcance directo de transmisión, la información debe propagarse mediante nodos intermedios. Por ello, la figura permite comprender que la cobertura, la disponibilidad y la eficiencia de una red ad hoc dependen de la ubicación de los dispositivos, del alcance de difusión y de los mecanismos de enrutamiento utilizados para mantener la comunicación entre estaciones móviles.

2.3.4. Arquitectura Lógica

Se pueden dividir en varias arquitecturas de acuerdo con la interoperabilidad de los usuarios y de los equipos Access Point entre sí para brindar una experiencia de movilidad transparente al usuario.

Las arquitecturas BSS, IBSS, DS y ESS son fundamentales para comprender la organización lógica de las redes inalámbricas IEEE 802.11. Un Basic Service Set (BSS) representa el conjunto básico de estaciones que se comunican dentro de una WLAN; en modo infraestructura, estas estaciones se asocian a un punto de acceso que coordina la conectividad inalámbrica. Por su parte, el Independent Basic Service Set (IBSS) permite la comunicación directa entre estaciones sin depender de un punto de acceso, por lo que se asocia con redes ad hoc o configuraciones temporales de comunicación inalámbrica (Institute of Electrical and Electronics Engineers [IEEE], 2021).

El Distribution System (DS) permite interconectar diferentes BSS mediante puntos de acceso, facilitando el tránsito de datos entre segmentos inalámbricos y la red de distribución. Cuando varios BSS se integran a través de un mismo sistema de distribución, se conforma un Extended Service Set (ESS), lo que permite ampliar la cobertura WLAN y ofrecer continuidad de servicio en redes empresariales, institucionales o de mayor extensión. En estudios recientes sobre tecnologías WLAN, estas arquitecturas se consideran configuraciones relevantes para evaluar el desempeño de servicios concurrentes sobre redes IEEE 802.11, especialmente al comparar escenarios BSS, ESS e IBSS (Ali et al., 2023).

La primera de ellas es la arquitectura “BSS” conocida como conjunto de servicios básicos, se basa en un equipo central que provee conectividad a las STA (estaciones base) dentro de un área única de cobertura, a medida que se aleja de su AP su velocidad de transferencia disminuye, además un BSS contiene una única ID de servicios conocido como SSID.

La arquitectura “IBSS”, conjunto de servicios básicos independientes, es el tipo más básico de LAN IEEE 802.11. regularmente se las denomina así cuando dos equipos se conectan en modo ad-hoc.

También existe arquitectura de sistema de distribución DS ayuda a sobrellevar las limitaciones de cobertura que poseen las BSS debido a que a través de un backbone de servicios se conectan múltiples access point creando BSS adyacentes que comparten los mismos servicios y que pueden o no tener servicios de roaming y/o handover a nivel de celda wifi.

Finalmente tenemos la arquitectura “ESS”, conjunto de servicios extendidos, que se define a diferencia del anterior como varias BSS conectadas entre sí, pero no independientes, sino compartiendo los servicios y permitiendo el traspaso de una celda a otra manteniendo la sesión del usuario, para ello generalmente se hace uso de Wireless controller, sistemas que administran y gobiernan varios puntos de acceso permitiendo una administración centralizada e independiente.

Además de las arquitecturas ya mencionadas, podemos considera que existe una topología muy diferente a la ESS y WGB, ya que en la primera todos los equipos deben estar conectados en modo “AP” y en la segunda es un puente inalámbrico que a través del espectro electromagnético conecta un “AP” con un switch para extender una red cableada, por ello se puede considerar como otra topología a una WLAN con acceso a repetidores, donde la superposición entre celdas debe ser al menos del 50%, el usuario puede extender su red usando varios repetidores,

Cuando pensamos en seguridad de acceso es fundamental conocer las arquitecturas y topologías con las que el usuario final se enfrenta ya que el atacante hará un previo estudio para saber si se debe atacar, un AP, un repetidor, un WGB, o penetrar el Wireless controller, además de conocer si existen sistemas redundantes y de standby que también deben ser asegurados y fortalecidos para evitar la intrusión, por ello se estudian varias cualidades de las topologías Wireless lan.

La redundancia y el equilibrio de carga al ser parte de la topología deben ser estudiados para comprender su funcionamiento y poder protegerlos de las amenazas externas de acceso. Las topologías redundantes se utilizan cuando un AP no puede soportar el exceso de tráfico que genera la sobrecarga de clientes y por ello debe apoyarse en un segundo equipo para

balancear la carga. Por otro lado, las topologías de Standby permite garantizar la alta disponibilidad del servicio inalámbrico debido a que dos AP con configuraciones similares se encuentras instalados en el mismo sitio uno se encuentra activo y el otro están monitoreando el funcionamiento a la espera de que el AP principal falle para levantarse automáticamente y adoptar a los clientes para que no pierdan conectividad.

2.4 Especificaciones de las capas de acceso y física

Para proteger un equipo access point y a sus clientes es necesario comprender como es el proceso de asociación, que mecanismos a nivel de capa de enlace y física permiten que un usuario sea asociado a un AP y como este va a poder responder a las solicitudes de información y transmisión de datos e información de control.

2.4.1. Servicios LLC y MAC

La capa MAC y LLC proveen control de acceso al medio asegurando la interoperabilidad para servicios de la capa física y de las capas superiores respectivamente.

En redes WLAN, esta separación permite diferenciar las funciones de control lógico de enlace de aquellas asociadas a la transmisión inalámbrica, la administración del canal y los procedimientos definidos por la subcapa MAC de IEEE 802.11(Ficara et al., 2024). LLC no depende de la topología implementada, ni del medio de transmisión que se utilice, ni mucho menos de las técnicas de acceso al medio que se empleen.

Los servicios que provee la capa MAC son básicamente tres descritos a continuación:

1. Servicio de datos asíncronos
2. Servicios de seguridad
3. Ordenamiento de MSDUs

El servicio de datos asíncronos permite intercambiar PDU de datos de los servicios MAC (MSDU), que no son otra cosa que control de acceso a los medios de comunicación para unidad de servicios de datos que permite determinar quién puede acceder al medio en cualquier momento a través de una función de coordinación, además es compatible con el proceso de

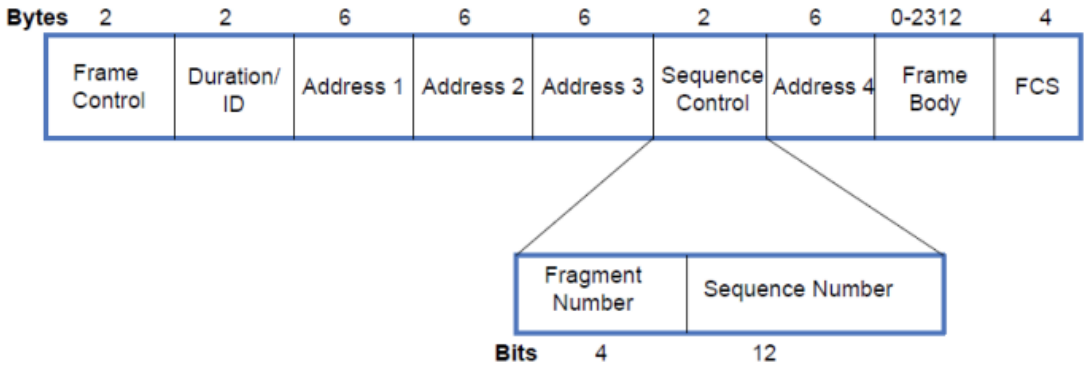
fragmentación cuando se requiere enviar PDU’s de mayor tamaño y con el cifrado que se utilice. Este mecanismo es basado en el mejor esfuerzo y sin conexión, eso quiere decir que no existen garantías de que esta sea entregada.

En este contexto, la función de coordinación distribuida, DCF, constituye el mecanismo base de acceso por contienda y se apoya en Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) junto con algoritmos de retroceso para reducir la probabilidad de colisiones. De forma complementaria, la función de coordinación puntual, PCF, se define como un mecanismo centralizado y opcional orientado a servicios libres de colisión y con restricciones temporales; sin embargo, DCF se mantiene como el método predominante de control de acceso al medio en redes WLAN IEEE 802.11 (Lin et al., 2023).

Estos esquemas de acceso son ineficientes para diferenciar la prioridad de los datos sobre todo cuando se utilizan datos multimedia como voz y video, por ello fue necesario que se realice una enmienda al estándar IEEE 802.11e para agregarle un nivel aceptable de QoS para multimedia, este estándar propone una función de coordinación híbrida HCF, que utiliza un método de acceso basado en contención EDCA, tiene la capacidad de operar simultáneamente con un sondeo basado en acceso HCF controlado (HCCA). Además, agrega la transmisión por oportunidad TXOP que es un intervalo de tiempo donde se produce un envío masivo de múltiples tramas para acelerar el envío y utilizar acuses de recibo basado en lotes.

Figura 4

Formato de Trama MAC 802.11



Nota. Adaptado de IEEE standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications (IEEE Std 802.11-2020), por.Institute of Electrical and Electronics Engineers [IEEE], 2020

Los servicios de seguridad de IEEE 802.11 se basan en la permisión o denegación del intercambio de datos de una STA a otra, para ello se realiza el cifrado de la MSDU en el caso de los mecanismos de privacidad equivalente al cableado (WEP), este se visualiza como servicio de LLC pero que se encuentra ubicado dentro de la capa MAC.

Las estaciones de trabajo, para transmitir cualquier tipo de información previamente deben construir una PDU de MAC conocida como unidad de datos del protocolo MPDUs o también llamados frames; estos frames están compuestos de un encabezados MAC, el cuerpo es de longitud variables y una secuencia de verificación FCS.

Cada tipo de frame tiene una función específica, los frame de datos son destinados al envío de la información, los frame de control para el establecimiento de sesiones y solicitudes de uso de canal a través de paquetes RTS, CTS, y finalmente los frame de administración que no contiene información de las capas superiores ni la envía a ellas, solo realiza funciones de background con el cliente, como por ejemplo el anuncio de la disponibilidad de la red.

Otro de los servicios de MAC es el uso de las técnicas de acceso, para lo cual utilizan CSMA/CA, que realiza la función de coordinación entre la transmisión de los usuarios y los subcanales disponibles dentro del espectro utilizado. Para ello hace uso de dos paquetes, Request to Send (RTS) que

notifica al access point de la solicitud de transmisión de la STA, luego de verificar la disponibilidad de canal, ejecuta un Clear to Send (CTS) para liberar o “limpiar” ese subcanal permitiendo al usuario la transmisión por él.

2.4.2. Servicios de la Capa PHY

El complemento a todas las operaciones que ocurren en la capa MAC es la presenta capa PHY que contiene tres elementos funcionales.

- Procedimiento de convergencia de la capa física (PLCP), que permite adaptar las capacidades dependiendo de qué medio físico se esté utilizando
- Sistema dependiente del medio físico (PMD), se encarga de definir qué características tiene el medio inalámbrico, así como los métodos de transmisión y recepción a utilizar para transmitir entre dos o más estaciones
- Administración de las funciones de la capa

Además, la capa física especifica las diferentes técnicas de modulación que permiten el uso de diversos canales FHSS, DSSS OFDM, así como las modulaciones para el envío de datos como BPSK, QPSK y QAM.

2.4.3. Estándares IEEE 802.11

Dentro de los dos niveles inferiores de la capa OSI mostrados anteriormente, física y enlace de datos con el uso de MAC y LLC, se definen las normas de funcionamiento de una Wireless lan, para ello se describen los protocolos 802.X para redes de área local y metropolitanas.

- 802.11a: Define la operación sobre frecuencias de 5GHz, a velocidades de 54Mbps
- 802.11ac La mejora actual a los protocolos 802.11 permitiendo velocidades superiores a 1.3 Gbps e introduciendo 256 QAM
- 802.11b: Define la operación sobre frecuencias de 2.4GHz, a velocidades de 11Mbps

- 802.11d: Complemento del 802.11 que permite el uso internacional de las WLAN para el uso de frecuencias de acuerdo al país
- 802.11e: Añade características de Quality of Service (QoS) y de soporte multimedia manteniendo la compatibilidad.
- 802.11f: Define el protocolo Inter-Access Point Protocol (IAPP) para que los usuarios puedan mantener la itinerancia y compatibilidad entre distintos proveedores de puntos de accesos.
- 802.11g: Define la operación sobre frecuencias 2.4GHz, a velocidades de 54Mbps
- 802.11h: Ayuda a la coexistencia de las redes WLAN con los sistemas de radares y satelitales debido a que las bandas de 5 Ghz tienen diferentes aplicaciones como el uso militar. Dynamic Frequency Selection (DFS) averígua si existe interferencias de canal, además Transmit Power Control (TPC) controla y regula la potencia de acuerdo a la región.
- 802.11i: Define mejoras en los procesos de encriptación y autenticación agregando seguridad.
- 802.11j: Es similar a la regulación que realiza 802.11h pero para Japón en canales (4.9-5.1 GHz)
- 802.11k: Mejora la administración de la frecuencia del cliente, se lo implementa en software.
- 802.11n: Define la operación sobre frecuencias 2.4GHz/5Ghz, a velocidades de 600Mbps teórico, agregando MIMO
- 802.11 p Estándar destinado para la operación en frecuencias de 5.90 y de 6.20 para sistemas de automóviles y carreteras.
- 802.11ax: Corresponde a Wi-Fi 6 y Wi-Fi 6E. Define mejoras de eficiencia para redes WLAN de alta densidad mediante

operación de alta eficiencia en la capa PHY y la subcapa MAC. Incorpora tecnologías como OFDMA, MU-MIMO, 1024-QAM, BSS Coloring y Target Wake Time (TWT). Opera en las bandas de 2,4 GHz y 5 GHz; en el caso de Wi-Fi 6E, extiende su operación a la banda de 6 GHz.

- 802.11be: Corresponde a Wi-Fi 7 y se orienta al enfoque Extremely High Throughput (EHT). Define mejoras en la capa PHY y la subcapa MAC para alcanzar al menos un modo de operación con rendimiento máximo de 30 Gbit/s en el punto de acceso al servicio MAC. Incorpora canales de hasta 320 MHz, modulación 4096-QAM, Multi-Link Operation (MLO) y mejoras para reducir latencia, aumentar capacidad y mantener compatibilidad con dispositivos IEEE 802.11 heredados en las bandas de 2,4 GHz, 5 GHz y 6 GHz.

Aunque la familia IEEE 802.11 incluye diversas enmiendas adicionales y complementarias orientadas a funciones específicas, como itinerancia, gestión de radiofrecuencia, seguridad, calidad de servicio, redes vehiculares, operación regional y optimización del acceso inalámbrico, en este apartado se mencionan únicamente los estándares más representativos asociados con las tecnologías legacy y las generaciones actuales de Wi-Fi.

2.5 Técnicas de Modulación para 802.11

Las diversas técnicas de modulación permitieron explotar al máximo el espectro de frecuencias no licenciadas para WLAN evolucionando con el pasar de los años para lograr velocidades similares a las que ofrecen las redes ethernet tradicionales concebidas para trabajar sobre cobre, las codificaciones de chip’s permiten adherir mayor volumen de información y la agilidad de frecuencia mejoran la eficiencia del canal así como el ancho del mismo, además incorporan técnicas modernas que aprovechan los trayectos multirutas a través de la diversidad de espacio aprovechando las múltiples entradas y salidas a través del uso de simultaneo de varias antenas.

2.5.1. FHSS

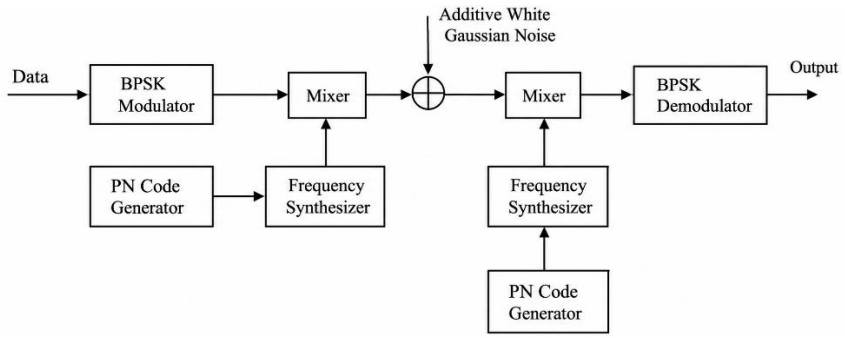
Es el primer método Spread Spectrum que se desarrolló para las

transmisiones WLAN, se establece una secuencia sincronizada para que al variarla el receptor pueda interpretar y decodificar la información.

Según de Curtò et al. (2024), Frequency Hopping Spread Spectrum (FHSS) es una técnica robusta de comunicación inalámbrica en la que la frecuencia portadora cambia rápidamente siguiendo una secuencia específica conocida por los dispositivos que participan en la comunicación. Este mecanismo permite distribuir la transmisión sobre diferentes frecuencias, aumentando la resistencia frente a interferencias y dificultando la interceptación de la señal. En el contexto de las primeras redes WLAN, FHSS constituyó una técnica de espectro ensanchado utilizada para organizar la transmisión inalámbrica mediante saltos de frecuencia sincronizados entre transmisor y receptor.

Figura 5

Diagrama de bloques funcional de FHSS



Nota. Tomado de “Design and Implementation of FHSS and DSSS for Secure Data Transmission” (p. 146), por (Hasan et al., 2015), International Journal of Signal Processing Systems, 4(2), 144–149.

2.5.2. DSSS

Esta tecnología se situaba en el rango de frecuencias de 900 Mhz donde su funcionamiento se basaba en el uso de todo el canal para obtener un solo canal rápido de 860 Kbps, cuando era necesario este canal se segmentaba en rangos más pequeños para obtener mayor número de ellos, pero las velocidades individuales eran más lentas.

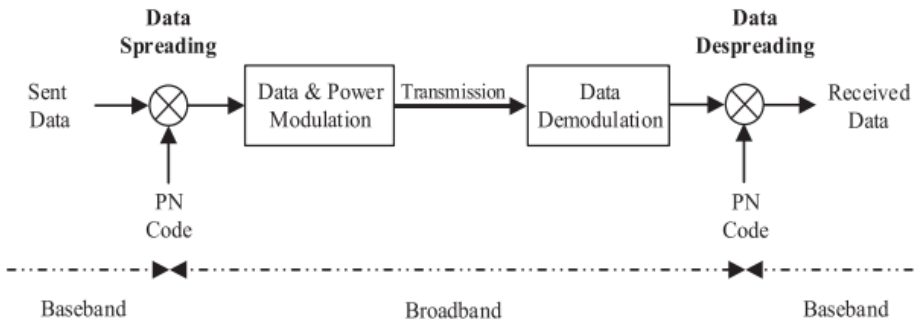
Según (Trînc et al., 2026), los sistemas tradicionales IEEE 802.11b empleaban Direct Sequence Spread Spectrum (DSSS) con un ancho de canal

aproximado de 22 MHz dentro de la banda de 2,4 GHz, mientras que estándares posteriores como IEEE 802.11g e IEEE 802.11n adoptaron OFDM con un ancho efectivo de 20 MHz. Debido a que los canales en 2,4 GHz se encuentran separados por 5 MHz, el uso de DSSS en 802.11b genera superposición entre canales adyacentes, por lo que, en la práctica, los canales 1, 6 y 11 suelen considerarse como los principales canales no superpuestos para reducir la interferencia en redes WLAN cercanas.

En el método Direct Sequence Spread Spectrum “una señal se genera a partir de la multiplicación de una señal de información y una secuencia pseudoaleatoria”

Figura 6

Diagrama de bloques funcional de DSSS



Nota. Tomado de “Direct Sequence Spread Spectrum-Based PWM Strategy for Harmonic Reduction and Communication, por (Wang et al., 2017), IEEE Transactions on Power Electronics, 32(6),

Uno de los problemas que enfrenta este tipo de modulación es la superposición de canales debido a que están separados por 5 Mhz, teniendo 22 Mhz lo cual los hace estar contiguos e interferidos.

2.5.3. OFDM

Este tipo de modulación se basa en el multiplexado por división de frecuencia ortogonal y permite alcanzar velocidades superiores a 54 Mbps. Su esquema de funcionamiento consiste en dividir una señal portadora de datos de alta velocidad en múltiples subportadoras de velocidad más pequeña que permiten la transmisión en paralelo.

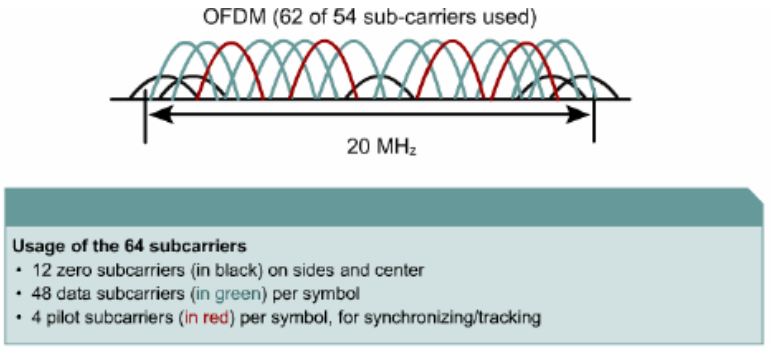
Según Farej & Ali (2021), en el análisis del rendimiento de IEEE

802.11ac, un canal de 20 MHz considera 52 subportadoras OFDM para el cálculo de la transmisión, mientras que Ko y Wang (2024) precisan que en sistemas IEEE 802.11 basados en OFDM existen subportadoras piloto destinadas al seguimiento y estimación del canal. En consecuencia, en las implementaciones OFDM heredadas de IEEE 802.11, la portadora de 20 MHz se organiza mediante subportadoras ortogonales, de las cuales una parte se emplea para datos y otra para funciones piloto, lo que permite mantener la sincronización y mejorar la recepción frente a variaciones del canal inalámbrico.

Según Harkat et al. (2022), los sistemas MIMO-OFDM constituyen una tecnología relevante en comunicaciones inalámbricas modernas, debido a que combinan transmisión multiportadora con arreglos de múltiples antenas. OFDM emplea procesamiento IFFT en el transmisor y FFT en el receptor, junto con prefijo cíclico, lo que facilita la demodulación, la ecualización en el dominio de la frecuencia y la mitigación de interferencias intersimbólicas e interportadoras en canales selectivos o con propagación multicamino, en la figura 7 se muestran el espectro de canales utilizados por OFDM en redes wifi.

Figura 7

Sistema de canales OFDM para wifi



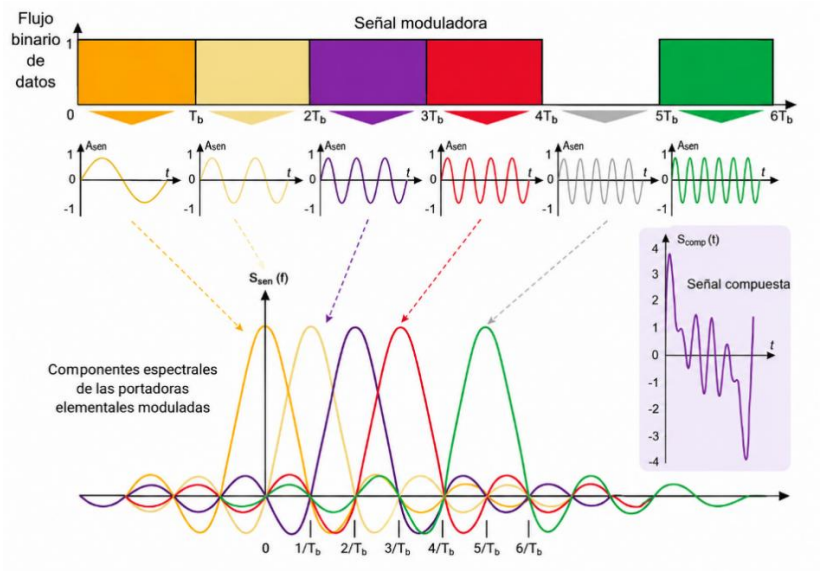
Nota. Tomado de Fundamentals of Wireless LANs (p. 52), por Cisco Systems, 2009.

El uso de COFDM ayuda a lograr velocidades de datos más altas con un sistema eficiente de recuperación de señales dispersas por el fenómeno de reflexión multiruta apoyado en métodos de corrección de errores en el

receptor.

Figura 8

Sistema de modulación OFDM



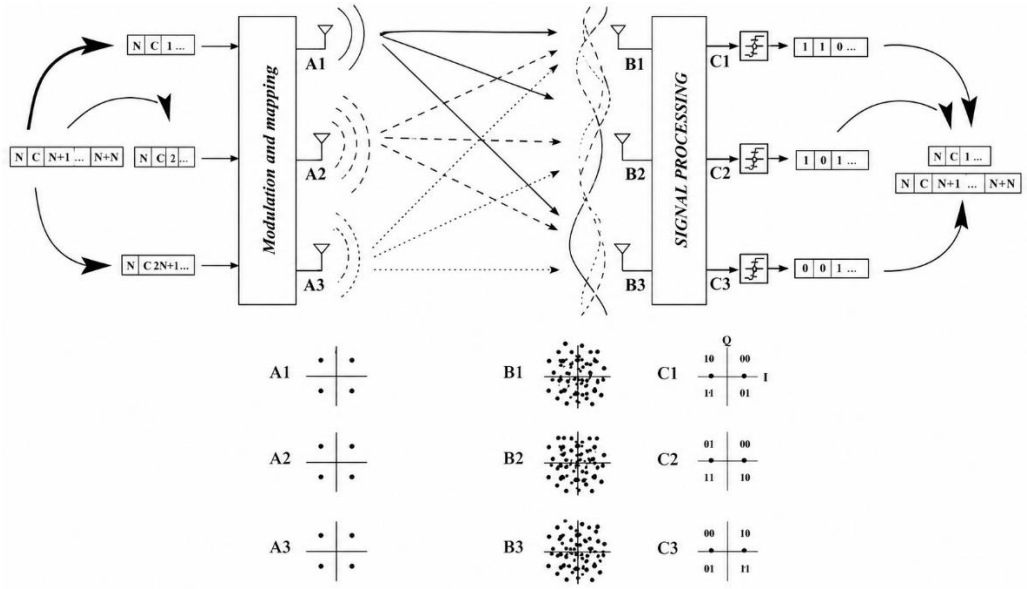
Nota. Tomado de Sistemas de Radiocomunicaciones, por Ramón, 2015, Ediciones Paraninfo.

La Figura 8 muestra como funciona OFDM utilizando la modulación por división de frecuencia ortogonal para que los flujos de datos binarios puedan dividirse por todo el espectro usando varias portadoras elementales.

Como se evidencia en la figura 9, OFDM se apoya aprovechan las bondades de la técnica de múltiple entrada múltiple salida MIMO debido a que es una tecnología que aprovecha los fenómenos físicos que genera la reflexión como el trayecto multiruta para aumentar la tasa de transmisión. En un enlace con N antenas transmisoras y M receptoras donde cada antena responde a su par, a través de un camino de desvanecimiento que se degrada por diversos factores como el ruido y la distancia, se introducen conceptos de mejoramiento que mejora la estadística de desvanecimiento utilizando técnicas de diversidad temporal, de espacio y espectral.

Figura 9

Diversidad MIMO



Nota. Adaptado de “Guide to Understanding MIMO”, por Telco Antennas Pty Ltd, s. f., https://www.telcoantennas.com.au/site/how-does-mimo-work

2.6 Seguridad en WLAN

La seguridad inalámbrica es uno de los principales tópicos que deben ser mejorados permanentemente, se requieren actualizaciones periódicas que blinden los mecanismos de acceso debido a que el medio de transmisión es compartido y muchos dispositivos tienen la capacidad de acceder buscando autenticarse para poder ingresar, de ello nace la inquietud de preguntarse, si los datos se envían por el espacio abierto como se podría garantizar la confidencialidad e integridad de estos.

El estándar IEEE 802.11 ofrece diversos mecanismos que incorporan seguridad de acceso, autenticación y encriptación, además es responsabilidad del administrador impulsar políticas y manuales de buenas prácticas que ayudan a concientizar al usuario de las estrategias y cuidados que debe toma al configurar y/o acceder a una red wifi.

En función de lo anterior, el desarrollo del apartado de seguridad en WLAN se organizará siguiendo una secuencia conceptual que permita comprender primero el origen del problema y, posteriormente, los mecanismos de protección aplicables. Finalmente, se establecerá una comparación de la seguridad en Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7, para sustentar estrategias de prevención, detección y mitigación orientadas al fortalecimiento

de la seguridad de acceso en entornos WLAN actuales.

2.6.1. Tipos de amenazas en redes 802.11Cuando el administrador omite cambiar los parámetros

La clasificación de las amenazas a las redes inalámbricas se divide en dos grandes grupos, primero por su nivel de conocimiento, destreza y experiencia en aplicar o desarrollar herramientas con fines de acceso al dispositivo, a sus usuarios o perturbación de las comunicaciones. Y el segundo grupo depende del lugar de donde proviene la amenaza, ya sea interna a la empresa o externa a ella.

Para clasificar las amenazas desde la perspectiva técnica del atacante se segmentarán en cuatro grandes categorías: snooping, modificación, enmascaramiento y denegación de servicio.

Snooping, acceso a la información que es de propiedad de la empresa o individuo con fines de beneficio personal, en este tipo de ataque es necesario que el intruso conozca la clave de cifrado de los mensajes.

Modificación, permite que el atacante intercepte los mensajes enviados con el propósito de cambiar los campos del paquete IP o de las tramas para redireccionar la información a otro destinatario, o modificar direcciones físicas o lógicas para lograr acceder a la red.

Enmascaramiento, basado en la suplantación de identidad, el intruso utiliza credenciales falsas para robar sesiones y acceder a la red.

Denegación de Servicio, consiste en determinar las vulnerabilidades que pueda tener la red y a partir de ello lanzar ataques que busquen inhabilitar los servicios críticos de la red al punto de dejarlo sin operatividad, las redes inalámbricas son blanco del jamming a través de la anulación de su frecuencia para denegar el servicio de la red.

Detrás de las amenazas que rodean a las redes wifi se encuentran diferentes tipos de atacantes que usan diversas técnicas para lograr acceder a las redes con fines diversos, a continuación, se describen los principales tipos de atacantes.

Según Rosales et al. (2022), un hacker es "un experto en informática que utiliza sus habilidades para mejorar la seguridad informática y la

privacidad, mientras que un cracker utiliza sus habilidades para violar la seguridad informática" (p. 6).

Por su parte Soltani et al. (2021) menciona, "los crackers son individuos con conocimientos avanzados en informática y habilidades para acceder a sistemas informáticos sin autorización y con fines malintencionados" (p. 55).

Un sniffer es un tipo de ataque informático muy común en redes inalámbricas y ataques de tipo war driving, donde el atacante escucha las tramas administrativas de conexión de los equipos AP y logra acceder al tráfico que pudiese comprometer la seguridad o acceder a pistas que le permiten identificar vulnerabilidades de acceso o ataques de desautenticación y suplantación. De acuerdo con Joseph et al. (2024), las herramientas de sniffing de paquetes son comúnmente utilizadas por los hacker para monitorear y husmear el tráfico de la red afin de detectar problemas por vulnerabilidades y de esta forma se mejoren las políticas de seguridad

Se suele utilizar el término de Lamer para encacillar en este término a todo individuo que realice actividades ilegales como hacking o phishing con el objetivo de obtener beneficios personales o causar perjuicios. Estos individuos a menudo utilizan herramientas y técnicas disponibles públicamente para llevar a cabo sus acciones delictivas. Esta palabra se origina a partir de la unión de las palabras "lamer" (un término en inglés que se refiere a alguien sin habilidades en un juego en línea) y "hacker". Adaptado de (Al-Saggaf et al., 2020). A continuación, se resume la tipología de las amenazas en la tabla 3.

Tabla 3

Tipología de amenazas en redes IEEE 802.11

Tipo de amenaza	Descripción conceptual	Manifestación en redes WLAN	Impacto principal
Snooping	Analiza el tráfico que fluye por la red sin modificarlo.	Analiza paquete de administración.	Podría obtener claves o credenciales
Modificación o alteración del tráfico	Manipulación de datos, tramas o parámetros de comunicación con el fin de cambiar el comportamiento normal del intercambio de información.	Alteración de paquetes, redirección de tráfico, manipulación de sesiones o degradación de mecanismos de seguridad.	Afectación de la integridad de los datos, pérdida de confianza en la comunicación y posibilidad de acceso no autorizado.

Tipo de amenaza	Descripción conceptual	Manifestación en redes WLAN	Impacto principal
Enmascaramiento o suplantación de identidad	Situación en la que un atacante aparenta ser un usuario, dispositivo, punto de acceso o servicio legítimo dentro de la red.	Suplantación de SSDI o direcciones físicas	Acceso indebido y escalamiento de privilegios
Ataques de autenticación	A través de diversos mecanismos provoca que los usuarios expongan sus credenciales	Principalmente mediante ataques de diccionario o fuerza bruta, además de debilidades en la reasociación	Acceso al dispositivo y a la red
Ataques de cifrado	Explota vulnerabilidades en la encriptación.	Uso de protocolos en versiones obsoleta.	Vulnera la confidencialidad
DoS	Ataque que afecta a la disponibilidad del servicio wifi	A través de interferencia o saturación del espectro	No disponibilidad del servicio
Debilidad en configuraciones	Omisión de cambio en parámetros configurados por defecto	Mantener servicios innecesarios activados o uso de versiones obsoletas	Amplifica las posibilidades de ataques de acceso

Nota. Elaboración propia con base en la clasificación de amenazas de disponibilidad, datos, malware e ingeniería social presentada por European Union Agency for Cybersecurity (2024), el uso dual de herramientas de captura y análisis de paquetes descrito por Joseph et al. (2024), la revisión de vulnerabilidades y ataques asociados a WPA3 desarrollada por Halbouni et al., (2023), y el análisis de ataques de downgrade en redes WPA3 propuesto por Tareef et al., (2025).

Para el presente estudio se tomarán en cuenta las vulnerabilidades en el acceso y las técnicas empleadas para autenticarse en una red wifi por encima del tipo de amenaza, propósito o fin que persiga el intruso, sin embargo, es importante conocer de quienes provienen los ataques.

2.6.2. Principales riesgos de acceso en redes 802.11

Cuando pensamos en los riesgos de las redes wifi, debemos enfocarnos en aspectos fundamental que históricamente son blancos de explotación de los atacantes, la identificación del dispositivo es relativamente sencilla debido a que su nombre se anuncia mediante un SSID público, la autenticación del usuario debe ser externa al equipo y no centralizarse en él, la autorización de acceso debe ser responsabilidad de una entidad que valide que el usuario no está siendo suplantado, la configuración del AP debe realizarse a través de protocolos de acceso remoto seguro como SSH, gestión de credenciales debería ser responsabilidad del servidor AAA y la protección del tráfico se debe cifrar con una infraestructura PKI.

Por lo expuesto anteriormente es evidente que los riesgos no se limitan

a conseguir una contraseña que no es más que una llave de cifrado sino que la superficie de explotación es mucho más amplia y se maximiza debido a la fácil exposición de las redes wifi que aunque no sean visibles pueden estar disponibles más allá del entorno al cuál debe servir, a diferencia de las redes LAN, en Wi-Fi es difícil mantener el control del espectro de cobertura porque limitar el área podría significar afectar a la tasa de transmisión por ello es imperioso implementar controles más estrictos y configuraciones más robustas.

El principal riesgo es producto de la poca cultura de seguridad del personal, quienes acostumbran a utilizar contraseñas que no cumplen los estándares mínimos para su elección o por la ausencia de políticas de contraseña en las empresas que obliguen a renovarlas periódicamente y a convertir en corresponsables a los usuarios. Cuando no existen políticas de contraseñas no existirán credenciales con criterios mínimos permitidos de complejidad e incluso existirá exposición involuntaria de las claves escribir en notas de papel.

Una debilidad de los administradores es la de omitir cambiar los valores que se incluyen por defecto de fabrica en los equipos, como por ejemplo, contraseñas y nombres de usuarios administradores, ip’s por defecto para administración comprometiendo las interfaces administrativas, además de evitar segmentar en redes vlan para usuarios públicos y privados para no mezclar el tráfico, además otro error común es no actualizar constantemente y parchar los equipos con los firmware más recientes que entregue el fabricante,

Al final pero no menos importante, es necesario realizar un monitoreo permanente de los equipos autenticados y la actividad que estos realizan desde los paneles de gestión que provea el fabricante en sus estaciones controladoras de AP´s, al existir equipos no solo informáticos o de comunicación, sino equipos IoT pueden abrir la puerta a la clonación de los mismo para ganar acceso comprometiendo la integridad de los usuarios, a continuación en la tabla 4 sintetizaremos los principales riesgos en las redes

Wi-Fi modernas.

Tabla 4

Principales riesgos de acceso y administración en redes Wi-Fi modernas

Riesgo de acceso	Condición que lo produce	Manifestación en redes Wi-Fi modernas	Efecto sobre la seguridad
Credenciales débiles, compartidas o expuestas	Uso de contraseñas sencillas	Acceso de usuarios no autorizados, pérdida de control sobre quién utiliza la WLAN y baja trazabilidad de conexiones.	Accesos no autorizados
Protocolos de administración del AP	Acceso a la plataforma de administración del equipo mediante ssh o la web.	Acceso al Wireless controller y equipos reconfigurándolos para convertirlos en vulnerables.	Integridad, disponibilidad y confidencialidad
Falta de gestión y monitoreo	No identificar a los usuarios de su red y perdida en la trazabilidad	Autenticación de clientes que no deben tener acceso	Expone a todos los usuarios y equipos y falta de control
WiFi publicas	Priorizar la facilidad de acceso	No existe control ni identificación de las intenciones de los usuarios conectados	Afecta a la confidencialidad
Falla del control de cobertura	El espectro de cobertura excede los límites del espacio permitido	Posibilidad de ser Snifeadas por atacantes	Compromete la privacidad
Ausencia de segmentación vlan	El tráfico de varios niveles de privacidad se mezcla	Movimiento lateral entre grupos de usuarios y escalamiento en privilegios	Acceso no autorizado, abuso de confianza
Uso de protocolos antiguos u obsoletos	Por facilidad de configuración se utilizan servicios que ya fueron reemplazados por versiones modernas	Protocolos de reasociación débiles y vulnerables	limita los beneficios de WPA3, SAE entre otros comprometiendo a la triada de seguridad.
Deficiente gestión de actualización de firmware y parches	Administradores no tienen un control de versiones	Persistencia de fallas conocidas, errores de implementación o debilidades corregidas por el fabricante.	Incrementa el riesgo de explotación de vulnerabilidades y afecta la disponibilidad e integridad del servicio.
Ausencia de monitoreo	No hay sistemas de gestión y monitoreo centralizado para identificar actividades sospechosas	Complejidad en la identificación y detección de actividades sospechosas o usuarios no autorizados	Degrada la capacidad de reacción e identificación de amenazas y reacción.
Ausencia de políticas y manual de buenas prácticas	Ausencia de normas sobre contraseñas, invitados, BYOD, IoT, redes públicas, administración, actualización y revocación de accesos.	La seguridad se basa en la confianza de que el usuario es capaz de evitar los riesgos y conoce de buenas prácticas	Deficiente gobernanza de la infraestructura

Nota. Elaboración propia. La tabla permite conocer los principales riesgos que exponen a las redes actuales identificando los efectos. Se fundamenta en estudios sobre contraseñas Wi-Fi, WPA3, sniffing de paquetes, degradación de seguridad y panorama de ciberamenazas recientes. European Union Agency for Cybersecurity, 2024; Halbouni et al., 2023; Joseph et al., 2024; Tareef et al., 2025; (Veroni et al., 2022).

De acuerdo con Kasana (2021) los riesgos de acceso más comunes reportados en la actualidad son: Interceptación de datos, ataques de phishing, malware, ataques Man-in-the-Middle, suplantación de identidad, configuración

insegura de la red, ataques de fuerza bruta, uso de redes wifi públicas, falta de actualizaciones de seguridad

Por otro lado, según TechNadu (2023), establece que el estándar 802.11 tienes varias vulnerabilidades y riesgos de seguridad a nivel de protocolos, entre los cuales se destacan los siguientes: uso de protocolos y servicios obsoletos, vulnerabilidades en el cifrado WPA2, ataques de desautenticación, rogue APs, ataques de inyección de paquetes, falta de actualizaciones de seguridad, configuración de red predeterminada

Las redes Wi-Fi públicas o de acceso compartido, comunes en lugares de afluencia masiva, están propensas a problemas de confidencialidad debido a que priorizan la facilidad de acceso por sobre la privacidad del usuario incrementando la superficie de los ataques por acceso indebido, lo usuarios acceden a través de un portal cautivo sin ninguna garantía de protección del tráfico que genere.

Los ataques identificados afectan a la triada de la seguridad, la confidencialidad nos garantiza través del cifrado que la información viaja sin ser identificada y aun que fuese interceptada esta es ilegible, la integridad por su parte se apoya en los principios del hashing para garantizar que la información no haya sido alterada desde su concepción hasta su recepción y la disponibilidad nos ayuda a conservar la accesibilidad a los recursos, estos elementos son los que garantizan una conexión fiable ante las amenazas identificadas anteriormente.

2.6.3. Vulnerabilidades, configuraciones inseguras y coexistencia con protocolos heredados

Las vulnerabilidades en redes WLAN se originan por diversas causas, principalmente técnicas, de administración y operación que afectan al control de acceso y gestión de usuarios. Se vuelve más complejo gracias al espectro electromagnético compartido donde es fácilmente censado por los dispositivos vecinos, por ello se considera una red de buen rendimiento, pero con muchas vulnerabilidades y puntos débiles que afectan a la seguridad.

La carente administración y gestión de puntos de acceso por parte de

los responsables de la infraestructura de AP, routers AP, controladores incrementa el vector de exposición. De acuerdo con la National Security Agency (2023) se sugiere la administración de parches y firmware actrualizados, además de usar handshake y preshared key robustas, sin omitir la segmentación y segregación de usuarios para minimizar el riesgo de exposición. Está claro que la seguridad de acceso no depende solo del protocolo elegido, sino también de cómo se configura y mantiene el entorno en el día a día.

Otra debilidad común y cuidado es la mantener protocolos obsoletos por pensar que al actualizarlos se perderá la compatibilidad. Usar WEP, WPA con TKIP o esquemas mixtos puede bajar el nivel de protección de toda la WLAN, incluso si hay dispositivos que ya soportan esquemas más modernos, se recomienda siempre el estudio y evaluación de los protocolos a configurar para tomar la decisión más acertada.

Con base en todo lo expuesto anteriormente podemos inferir que vulnerabilidades, configuraciones inseguras y dependencias heredadas amplían la superficie de exposición de las redes Wi-Fi sin importar la generación a la que perteneces y abren las puertas a los accesos no autorizados, pérdida de control administrativo, exposición del tráfico o una seguridad de acceso más débil en general. A continuación, la tabla 5 expone de forma resumida las vulnerabilidades de protocolos heredados.

Tabla 5

Vulnerabilidades, configuraciones inseguras y debilidades asociadas a protocolos heredados en WLAN

Categoría	Debilidad identificada	Impacto en la seguridad WLAN	Riesgo asociado	Consideración general de seguridad
Protocolo heredado	Uso de WEP	Protección obsoleta del tráfico inalámbrico.	Exposición de datos y control de acceso débil.	No es adecuado para WLAN actuales.
Protocolo heredado	Uso de WPA con TKIP	Compatibilidad antigua con menor nivel de seguridad.	Menor robustez del cifrado y de la confianza operativa.	Debe evaluarse como riesgo heredado.
Compatibilidad	Configuraciones mixtas WPA/WPA2	Expone el equipo con protocolos inseguros	Acceso por debilidades del protocolo	No active protocolos inseguros
Credenciales	Contraseñas PSK débiles	Acceso por fuerza bruta	Acceso indebido	Se requiere una entidad externa que valide la transacción

Categoría	Debilidad identificada	Impacto en la seguridad WLAN	Riesgo asociado	Consideración general de seguridad
Configuraciones por defecto	SSID y credenciales por defecto	Acceso a información del equipo o su configuración	Ataque de reconocimiento de acceso	Usar contraseñas fuertes que cumplan el estándar
Mantenimiento	Versiones antiguas de Firmware	Múltiples debilidades que afecta a la C+D+I	Amplifica la exposición	Debe existir una política de actualización
Configuración de protección	Protección de las tramas de control desactivada	No hay seguridad en el tráfico administrativo	Sniffin y acceso no autorizado a la administración	Se debe considerar su configuración
Control de acceso	Inexistencia de control de tramas fuerte	No existe garantía de que el usuaria sea quien dice ser	Dispositivos no autorizados o no confiables.	Requiere políticas de validación adecuadas.
Arquitectura de red	No existe división de redes	Tráfico mezclado sin identificación	Exposición de servicios	Estrategias de división por subredes.
Compatibilidad operativa	Existencia de dispositivos antiguas vulnerables	Protocolos inseguros y vulnerables	Facilidad en la explotación de vulnerabilidades en equipos heredados	Mantener protocolos actualizados

Nota. Elaboración propia con base en el análisis conceptual del apartado y en recomendaciones técnicas generales sobre actualización de equipos, administración interna, uso de WPA3/WPA2, frases de paso robustas, protección de administración inalámbrica y segmentación de redes planteadas por la National Security Agency (2023).

Como muestra la Tabla 5, las vulnerabilidades, configuraciones inseguras y protocolos heredados no son fallas aisladas: son condiciones que, juntas, amplían la superficie de exposición de las WLAN actuales. La presencia de mecanismos obsoletos, credenciales débiles, administración deficiente y poca segmentación puede debilitar el control del acceso inalámbrico y limitar qué tan efectiva resulta la seguridad implementada.

2.6.4. Ataques contra autenticación, cifrado e integridad en redes Wi-Fi

Los ataques contra autenticación, cifrado e integridad en redes Wi-Fi comprometen justamente los procesos que validan a los usuarios, protegen la comunicación y garantizan que los datos transmitidos sean confiables. En redes IEEE 802.11 esto ocupa un espacio mayor porque el medio inalámbrico facilita inspeccionar la negociación inicial de conexión y mostrar información asociada al acceso, sobre todo cuando hay credenciales sencillas y escuetas o configuraciones de seguridad deficientes.

En cuanto a la autenticación, los riesgos se deben explícitamente a la captura de paquetes de tipo handshakes, la reutilización de claves precompartidas, la simplicidad de las credenciales y los intentos recurrentes de recuperar password como un mecamismo de debilidad. No se considera a esto una falla técnica o una debilidad del protocolo sino un conjunto de estrategias previsibles para vulnerar contraseñas sencillas de baja complejidad.

Los ataques que tiene como objetivo acceder al cifrado buscan debilitar la protección del tráfico inalámbrico o aprovechar debilidades en las condiciones de negociación de parámetros que le den pistas del cifrado. Chalyi (2025) indica que las técnicas más utilizadas en WPA2 consisten simplemente en el escaneo de aire, identificación del BSSI objetivo y provocar ataques de desautenticación para que mientras ocurre la reautenticación se capture los paquetes de negociación donde incluye información para el acceso, además WP3 y WPS se ayudan de la captura de datos de autenticación y en ataques offline de diccionario, y que configuraciones mal hechas —como ciertos modos de compatibilidad— pueden dejar la red expuesta a ataques de downgrade.

En Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7, qué tan expuesta está la red a estos ataques depende de cómo se configuran el acceso, el cifrado y la compatibilidad. Mantener claves débiles y controles incompletos amplía la superficie de ataque, lo que permite a posterior realizar un análisis de protocolos, controles y estrategias de mitigación.

Tabla 6

Principales ataques contra autenticación, cifrado e integridad en redes Wi-Fi

Categoría del ataque	**Vector o debilidad aprovechada**	**Propiedad de seguridad afectada**	**Impacto en la seguridad WLAN**	**Consideración general de seguridad**
Captura de handshake	Exposición del intercambio inicial de autenticación o reasociación.	Autenticación de los usuarios	Afecta a la confianza	cifrar las tramas de gestión
Ataques de diccionario	Uso de palabras comunes	Autenticación.	Afecta al acceso no autorizado	Considerar autenticación de doble factor
Fuerza bruta	Contraseñas débiles	Gana acceso mediante autentización forzada.	Ralentización de la red y compromete la privacidad	Credenciales complejas y autenticación descentralizada
Ataques de downgrade	Uso de mecanismos heredado o antiguos	Autenticación y cifrado.	En todos los niveles de C+D+I	Evitar la coexistencia de servicios heredados
Reutilización de cuentas y password	Contraseñas secuencias y con patrones comunes	Autenticación y privacidad.	Debilidad en los accesos	Diseño de políticas de cuentas y password
Cifrado obsoleto	Algoritmos criptográficos en desuso	Confidencialidad e integridad.	En todos los niveles de C+D+I	Evitarse siempre.

Categoría del ataque	Vector o debilidad aprovechada	Propiedad de seguridad afectada	Impacto en la seguridad WLAN	Consideración general de seguridad
tráfico no autorizado	Inyección de paquetes ajenos ala red	Integridad.	Puede comprometer a la disponibilidad del servicio	Mantener consolas de gestión.
Reenvío o repetición de tramas	Afecta a protocolos de tres vías para capturar ese tráfico.	Integridad y autenticidad.	Complica el proceso de comunicación por duplicidad de tramas	Implementar mecanismos de protección de sesiones
Autenticación débil	Validación débil de las cuentas.	Autenticidad y control de acceso.	Acceso de usuarios ajenos.	Implementar esquemas de autenticación externa

Nota. Elaboración propia con base en el análisis conceptual de ataques contra autenticación, cifrado e integridad en redes Wi-Fi y en el estudio de Chalyi (2025) sobre protocolos WPA2, WPA3, WPS, captura de datos de autenticación, ataques de diccionario, fuerza bruta y riesgos de downgrade asociados a configuraciones impropias.

Como se muestra en la Tabla 6, los ataques contra autenticación, cifrado e integridad afectan directamente a las estrategias de acceso por errores mayoritariamente humanos y principalmente del administrador de los equipos inalámbricos, la exposición de tramas de acceso o el uso de credenciales, hasta la protección de las tramas de negociación deben ser planificadas dentro del plan de fortalecimiento del entorno inalámbrico, es necesario auditar estos requisitos y aplicar las recomendaciones sugeridas.

2.6.5. Suplantación, puntos de acceso falsos, Man-in-the-Middle y denegación de servicio

La suplantación en redes WLAN tiene que ver con la capacidad de un actor no autorizado para hacerse pasar por un usuario, dispositivo o componente legítimo de la infraestructura. En entornos IEEE 802.11 esto pesa especialmente porque el cliente necesita reconocer y confiar en el punto de acceso disponible antes de sumarse a la red. Por eso la identidad de la infraestructura inalámbrica es tan crítica para mantener la seguridad de acceso.

Los puntos de acceso falsos identificados como Rogue Ap o evil twin son las estrategias por excelencia más utilizadas en entornos públicos para la intercepción de usuario o clientes empresariales, suelen venir acompañados de ataques de phishing para los portales cautivos o técnicas de scareware que pretenden sorprender al usuario, son formas de engañar la confianza del usuario y del dispositivo cliente y de estar forma inducir al cliente a entregar

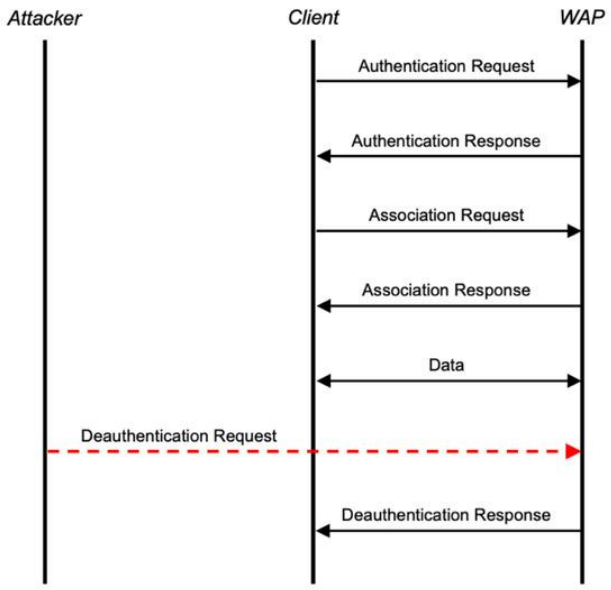
sus credenciales por el engaño del cuál es víctima. Por su parte Louca et al. (2023) manifiesta que principalmente los ataques Evil Twin Man-in-the-Middle se valen de mecanismos de itinerancia o de clientes que por urgencia buscan conectarse velozmente a puntos de accesos suplantados.

Los ataques Man-in-the-Middle implican que un tercero se interponga entre el cliente y el destino de la comunicación. Su importancia conceptual está en que rompen la confianza sobre el trayecto por el que viaja la información, y eso puede afectar la confidencialidad, la integridad y la autenticidad de la sesión. Este escenario deja claro que la seguridad WLAN depende también de cuán legítimo sea el punto de conexión utilizado.

La denegación de servicio en redes IEEE 802.11 golpea la disponibilidad del acceso inalámbrico a través de acciones que buscan degradar, interrumpir o directamente impedir la continuidad de la conexión. En una WLAN esto puede verse como pérdida de asociación, sesiones interrumpidas, rendimiento muy reducido o imposibilidad temporal de conectarse. Es un riesgo especialmente grave cuando la conectividad Wi-Fi sostiene procesos académicos, empresariales, sanitarios o industriales.

Figura 10

Escenario de configuración de un punto de acceso Evil Twin



Nota. Tomado de “WPFD: Active User-Side Detection of Evil Twins”, por F.-H. Hsu, M.-H. Wu, Y.-L. Hwang, C.-H. Lee, C.-S. Wang y T.-C. Chang, 2022, Applied Sciences, 12(16), 8088. https://doi.org/10.3390/app12168088. Licencia CC BY 4.0.

La Figura 10 muestra un escenario de punto de acceso falso tipo Evil Twin, donde un atacante monta una red inalámbrica fraudulenta que imita a la legítima para inducir a los usuarios a conectarse.

Se identifica cómo la confianza en el SSID o en la simple disponibilidad de una red puede explotarse para comprometer la autenticidad del acceso inalámbrico. Según Hsu et al. (2022), los métodos de de denegación Evil Twin pueden facilitar escenarios de intercepción y Man-in-the-Middle, sobre todo en redes Wi-Fi abiertas o públicas.

En conjunto, la suplantación, los puntos de acceso falsos, los escenarios Man-in-the-Middle y la denegación de servicio amplían la exposición de las redes inalámbricas porque afectan la identidad, la confianza en la infraestructura y la continuidad del acceso.

2.6.6. Principios de seguridad de acceso en redes IEEE 802.11

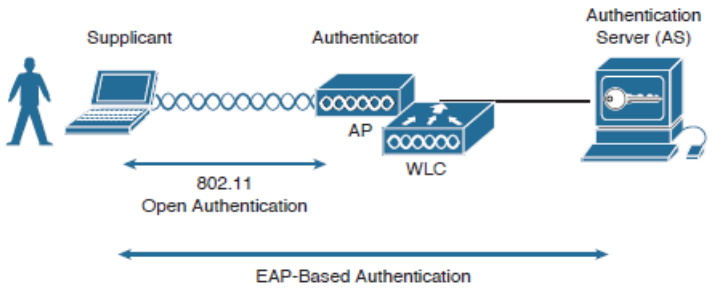
La seguridad en el acceso durante la autenticación en redes wifi aborda los elementos que seleccionan que usuarios pueden y deben conectarse y respetando que condiciones para el nivel de confianza al cuál le corresponde, no implica en tan solo negar el acceso a la conexión, sino exige validación de identidad, protección de las tramas de control para el intercambio de sesión y garantizar la estabilidad mientras la conexión se mantiene. El estándar IEEE 802.11 incorpora los elementos de acceso, autenticación y protección dentro de las redes WLAN (Institute of Electrical and Electronics Engineers [IEEE], 2021).

Aunque la triada incorpora a la confidencialidad, integridad y disponibilidad, se requiere establecer mecanismos seguros de autenticación del usuario, autorización de acceso, autenticidad de las credenciales, trazabilidad de los eventos que ocurren durante y después de su sesión, incorporar mínimo privilegio y defensa en profundidad y en la medida de lo posible respetar los principios de zero trust. Halbouni et al. (2023) informa y aconseja que WPA3, aunque incorpora mecanismos que mejora y fortalece la seguridad, este no elimina los problemas de seguridad que producto de una

mala implementación o configuración.

Figura 11

Proceso de autenticación 802.1X en una red WLAN empresarial



Nota. Tomado de CCNA Wireless 200-355 Official Cert Guide (Figura 14-7, "802.1x Client Authentication Roles"), por Hucaby, 2016, Cisco Press.

La Figura 11 representa el proceso lógico de autenticación 802.1X en una red WLAN empresarial, con tres entidades en juego: el supplicant o cliente inalámbrico, el authenticator (el punto de acceso o el controlador WLAN) y el servidor de autenticación. Este esquema ayuda a entender que la seguridad de acceso no se agota en la asociación inicial 802.11, hace falta una validación posterior de identidad antes de dejar usar los recursos de la red. Hucaby (2016) explica que, en 802.1X, el cliente puede asociarse al punto de acceso desde el principio, pero no transmite datos hacia la red hasta completar con éxito la autenticación mediante EAP y un servidor dedicado. En este modelo, mecanismos como 802.1X/EAP, WPA2/WPA3 empresarial, PEAP o EAP-TLS ponen en práctica los principios de autenticación, autorización, confidencialidad, integridad y trazabilidad, separando la conexión inalámbrica inicial de la validación formal de credenciales.

2.6.7. Protocolos de autenticación y cifrado WLAN: WPA2, WPA3, SAE y OWE

La seguridad WLAN pasó de mecanismos pensados solo para dar una privacidad básica a esquemas capaces de combinar autenticación, cifrado y control del acceso inalámbrico. En las redes IEEE 802.11 actuales, este cambio responde a la necesidad de validar dispositivos y usuarios antes de dejarlos usar la red, proteger el tráfico que circula por el medio radioeléctrico y reducir la exposición que traen las conexiones no autorizadas.

Los protocolos de autenticación y cifrado cumplen un papel estructural en la seguridad de acceso, porque conectan la identidad del cliente con la generación de material criptográfico y la protección posterior de la comunicación, aunque esto no depende tan solo de dicho proceso, ni del algoritmo desplegado, sino de como se establecen las reglas de asociación, autenticación, establecimiento de claves y protección del tráfico de datos entre el o los clientes y el AP durante el establecimiento de la asociación.

El algoritmo de cifrado que predominó durante muchos años fue WPA2 y se masifico en todos los dispositivos y en todas las implementaciones domésticas o empresariales, sin embargo su versión sucesora mejora el proceso de autenticación y reduce el impacto que provoca la exposición de contraseñas débiles, aunque a pesar de aquello su eficacia sigue dependiendo de los mecanismos utilizados al desplegarlo así como de la compatibilidad y los parámetros que se configuren para afinarlo al máximo de protección (Halbouni et al., 2023a).

SAE y OWE completan esta evolución desde dos necesidades distintas. SAE fortalece la autenticación en redes personales con un intercambio más resistente a la validación no autorizada de contraseñas, mientras que OWE aporta cifrado oportunista en redes abiertas sin exigir una clave compartida. Los dos refuerzan la protección del acceso, pero ninguno reemplaza una buena gestión de credenciales, identidad y políticas de uso inalámbrico.

Tabla 7

Comparación conceptual de WPA2, WPA3, SAE y OWE en la seguridad de acceso WLAN

Protocolo o mecanismo	Tipo de función	Estándar, certificación o entorno WLAN donde se utiliza	Cómo funciona o para qué sirve	Aporte a la seguridad de acceso	Limitaciones o consideraciones técnicas
WPA2	Autenticación y cifrado	Estándar IEEE 802.11i usado mundialmente por su compatibilidad	Provee autenticación y cifrado mediante el uso de una clave	Útil en entornos básicos	Vulnerable y dependiente del nivel de complejidad de la contraseña del usuario

WPA3	Autenticación y cifrado fortalecido	Usado en equipos modernos	Seguridad actualizada para la autenticación	Reduce la superficie del ataque cuando existen contraseñas débiles.	Depende de la compatibilidad con todos los equipos
SAE	Mecanismo de autenticación para redes personales.	Trabaja con WP3 cuando utilizan frases de paso	Requiere de autenticación mutua	Fortalece la autenticación de los clientes	Mantiene la necesidad de frases de paso.
OWE	Mecanismo de cifrado oportunista para redes abiertas.	Muy útil en redes Enhanced Open	Cifra el enlace entre el cliente y el AP	Incrementa la del tráfico en redes públicas.	Es un cifrado y no un control de identidad

Nota. Elaboración propia con base en el análisis conceptual del apartado y en la revisión de protocolos de seguridad WPA3 realizada por Halbouni et al. (2023).

Como muestra la Tabla 7. La diferencia está en que WPA2 y WPA3 organizan el marco general de protección del acceso, SAE refuerza la autenticación en redes personales y OWE mejora la privacidad en redes abiertas sin llegar a convertirlas en redes autenticadas.

Estos componentes son de vital importancia para mejorar la seguridad en el acceso de los usuarios frente a problemas de seguridad en la autenticación y cifrado aunque no redule el problema de contar con una sola contraseña. En Wi-Fi 5 y superiores su despliegue depende de la compatibilidad entre clientes, puntos de acceso y controladores.

Ahora que comprendemos WPA2, WPA3, SAE y OWE entendemos que pueden resultar útiles y complementarias una de otra para proteger el acceso inalámbrico en los entornos IEEE 802.11 actuales. La importancia no se destacada por el protocolo que se elige sino en la coherencia entre una configuración segura, el soporte de los dispositivos, el tipo de red y el nivel de protección que se necesita.

2.6.8. Control de acceso empresarial: IEEE 802.1X y EAP-TLS

Las redes WLAN enfocadas en el sector empresarial requieren de mecanismos de acceso que tengan la posibilidad de separar a usuarios y dispositivos con diferentes privilegios de conexión sin depender de una clave única. En redes itinerantes y con movilidad de usuarios el uso de una contraseña no es suficiente para el control individual, revocación de permisos y por ello es necesario validar identidades antes de conceder acceso real a la

red.

El servicio de radius nos brinda un entorno de control de acceso basado en autorización del servidor, se implementa en redes cableadas e inalámbricas sin distinción de funciones, dado que el punto de acceso o el controlador cumplen el rol de autenticador y dicho servidor actúa como intermediario. Sethi et al. (2022) menciona que la arquitectura consta de tres entidades, el autenticador que se despliega en un equipo externo o en el AP, el servicio EAP que ofrece métodos seguros de verificación de identidad en IEEE802.1x y se configura en el cliente EAP peer y en el servidor EAP server.

Por otra parte, EAP-TLS esta orientado al entorno empresarial ya que depende de la extensión de certificados criptográficos que se validan mutuamente para establecer la confianza entre el cliente y servidor. A diferencia de los métodos basados solo en usuario y contraseña, este esquema permite reforzar la autenticación mutua y reducir la exposición que trae usar credenciales compartidas. Xiao et al. (2025) sostienen que EAP-TLS es un protocolo basado en certificados usado en redes inalámbricas empresariales, acceso remoto VPN y comunicaciones IoT seguras, pensado para autenticar a las entidades participantes y evitar accesos no autorizados.

El hecho de que EAP-TLS sea sólido depende de una implementación rigurosa, de validar bien los certificados y de administrar como corresponde la infraestructura criptográfica que sostiene la autenticación. En este modelo los certificados digitales dan evidencia verificable de identidad, mientras RADIUS y los servicios AAA permiten centralizar autenticación, autorización y registro. Esta arquitectura es especialmente útil en entornos corporativos, académicos e institucionales donde hace falta control de acceso basado en identidad y trazabilidad de las conexiones.

Tabla 8

Componentes del control de acceso empresarial WLAN basado en IEEE 802.1X y EAP-TLS

Componente o mecanismo	Tipo de función	Rol dentro del control de acceso WLAN	Cómo funciona o para qué sirve	Aporte a la seguridad de acceso	Limitaciones o consideraciones técnicas
IEEE 802.1X	Framework de acceso basado en radius	Autoriza mediante validación al cliente	Actúa como un agente externo validador de identidades.	Divide el permiso de ingreso a la red y la capacidad de uso de recursos	Necesita la implementación de una arquitectura AAA y compatibilidad entre protocolos
EAP	Marco extensible de autenticación.	Actúa como un medio de transporte de los mecanismos de autenticación entre C/S	Permite la encapsulación de métodos de autenticación	Provee un método de autenticación basado en credenciales	Dependerá del tipo de EAP implementado.
EAP-TLS	Autenticación basada en certificados TLS	Actúa como un validador de entidades previo a la autenticación	Se basa en la presencia de certificado en el cliente y servidor	Disminuye la necesidad de pre shared key	Requiere la gestión y control de certificados
RADIUS/AAA	Servicio de autenticación, autorización y administración de cuenta	Actúa como un portero permitiendo o negando el acceso a la red	Recibe peticiones de autenticación y aprueba o deniega	Mejor control basado en políticas	El servidor debe estar 100% disponible para acceder a la red
Supplicant	Es el cliente que envía peticiones	Punto de partida para la autenticación	Intercambia mensajes de tipo EAP para presentar credenciales o certificados.	Relaciona identidades con el acceso respectivo	Es necesario configurar un perfil adecuado y establecer niveles de confianza.
Authenticator	Agente intermediario entre el cliente y servidor	Especifica un método de conexión	Establece un puerto de acceso al Wireless controller y al servicio radius	Limita la capacidad de acceso del usuario antes de identificarse.	Requiere q su despliegue se integre a radius y cuente con políticas coherentes
Authentication server	Servidor de autenticación.	Responsable de la toma de decisiones	Realiza la validación de certificados, credenciales y políticas antes de conceder el acceso.	Existe un punto único de control centralizado	Se necesita que se encuentre operativo y disponible.
Certificados digitales/PKI	Infraestructura criptográfica de identidad mediante el uso de claves públicas o privadas	Credencial que valida a un usuario o dispositivo	Responsable de la gestión de los certificados	Reduce la superficie de exposición e incrementa la confianza en la red	Implica una constante gestión de validez de los certificados

Nota. IEEE 802.1X, EAP, EAP-TLS, RADIUS/AAA y certificados digitales/PKI no son generaciones Wi-Fi, sino mecanismos, protocolos o componentes de una arquitectura de autenticación empresarial aplicable a redes IEEE 802.11 según compatibilidad, configuración y políticas de seguridad. Elaboración propia con base en EAP-TLS 1.3, el manejo de certificados en métodos EAP basados en TLS y el análisis formal reciente de EAP-TLS (Preuß Mattsson et al., 2022; Sethi et al., 2022; Xiao et al., 2025).

Como muestra la Tabla 8, el control de acceso empresarial en WLAN no depende de un solo componente, sino de cómo se coordinan el cliente, el autenticador, el servidor de autenticación, el marco EAP, RADIUS/AAA y la infraestructura de certificados. Radius gestiona el control de acceso al puerto lógico, mientras EAP-TLS ofrece autenticación cliente servidor sustentada en el paso de certificados, esto refuerza la gestión de identidad previo al uso y

acceso de la red interna.

IEEE 802.1X y EAP-TLS son servicios idóneos para garantizar acceso más robusto independiente de la generación de WiFi a la que se haga referencia, sobre todo en esquemas donde no existe autenticación individual, mecanismos de gestión, control de acceso y revocación selectiva de permisos por ello muestran pertinencia y se alinean al trabajo propuesto al limitar las posibilidades de ser víctimas de suplantación de identidad y mejorar la gestión de usuarios y dispositivos en los entornos IEEE 802.11 actuales.

El control de acceso empresarial aporta una base técnica para fortalecer la autenticación, la trazabilidad y la validación de identidad en las redes WLAN modernas. Su eficacia depende de que infraestructura, políticas de acceso, certificados digitales y compatibilidad de clientes encajen bien entre sí, lo que permite armar un modelo de autenticación más robusto y controlado.

2.6.9. Protección de tramas de administración mediante PMF

Una de las debilidades más críticas en las redes inalámbricas es la denegación de servicio DoS, esto puede ocurrir en dos escenarios, el primero es la sensibilidad al abuso y mala configuración de canales que provocan una saturación del espectro interfiriendo la señal drásticamente por contaminación radioeléctrica y la segunda por saturación de tramas de administración y control. Ante lo primero, la mejor estrategia consiste en mediante el escaneo de aire y uso de herramientas de sensibilidad, establecer el perímetro de cobertura para evitar y selección del canal más idóneo para la transmisión.

Ante el segundo problema se sugiere la implementación de protección de tramas de administración mediante PMF para contar con una eficiencia en la gestión de la conexión y reasociación de clientes, las tramas de gestión que pueden ser afectadas son aquellas que permiten funciones como descubrimiento de red, autenticación inicial, asociación, reasociación, desasociación, roaming y mantenimiento lógico de la sesión.

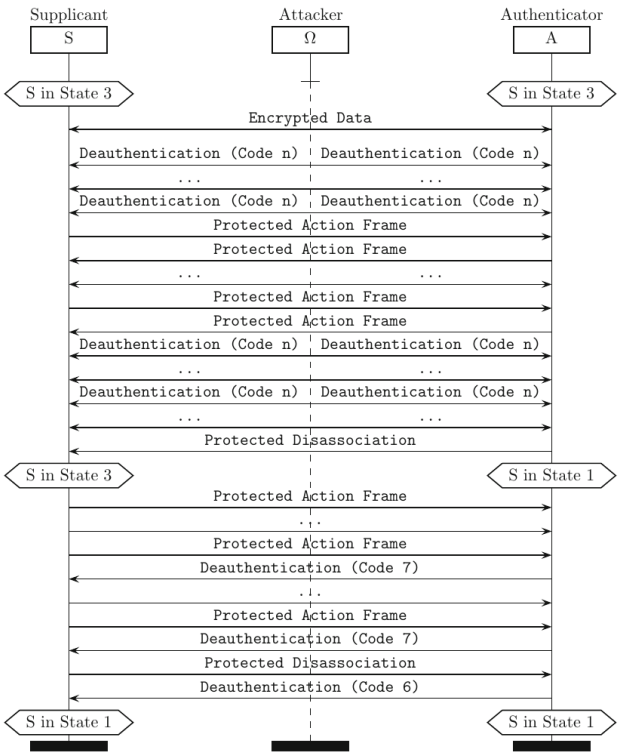
PMF responde justamente a esa necesidad, protegiendo una parte distinta del acceso WLAN, incorporado a partir de IEEE 802.11w, busca proteger ciertas tramas de administración robustas mediante mecanismos de

integridad, autenticación de origen y resistencia a la manipulación. Lounis et al. (2022) señalan que IEEE 802.11w se estandarizó para sumar mecanismos de seguridad sobre determinadas tramas de administración, con el fin de autenticar esos mensajes y reducir el riesgo de suplantación o alteración dentro del proceso de gestión WLAN.

El valor técnico de PMF está en reforzar la confianza del enlace una vez que ya se estableció la relación de seguridad entre cliente y punto de acceso. No valida usuarios ni cifra todo el tráfico de datos: su función es reducir la aceptación de mensajes de administración que no correspondan al contexto legítimo de la sesión. Así contribuye a la estabilidad del acceso inalámbrico y a mantener el estado de asociación.

Figura 12

Ataque de desautenticación mediante tramas unicast no protegidas en PMF



Nota. Tomado de “Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3” (p. 243), por K. Lounis, S. H. H. Ding y M. Zulkernine, 2022, en E. Aïmeur, M. Laurent, R. Yaich, B. Dupont y J. Garcia-Alfaro (Eds.), Foundations and Practice of Security: 14th International Symposium, FPS 2021 (Lecture Notes in Computer Science, Vol. 13291). Springer. https://doi.org/10.1007/978-3-031-08147-7_16. Copyright 2022 por Springer Nature Switzerland AG.

La Figura 12 muestra una secuencia de desautenticación en un entorno

PMF, donde el supplicant y el authenticator parten de State 3 (autenticados y asociados) mientras un actor externo inyecta tramas unicast sin proteger que afectan el estado lógico de la sesión. El aporte fundamental de la imagen consiste en mostrar los procesos de gestión, control y administración; y dejar por sentado que el proceso de protección no se simplifica en solo activar el PMF, sino, de como el cliente y AP tratan las tramas protegidas, las que no cuentan con protección y la transición entre estados. Lounis et al. (2022) evidencian que la interacción del cliente (supplicant) puede llevarlo a aun estado de no autenticado ni asociado, ello permite garantizar que PMF es necesario para mantener la continuidad y confiabilidad del enlace de gestión.

Es necesario comprender que este servicio no reemplaza a WPA2, WPA3, SAE, OWE, IEEE 802.1X ni EAP-TLS y tampoco reduce la interferencia electromagnéticas producto de la saturación de canales, mucho menos el jamming intencional, con esto nos referimos a los ataques que utilizan señales electromagnéticas potentes que bloquean los canales habilitados para wifi. Su valor se centra específicamente en proteger tramas de administración específicas, así que funciona como complemento del cifrado, la autenticación y el control de identidad.

2.6.10. Seguridad comparativa en Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7

Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 son generaciones IEEE 802.11 que se diferencian en capacidad, eficiencia, latencia, gestión del canal y operación multibanda. Wi-Fi 5 se relaciona con el estándar IEEE 802.11ac, mientras que Wi-Fi 6 con IEEE 802.11ax; y finalmente Wi-Fi 7 se asocial al estándar IEEE 802.11be, la nuevas generaciones han perfeccionado y mejorado el uso de OFDMA, BSS Coloring, Multi-Link Operation, para canales de 320 MHz y 4096-QAM según la generación a la cual se haga referencia (Farej & Ali, 2021; Karamyshev et al., 2025).

Para evitar confusiones es necesario distinguir entre rendimiento y seguridad ya que una no depende de la otra, Las redes de mayor capacidad permite la asociación de más clientes, bandas disponibles para su uso, canales con menos interferencia, y modos de compatibilidad heredados, por ello es necesario adecuar sus mecanismos de protección con el diseño real

de la WLAN. La National Security Agency (2023) sugiere implementar WPA3 o WPA2/3, usar frases que eviten palabras del diccionario y sean más robustas, además de activar la protección de tramas de administración cuando se cuente con el parámetro, esto evidencia nuevamente que la seguridad depende, en el fondo, de la configuración.

Contrastar las diferencias entre las redes WiFi nos ayuda a comprender la capacidades tecinas y limitaciones de cada una dependientes del entorno de despliegue aportando al estudio para interrelacionar autenticación, cifrado, control de acceso y condiciones operativas, sin minimizar o excluir la evaluación a un protocolo aislado ni a una sola familia de dispositivos.

Tabla 9

Comparación de funcionamiento, seguridad y debilidades en Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7

Estándar Wi-Fi	Base IEEE 802.11	Funcionamiento técnico relevante	Protocolos o mecanismos de seguridad asociados	Fortalezas de seguridad	Debilidades o riesgos principales	Relación con los objetivos del estudio
Wi-Fi 5	IEEE 802.11ac	Opera principalmente en 5 GHz, con canales de hasta 160 MHz, 256-QAM, beamforming y MU-MIMO en enlace descendente.	WPA2, WPA3 si el equipo lo soporta, IEEE 802.1X, EAP-TLS y PMF según configuración y compatibilidad.	Alta madurez, amplia compatibilidad y soporte para autenticación empresarial en despliegues corporativos.	Dependencia frecuente de WPA2/PSK, coexistencia con clientes antiguos y menor eficiencia en escenarios densos frente a generaciones posteriores.	Sirve como línea base para analizar seguridad de acceso en WLAN ampliamente desplegadas.
Wi-Fi 6	IEEE 802.11ax	Opera en 2,4 y 5 GHz; Wi-Fi 6E extiende operación a 6 GHz. Incorpora OFDMA, MU-MIMO ascendente y descendente, 1024-QAM, BSS Coloring y TWT.	WPA2/WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS y PMF,	Incrementa la cantidad de accesos posibles y la incorporación de estándares de cifrado modernos	Compatibilidad con protocolos heredados	Diferenciación con los otros estándares para comprender sus pros y contras
Wi-Fi 7	IEEE 802.11be	Opera en 2,4, 5 y 6 GHz; incorpora canales de hasta 320 MHz, 4096-QAM, Multi-Link Operation, Multi-RU y puncturing.	WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS y PMF,	Mejora el rendimiento disminuyendo la latencia e implementando versiones superiores de protocolos de seguridad.	La operación multienlace, canales amplios, compatibilidad con generaciones previas y relativamente un poco más compleja en la gestión	Diferenciar a los mecanismos más actuales contrastándolos con versiones anteriores

Nota. Elaboración propia con base en la evaluación de IEEE 802.11ac con QoS de Farej y Ali (2021), la evolución técnica de IEEE 802.11 descrita por Karamysheva et al. (2025), las recomendaciones de seguridad WLAN de la National Security Agency (2023), el análisis de protocolos Wi-Fi de Chalyi (2025) y la planificación de redes Wi-Fi 7 presentada por Trînc et al. (2026).

Como muestra la Tabla 9, Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 tienen capacidades técnicas distintas, pero comparten algo central: la seguridad de acceso

depende de cómo se articulan la autenticación, el cifrado, el control de identidad y la protección de gestión en cada generación. La tabla ayuda a distinguir entre el estándar de conectividad y los controles de seguridad que se le aplican, sin caer en la idea de que una generación Wi-Fi por sí sola reemplaza a WPA2, WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS o PMF.

Las diferencias de funcionamiento repercuten en cómo se protege la WLAN. En Wi-Fi 5 pesa su madurez y su alta compatibilidad; en Wi-Fi 6, la densidad de usuarios, OFDMA y BSS Coloring exigen controles consistentes; y en Wi-Fi 7, Multi-Link Operation y el uso de la banda de 6 GHz demandan políticas parejas entre enlaces, bandas y dispositivos (Karamyshev et al., 2025; Trînc et al., 2026).

Las debilidades no son producto de la sucesión de nuevas generaciones, sino de la capacidad de madurar tecnológicamente y emplear nuevas estrategias de mitigación de las debilidades técnicas y la deficiente administración y configuración de modos mixtos de operación con protocolos heredado para priorizar la compibilidad. (Chalyi, 2025) advierte que configuraciones débiles y con fallas técnicas producto del desconocimiento, como por ejemplo ciertos modos de compatibilidad pueden exponer a la red a ataques de downgrade.

2.6.11. Buenas prácticas y estrategias de prevención, detección y mitigación en seguridad WLAN

Proteger las redes IEEE 802.11 exige integrar controles técnicos, configuraciones seguras, monitoreo, gestión de identidad y una administración continua del acceso. Esto permite tratar la seguridad WLAN como un proceso operativo permanente, no como una decisión que se agota en elegir un protocolo de conexión. En las redes actuales, evaluar WPA2, WPA3 y OWE implica mirar tanto sus fortalezas como las debilidades de implementación y la exposición frente a ataques dirigidos a la autenticación y el cifrado (Mykhaylova & Nakonechny, 2024).

Es necesario priorizar la prevención y que los usuarios comprendan qye son la primera línea de defensa ante las diferentes amenazas para reducir la superficie y probabilidad de que un ataque logre su objetivo, entre ellos,

acceso no autorizado, del abuso de credenciales, exposición del tráfico. Es necesario reforzar y aplicar la estrategia del permiso mínimo para aplicar configuraciones menos permisivas, reforzar el proceso de asociación y limitar comportamientos automáticos (Chatzisofroniou & Kotzanikolaou, 2022).

El detectar un evento sospechoso o una intrusión mediante la prevención, no llega a eliminar el problema del todo, existen otros mecanismos ajenos a la responsabilidad del usuario como por ejemplo asociaciones anómalas, tramas sospechosas, puntos de acceso no autorizados, intentos de suplantación, inundación de beacons, desautenticación y variaciones inesperadas en el comportamiento de la WLAN. En puntos de acceso WPA3, es protocolo analiza, reconoce e identifica patrones propios del estándar 802.11 y puede generar alertar tempranas para minimizar el tiempo en que se encuentra expuestos a un evento que tenga como objetivo afectar a la red (Dalal et al., 2022).

Las estrategias de mitigación compilan un conjunto de estrategias técnicas y administrativas que buscan disminuir el impacto, restaurar el equipo a un punto seguro, corregir las debilidades en las configuraciones y mantener la continuidad operativa de los dispositivos inalámbricos.

En entornos empresariales y profesionales el uso de WPA3-Enterprise es mandatorial, la mitigación debe contemplar escenarios donde somos susceptibles de vectores asociados a SAE, downgrade, puntos de acceso falsos, suplantación de identidad y debilidades operativas asociadas a problemas de gestión de tramas y sobremodo a la correcta aplicación de buenas prácticas en la administración (Tleuberdin et al., 2025).

Tabla 10

Buenas prácticas y estrategias de prevención, detección y mitigación en seguridad WLAN

Dimensión	Buena práctica o estrategia	Mecanismo asociado	Amenaza o debilidad que reduce	Aporte a la seguridad de acceso	Consideración técnica
Prevención	Adoptar WPA3 cuando exista compatibilidad	WPA3-Personal o WPA3-Enterprise	Configuraciones heredadas y cifrado débil	Fortalece autenticación y protección del tráfico	Validar soporte de clientes y evitar modo mixto permanente

Dimensión	Buena práctica o estrategia	Mecanismo asociado	Amenaza o debilidad que reduce	Aporte a la seguridad de acceso	Consideración técnica
Prevención	Mantener WPA2 seguro cuando sea necesario	WPA2-AES/CCMP y control empresarial	Uso de WEP, TKIP	acceso seguro a equipos	Documentar las excepciones
Prevención	Usar SAE en redes personales	Intercambio SAE de WPA3-Personal	Ataques de diccionario fuera de línea y abuso de PSK	Mejora el establecimiento de claves de sesión	Requiere firmware actualizado y frases de paso robustas
Prevención	Aplicar OWE en redes abiertas	Cifrado oportunista Wi-Fi Enhanced Open	Exposición directa del tráfico en redes sin clave	Agrega cifrado sin autenticación previa	No reemplaza control de identidad ni segmentación
Prevención	Implementar IEEE 802.1X y EAP-TLS	Autenticación mutua con certificados	Suplantación, reutilización de credenciales y acceso no autorizado	Vincula el acceso a identidad verificable	Gestionar ciclo de vida de certificados y revocación
Prevención y mitigación	Exigir PMF cuando sea compatible	Protección de tramas de administración	Manipulación de tramas de desautenticación y desasociación	Reduce interrupciones y falsificación de gestión	Supervisar clientes incompatibles antes de exigirlo
Mitigación	Segmentar red y separar invitados	VLAN, políticas de acceso y aislamiento	Movimiento lateral y mezcla de niveles de confianza	Limita alcance del acceso concedido	Asociar SSID con dominios de seguridad definidos
Prevención	Gestionar credenciales con criterios robustos	Políticas de clave, rotación y administración segura	Abuso de credenciales, claves reutilizadas o débiles	Disminuye exposición por autenticación deficiente	Evitar PSK compartidas en entornos empresariales
Mitigación	Actualizar firmware y revisar configuraciones	Parches, hardening y línea base de configuración	Fallos de implementación y valores por defecto inseguros	Corrige debilidades conocidas del entorno WLAN	Mantener control de cambios y respaldo de configuración
Detección	Monitorear WLAN y detectar AP no autorizados	WIDS/WIPS, registros y análisis de eventos	Rogue AP, Evil Twin y asociaciones anómalas	Aporta alerta temprana ante desviaciones	Ajustar umbrales y firmas al contexto operativo
Prevención y detección	Inventariar y controlar dispositivos autorizados	Inventario, NAC y revisión de activos	Dispositivos desconocidos, obsoletos o no confiables	Restringe el acceso a activos reconocidos	Mantener inventario actualizado; no depender solo de MAC
Gestión y mitigación	Definir políticas de acceso, auditoría y trazabilidad	Revisión de accesos, registros y responsabilidades	Falta de evidencia, permisos acumulados y mala gobernanza	Facilita respuesta, rendición de cuentas y mejora continua	Establecer periodicidad de auditoría y retención de logs

Nota. La dimensión asignada a cada estrategia responde a su función predominante dentro de la gestión de seguridad WLAN. La síntesis se apoya en estudios recientes sobre ataques de asociación y controles de mitigación (Chatzisofroniou y Kotzanikolaou, 2022), WPA3-SAE y disponibilidad (Chatzoglou et al., 2022), detección de intrusiones en redes WPA3 (Dalal et al., 2022), análisis de WPA2, WPA3 y OWE (Mykhaylova et al., 2024), y vulnerabilidades en WPA3-Enterprise (Tleuberdin et al., 2025).

La tabla 10 aporta un conjunto de buenas prácticas y sugerencias de

varios autores, clasificadas por la dimensión en que puedan afectar, además de asociar cada estrategia con su mecanismo técnico y la debilidad que busca atenuar basándose en controles complementarios verificables.

La gestión de buenas prácticas es complementaria unas de otras ya que se aplican en diferentes niveles de las capas del modelo OSI y la integración proveedores de identidad con marcos IEEE 802.1X muestra que el control de acceso actual amalgama la autenticación con las políticas establecidas en la organización y la eficiencia operativa centrada en la experiencia sin debilitar la seguridad de la WLAN (Mortágua et al., 2024).

Tenga en cuenta que será necesario combinar diferentes mecanismos técnicos, administrativos compatibles de cada generación si pretende usar modos de acceso mixto, además no se debe descuidar la supervisión continua, y auditar periódicamente las configuraciones para identificar si nuevos firmwares incorporan funcionalidades mejoradas que requieran su adaptación e implementación. Es fundamenta aplicar este conjunto de estrategias dado que aún siendo protocolos recientes conservan riesgos de implementación, transición, configuración y operación y es mandatorio una revisión permanente (Mykhaylova & Nakonechny, 2024).

Capítulo 3: Resultados

3.1. Resultados del proceso de revisión sistemática PRISMA

La revisión sistemática siguió los lineamientos del método PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), con el fin de mantener la trazabilidad a lo largo de la identificación, depuración, cribado, elegibilidad e inclusión de literatura sobre seguridad WLAN en entornos IEEE 802.11. La búsqueda documental cubri{o a diferentes actores, entre ellos Scopus, Web of Science, IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, MDPI, Google Scholar, eLibro y Google Books, además de estándares técnicos, tesis y documentos web de empresas especializadas en ciberseguridad.

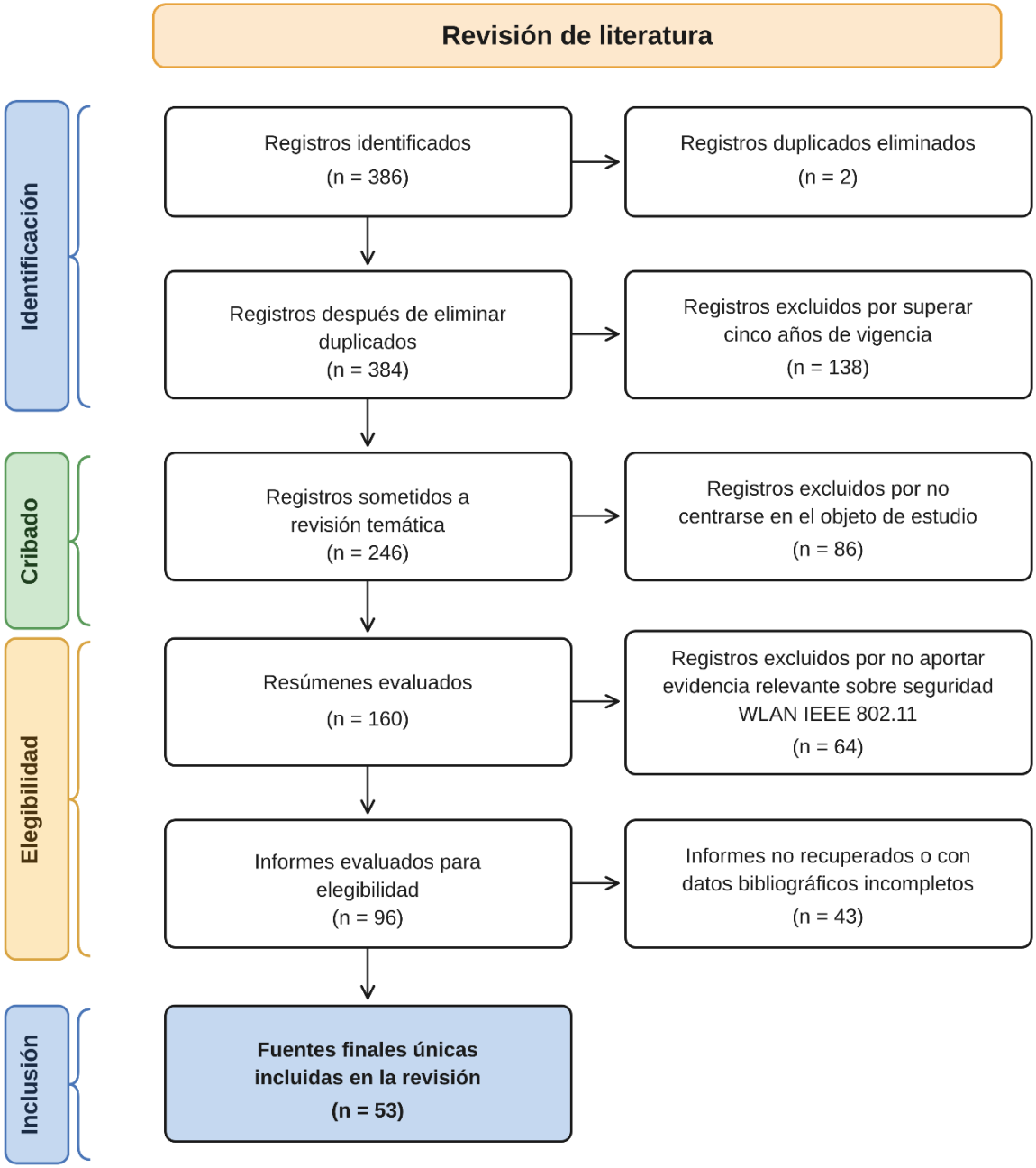
En función de los ejes temáticos principales se utilizaron los siguientes criterios de búsqueda WLAN IEEE 802.11, WPA, ataques a redes Wi-Fi, autenticación y cifrado WLAN, SAE, OWE, IEEE 802.1X, EAP-TLS, PMF, desautenticación, Evil Twin, Rogue AP, Wi-Fi 5, Wi-Fi 6, Wi-Fi 7 y mitigación de amenazas Wi-Fi. En la fase de identificación se obtuvieron 386 registros, y por duplicidad se eliminaron 2 documentos quedando 384 para la posterior revisión. Luego se excluyeron 138 registros candidatos por no presentar tecnologías actualizadas y superar el umbral de los 5 años, quedando 246 para la revisión temática en donde se descartaron otros 86 registros debido a que el tema no se centraba en el objeto de estudio y no aportaba a los fundamentos requeridos.

Posteriormente se mostrará la elegibilidad basada en el análisis de 160 resúmenes de artículos, que al ser depurados por falta de aporte quedaron en

Más adelante se leyeron y analizaron 160 resúmenes, que permitieron excluir 64 registros debido a que no aportaban evidencia relevante sobre seguridad WLAN dando un resultado de 96, en la fase de elegibilidad se debió excluir 43 registros dado que no eran open access y su contenido no era accesible completamente o tenía carencias bibliográficas. Al final se seleccionaron 53 fuentes únicas, que conformaron la base documental para el análisis de amenazas, debilidades y mecanismos de seguridad en redes IEEE 802.11, como se muestra en la Fig. 13.

Figura 13

Diagrama de flujo PRISMA para la revisión sistemática



Nota. Elaboración propia. El diagrama presenta el proceso de identificación, cribado, elegibilidad e inclusión de fuentes en la revisión sistemática sobre los fundamentos técnico y seguridad en WLAN IEEE 802.11.

El proceso PRISMA sirvió para ordenar y depurar la literatura recopilada hasta llegar a un conjunto final de 53 fuentes pertinentes para la

investigación. La selección tomó en cuenta la actualidad de los documentos, su relación directa con el objeto de estudio, el aporte teórico al funcionamiento de las redes IEEE 802.11 y que la información fuera verificable.

3.2. Caracterización de los estudios incluidos en la revisión

Los estudios incluidos forman la base documental que resultó de la revisión sistemática aplicada en esta investigación. Descubrir los elementos comunes que aportan valor al estudio permitió contar con 53 fuentes seleccionadas por criterios predominantes como criterios temporales, documentales, técnicos y temáticos, de tal forma que los registros resultantes se sustenten en evidencia claramente delimitada y verificable por encima de afirmaciones sueltas y escuetas sobre seguridad en redes WLAN.

Durante el proceso de selección se garantizó que la procedencia de los registros se obtuviese de fuentes confiables y bases de datos de alto impacto para darle un valor y peso documental significativo al estudio. El cuerpo del estudio complementa bases de datos bibliográficas, con bibliotecas digitales especializadas, plataformas editoriales, motores complementarios, libros académicos y técnicos, tesis, estándares técnicos, reportes especializados y documentos web sobre ciberseguridad, de acuerdo con la figura 13.

Organizar la evidencia por tecnología Wi-Fi, mecanismo de seguridad y amenaza abordada conecta lo revisado con los objetivos de identificación y análisis comparativo. Esta clasificación permite ubicar los estudios relacionados con redes IEEE 802.11, Wi-Fi 5, Wi-Fi 6, Wi-Fi 7, WPA2, WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS, PMF, suplantación, puntos de acceso falsos, desautenticación, Man-in-the-Middle y denegación de servicio.

Tabla 11

Caracterización de los estudios incluidos en la revisión sistemática

Criterio	Categorías identificadas	Resultado observado	Aporte al objetivo específico	Utilidad para el resultado
Año de publicación	Fuentes recientes y técnicas de apoyo.	Literatura actualizada y sustento técnico	Identificar vulnerabilidades y amenazas actuales.	Delimita los estudios actuales según su función.
Fuente de procedencia	Scopus, WoS, IEEE Xplore, ACM, ScienceDirect, SpringerLink, MDPI, Google Scholar, eLibro, Google Books, estándares, tesis y web especializada.	Fuentes confiables y de impacto	Sustenta todo el análisis realizado	Trazabilidad de la procedencia de la evidencia
Tipo de fuente	Artículos, libros, tesis, estándares, documentos técnicos, reportes y web.	Fuentes científicas y técnicas.	Permite analizar y sustentar las evidencias acerca de las amenazas y malas prácticas.	Agrega un orden estructuras basado en la naturaleza de la fuente
Tecnología Wi-Fi	Wi-Fi 5, Wi-Fi 6, Wi-Fi 7 e IEEE 802.11 general.	Evidencia orientada a generaciones actuales y al estándar base.	Relaciona amenazas y mecanismos con el alcance técnico.	Facilita el análisis comparativo.
Mecanismo de seguridad	WPA2, WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS, PMF y control de acceso.	Se prioriza los tópicos de autenticación, cifrado y protección de tramas.	Complementa el estudio de los mecanismos de protección y buenas prácticas de usuarios y administradores.	Permite realizar propuestas, aportes y sugerencias de mejora.
Amenaza o debilidad	Ataques a autenticación y cifrado, configuración insegura, protocolos heredados, rogue AP, evil twin, MITM, DoS, desautenticación y plano de administración.	Bases conceptuales sustentadas de las estrategias empleadas por los atacantes para comprometer las redes.	Identifica las amenazas y debilidades más relevantes.	Permite la construcción de la matriz de relación
Prevención, detección y mitigación	Buenas prácticas, hardening, monitoreo, segmentación, control de acceso y políticas.	Permite identificar los criterios técnicos actuales para prevención, detección y mitigación	Permite proponer estrategias para afrontar los ataques de autenticación y cifrado.	Establecimiento y propuesta de estratégias.

Nota. La tabla permite identificar el aporte de las fuentes obtenidas con respecto a los propósitos y objetivos del estudio de acuerdo a los criterios documentales, técnicos y temáticos vinculados con seguridad WLAN. WoS = Web of Science; ACM = Association for Computing Machinery; MDPI = Multidisciplinary Digital Publishing Institute.

En la Tabla 11, caracterizamos y sintetizamos el aporte de las fuentes al corpus documental de acuerdo con los criterios y sugerencias técnicas que tiene como finalidad el presente capítulo. Para una fácil comprensión fue necesario organizarlos por año, procedencia, tipo de fuente, tecnología, mecanismo de seguridad y amenaza abordadas, de esta forma es sencillo identificar el aspecto al cuál aporta en la investigación.

Esta distribución permite presentar los resultados que siguen sobre una base documental ordenada, sin repetir el marco teórico ni alargar la explicación metodológica. La clasificación de los estudios orienta el análisis comparativo de WPA2, WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS y PMF, además de la revisión de alternativas de fortalecimiento aplicables a Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7.

3.3. Síntesis analítica de amenazas y debilidades WLAN identificadas

La revisión sistemática permitió agrupar las amenazas y debilidades WLAN en categorías ligadas a autenticación, cifrado, integridad, disponibilidad, suplantación, administración del enlace y configuración insegura, permitiendo de esta manera comprender q los riesgos no se agrupan únicamente en una categoría, sino que se amplían hacia la gestión de credenciales, los mecanismos de protección, la compatibilidad entre dispositivos y las buenas prácticas de administración de la red.

En Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7, los resultados señalan que la generación tecnológica por sí sola no garantiza un nivel adecuado de seguridad. Reducir la exposición depende de configurar bien los mecanismos disponibles, de que haya compatibilidad real entre clientes e infraestructura, de aplicar controles de acceso y de articular medidas de prevención, detección y mitigación en la administración de la WLAN.

Tabla 12

Síntesis de amenazas y debilidades WLAN identificadas en la revisión sistemática

Categoría de amenaza o debilidad	Resultado identificado	Mecanismo o componente afectado	Impacto en la seguridad WLAN	Relación con el objetivo específico	Implicación para prevención o mitigación
Ataques contra autenticación	Presencia de riesgos orientados a comprometer el acceso y validar usuarios no autorizados.	WPA2, WPA3, SAE, 802.1X y EAP-TLS.	Afecta la confianza del proceso de asociación y acceso.	Identifica vulnerabilidades de autenticación en redes Wi-Fi modernas.	Requiere autenticación robusta, control de identidad y revisión de configuraciones.
Ataques contra cifrado	Evidencia de exposición asociada a claves débiles, tráfico mal protegido y configuraciones deficientes.	WPA2, WPA3, claves precompartidas y cifrado WLAN.	Compromete confidencialidad y protección del tráfico.	Relaciona mecanismos de cifrado con amenazas relevantes.	Exige cifrado actualizado y gestión segura de claves.
Debilidades de integridad	Se observaron riesgos sobre la protección del enlace y la alteración de comunicaciones.	Integridad de tramas, enlace inalámbrico y protocolos de protección.	Reduce la confiabilidad del intercambio de datos.	Apoya la identificación de debilidades técnicas del entorno WLAN.	Demanda controles de integridad y protección de tramas.
Configuraciones inseguras	La evidencia muestra exposición por ajustes débiles, administración deficiente o parámetros no endurecidos.	AP, controladores, SSID, políticas y perfiles WLAN.	Amplía la superficie de ataque y facilita accesos indebidos.	Permite reconocer debilidades operativas de seguridad.	Requiere hardening, revisión periódica y administración segura.
Protocolos o mecanismos heredados	Se identificó riesgo por coexistencia con mecanismos antiguos o menos robustos.	WEP, WPA heredado, WPA2 mal configurado y entornos mixtos.	Puede degradar el nivel efectivo de seguridad.	Relaciona compatibilidad con exposición técnica.	Implica retirar mecanismos obsoletos o limitar su uso.

Categoría de amenaza o debilidad	Resultado identificado	Mecanismo o componente afectado	Impacto en la seguridad WLAN	Relación con el objetivo específico	Implicación para prevención o mitigación
Credenciales débiles o compartidas	Los estudios revisados resaltan debilidades por contraseñas previsibles o uso compartido de claves.	PSK, frases de paso y gestión de credenciales.	Facilita acceso no autorizado y abuso de credenciales.	Identifica vulnerabilidades de control de acceso.	Requiere políticas de claves, rotación y autenticación individual.
Rogue AP y evil twin	Se identificaron amenazas de suplantación de puntos de acceso y redes falsas.	SSID, AP, asociación cliente y validación de red.	Compromete la confianza del usuario y la selección del AP.	Determina amenazas de acceso y suplantación WLAN.	Demanda monitoreo WLAN, validación y detección de AP no autorizados.
Man-in-the-Middle	La revisión evidenció riesgos de intermediación cuando la red o el usuario confían en infraestructura no legítima.	Canal inalámbrico, autenticación, cifrado y sesión de usuario.	Puede exponer credenciales, tráfico o sesiones.	Vincula amenazas de acceso con protección de autenticación y cifrado.	Requiere autenticación fuerte, cifrado y detección de anomalías.
Desautenticación y denegación de servicio	Se observó presencia de amenazas orientadas a interrumpir asociación, conectividad o disponibilidad.	Tramas de administración, PMF y disponibilidad WLAN.	Afecta la continuidad del acceso inalámbrico.	Identifica amenazas de disponibilidad y gestión del enlace.	Exige PMF, monitoreo y planes de respuesta ante interrupciones.
Debilidades del plano de administración	La evidencia revisada muestra exposición en funciones de gestión, control y operación de la WLAN.	Tramas de administración, controladores, AP y políticas.	Incrementa riesgos de manipulación o degradación del servicio.	Relaciona seguridad de administración con protección del acceso.	Requiere protección de gestión, trazabilidad y control de cambios.
Compatibilidad y coexistencia Wi-Fi 5/6/7	Se identificaron brechas por transición tecnológica, clientes heterogéneos y modos mixtos.	Generaciones Wi-Fi, WPA2/WPA3, clientes y AP.	Genera diferencias entre capacidad disponible y seguridad aplicada.	Contextualiza amenazas según generación tecnológica.	Implica validar compatibilidad y aplicar el mayor nivel de protección posible.
Ausencia o mala aplicación de buenas prácticas	Los hallazgos muestran debilidades por falta de monitoreo, segmentación o políticas de acceso.	Administración WLAN, segmentación, inventario y monitoreo.	Reduce capacidad de prevención, detección y respuesta.	Apoya el análisis de políticas y buenas prácticas defensivas.	Requiere gestión continua, segmentación y auditoría de acceso.

Nota. La tabla sintetiza las amenazas y debilidades identificadas en las 53 fuentes finales de la revisión sistemática, y su relación con mecanismos de prevención o mitigación WLAN.

Como se observa en la Tabla 12, las amenazas y debilidades identificadas se reparten entre componentes de autenticación, cifrado, integridad, disponibilidad, administración y configuración. Esta clasificación distingue los puntos de exposición que afectan la seguridad WLAN y los vincula con los mecanismos o componentes que exigen mayor atención en redes IEEE 802.11.

Los resultados contribuyen a identificar vulnerabilidades y amenazas relevantes, y muestran que hace falta analizar los mecanismos de autenticación, cifrado, control de acceso, PMF y las buenas prácticas de

administración segura. De la clasificación se desprende algo más: la mitigación no recae en un solo protocolo, sino en cómo se combinan los controles técnicos y operativos.

Con ello podemos inferir que esta síntesis de amenazas y debilidades fija la base técnica para los resultados comparativos de los mecanismos de seguridad y para las alternativas de fortalecimiento WLAN que se desarrollarán, además de ordenar los hallazgos de la revisión sistemática y prepara el análisis de prevención, detección y mitigación.

3.4. Resultados comparativos de mecanismos de autenticación, cifrado y protección de acceso en Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7

Se ordenaron diversos mecanismos de seguridad en función del acceso inalámbrico. Se obtuvo una comparativa que se divide en controles orientados al cifrado del enlace, la autenticación del usuario, la identidad de la organización empresarial, la protección de redes de acceso al público y el custodio del plano de administración.

En escenarios mucho más complejos asociados al entorno empresarial, Radius y EAP-TLS destacan en el control de acceso centrado en identidad del usuario. Los registros revisados diferencia cada uno de los modelos basados en claves simétricas con esquemas de autenticación centralizada que ayuda en la gestión de certificados digitales, revocación selectiva y mayor trazabilidad de usuarios y dispositivos.

PMF funciona bajo un esquema complementario para apoyar a mantener la integridad del tráfico administrativo y la autenticidad de ciertas tramas de control.

Tabla 13

Comparación de mecanismos de autenticación, cifrado y protección de acceso WLAN

Mecanismo	Resultado comparativo	Debilidad que reduce	Prevención	Mitigación	Condición o límite	Aplicación en Wi-Fi moderno
WPA2	Control de continuidad en redes desplegadas.	Claves débiles, tráfico expuesto y configuraciones heredadas.	Exige claves robustas y cifrado activo.	Sostiene protección cuando no existe migración completa.	Sensible a PSK débiles y modos mixtos.	Protocolo heradado

WPA3	Perfil robusto	Ataques a contraseñas y degradación por transición.	Ayuda a la autenticación y protección	Capacidad de recuperarse de un incidente	Requiere de software em el lado del cliente	Usado en todas las versiones wifi
SAE	Autenticación personal robusta	Ataques de diccionario y fuerza bruta	Reduce viabilidad de validación offline.	Limita efectos de material capturado.	No compensa frases de paso débiles.	Propio de WPA3-Personal.
OWE	Cifra el enlace en redes abiertas.	Exposición pasiva de tráfico sin contraseña.	Protege comunicación básica sin PSK.	Reduce lectura no autorizada del tráfico.	No autentica usuario ni AP.	Útil en redes públicas compatibles.
IEEE 802.1X	Centraliza el control de acceso empresarial.	Uso colectivo de claves y acceso no diferenciado.	Valida identidad antes del acceso efectivo.	Facilita revocación y control por entidad.	Requiere AAA y políticas consistentes.	Aplicable en WLAN empresariales Wi-Fi 5/6/7.
EAP-TLS	Fortalece autenticación mediante certificados.	Credenciales débiles, robo de claves y suplantación.	Exige identidad criptográfica verificable.	Reduce impacto de contraseñas comprometidas.	Demanda gestión PKI y ciclo de certificados.	Adecuado para entornos de alta criticidad.
PMF	Protección de tramas de control	Manipulación de paquetes y suplantación de identidad	Apoya a la autenticidad en la gestión	Reduce la posibilidad de ser afectado por tramas duplicadas	No utiliza cifrado	Siempre que el cliente lo soporte

Nota. Resumen comparativo de los mecanismos sugeridos para la autenticación y control y prevención de ataques.

Como muestra la Tabla 13, los mecanismos revisados cumplen funciones que se complementan dentro de la seguridad WLAN. WPA2, WPA3, SAE y OWE tienen que ver con la protección de acceso en redes personales o abiertas; IEEE 802.1X y EAP-TLS refuerzan el control empresarial basado en identidad; y PMF protege una parte específica del plano de administración.

Los mecanismos analizados no pertenecen en exclusiva a una sola generación Wi-Fi, ya que su uso depende de la compatibilidad del punto de acceso, de los clientes y de la configuración aplicada. WPA2 es heredado y sigue presente en Wi-Fi 5, Wi-Fi 6 y en algunos equipos certificados con Wi-Fi 7. WPA3 y SAE son elementales de la versión 6. OWE es idóneo para redes abiertas modernas compatibles.

La comparativa apoya la idea de que la efectividad de estos mecanismos depende de las políticas de configuración que implementen los administradore y delimita la base técnica para plantear alternativas de fortalecimiento de la WLAN.

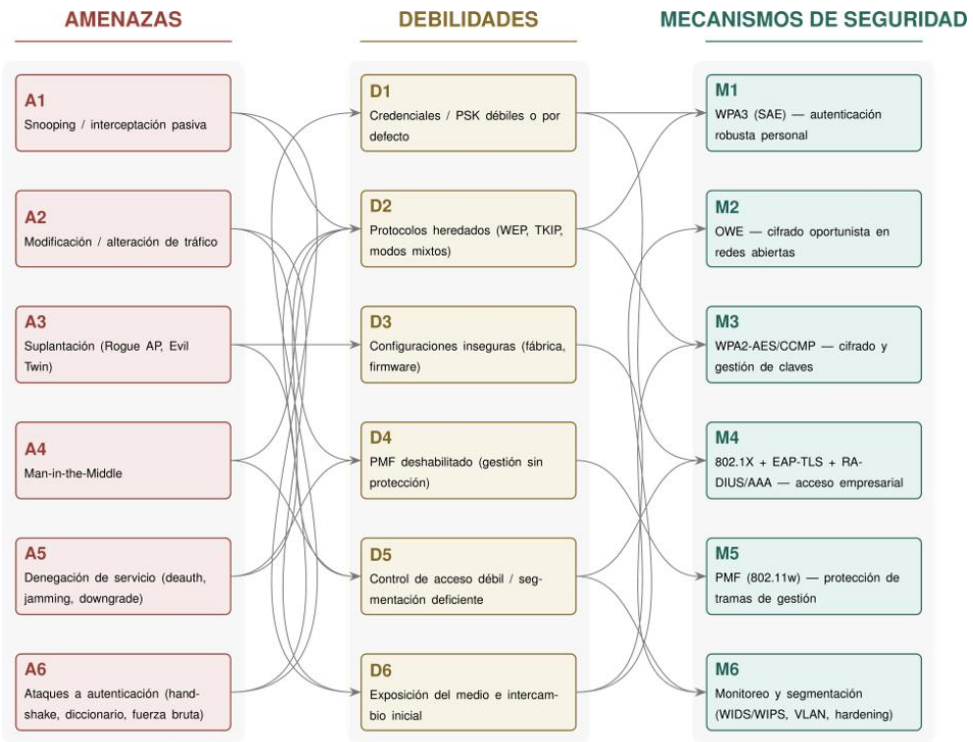
3.4.1. Relación entre amenazas, debilidades y mecanismos de seguridad

Analizar los hallazgos en conjunto permitió establecer que las amenazas WLAN no actúan por separado, sino que se aprovechan de debilidades concretas de autenticación, cifrado, configuración, administración y control de acceso. Por eso este apartado ordena esas relaciones y las

conecta con los mecanismos de seguridad más pertinentes para prevenirlas, detectarlas o mitigarlas. Esta integración permite pasar de identificar los riesgos uno por uno a una visión articulada de la seguridad de acceso, en la que cada debilidad puede tratarse con controles complementarios aplicables a las tres generaciones Wi-Fi actuales.

Figura 14

Amenazas, vulnerabilidades y mecanismos de mitigación de ataques de autenticación y cifrado en redes Wi-Fi (IEEE 802.11)



	A1	A2	A3	A4	A5	A6
D (habilita)	D6, D2	D4, D6	D5, D3	D2, D5	D4, D2	D1, D2
M (mitiga)	M1, M2, M3	M2, M3, M5	M4, M6	M1, M3, M4, M6	M1, M3, M5	M1, M3, M4

A = amenaza · **D** = debilidad/vulnerabilidad que la habilita (A→D) · **M** = mecanismos de mitigación resultantes (A→D→M). Los códigos A1–A6, D1–D6 y M1–M6 corresponden a la figura superior y su leyenda.

Nota. Elaboración propia del autor con apoyo de Claude (Anthropic) para la organización visual de las relaciones entre amenazas, debilidades y mecanismos de seguridad en redes Wi-Fi IEEE 802.11.

Como muestra la Figura 14, existe una clara relación entre las debilidades de autenticación del cliente, con el cifrado y la configuración y administración que implementen los administradores. La captura pasiva del tráfico, la modificación no autorizada de este y la suplantación de identidad junto con los ataques Man-in-the-Middle y el DoS, son los mecanismos

utilizados masivamente por los hackers cuando atacan las redes inalámbricas,

La matriz que se expone en el grafico permite visualizar y asociar de mejor manera la trazabilidad de las amenazas y ver como se asocian entre ellas para tener una clara visión de las relaciones. Leerla por columnas facilita ir del ataque a la respuesta defensiva; leerla por filas ayuda a reconocer patrones que se repiten y a priorizar controles.

Los resultados evidencian que no se puede y debe confiar en que el proceso es responsabilidad de un protocolo, sino de una combinación confiable entre autenticación robusta, cifrado vigente, control de identidad, protección de tramas y supervisión continua.

3.5. Alternativas de fortalecimiento de la seguridad de acceso WLAN

Los resultados permiten organizan en dos niveles que se complementan. El primero conecta los ataques de autenticación y cifrado con estrategias de prevención y mitigación; el segundo fija criterios técnicos para fortalecer la arquitectura y la administración de las redes IEEE 802.11. Separarlos así ayuda a distinguir la respuesta ante eventos concretos de las decisiones estructurales que sostienen la seguridad en Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7.

Tabla 14

Propuesta de estrategias de prevención y mitigación frente a ataques de autenticación y cifrado WLAN

Ataque o debilidad priorizada	Estrategia de prevención	Estrategia de mitigación	Mecanismo asociado	Aplicación en Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7	Resultado esperado
Ataques contra autenticación	Priorizar mecanismos de autenticación offline que permitan control individual de cada identidad conectada.	Al haber ocurrido el ataque revocar credenciales afectadas y aislar sesiones con comportamiento anómalo.	WPA3/SAE; IEEE 802.1X; EAP-TLS.	Wi-Fi 5 es soportado; respaldo real en Wi-Fi 6 y Wi-Fi 7.	La probabilidad de acceso indebido baja y deja mejor rastro para investigar incidentes
Ataques contra cifrado	Usar perfiles criptográficos vigentes y eliminar cifrados heredados o modos degradados aún activos.	Migrar clientes inseguros renovando claves de sesión regularmente.	Algoritmos de última generación y compatibles con los usuarios AES	Útil en todas, pero se recomienda la tercera versión.	Incrementa la confidencialidad

Ataque o debilidad priorizada	Estrategia de prevención	Estrategia de mitigación	Mecanismo asociado	Aplicación en Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7	Resultado esperado
Credenciales débiles	Uso de EAP-TLS	Rotar o revocar credenciales comprometidas.	Sistema de gestión radius.	Aplicable en todas las generaciones.	Disminución del abuso de claves compartidas.
Redes abiertas sin protección	Incorporar cifrado oportunista y aislar clientes.	Segmentar el servicio, limitar privilegios por defecto y monitoreando actividad sospechosa	OWE; aislamiento de clientes; segmentación.	Pertinente especialmente en redes públicas modernas compatibles.	Menos exposición pasiva del tráfico y alcance acotado si ocurre un incidente-
Suplantación de punto de acceso	Validar identidad de la infraestructura antes de conectar, siendo estos confiables.	Monitorear equipos AP periféricos que se unan o tengan el mismo ssid.	Solicitar certificados para autenticar.	Válidos en todas las generaciones.	Mayor confianza en la infraestructura de conexión.
Rogue AP y evil twin	Mantener un inventario autorizado y supervisado del entorno radioeléctrico.	Localizar, aislar y retirar puntos de acceso no autorizados; alertar a usuarios que se vieron afectados.	WIDS/WIPS; EAP-TLS; control de inventario.	Necesario en despliegues Wi-Fi 5/6/7 con múltiples AP.	Detectar de forma temprana la infraestructura fraudulenta.
Man-in-the-Middle	Exigir autenticación mutua, validar los certificados y cifrar del enlace.	Interrumpir la sesión comprometida y aislar el segmento y restablecer la confianza criptográfica de cero.	EAP-TLS; WPA3; OWE; segmentación.	Aplicable según el tipo de red y soporte de clientes.	Menor exposición a la interceptación y manipulación del tráfico.
Desautenticación y manipulación de gestión	Aplicar PMF con el nivel de exigencia adecuado con el entorno	Bloquear fuentes sospechosas y recuperar asociaciones legítimas y revisar registros de eventos.	PMF; monitoreo WLAN; registros de eventos.	Disponible en Wi-Fi 5 compatible y con mayor relevancia en Wi-Fi 6/7.	Garantizar mejor estabilidad de la sesión y protección del plano de administración.
Accesos no autorizados empresariales	Centralizar autenticación, autorización y registro por medio de identidad individual por usuario	Revocar cuentas o certificados comprometidos	IEEE 802.1X; EAP-TLS; AAA/RADIUS; segmentación.	Aplicable a WLAN empresariales Wi-Fi 5/6/7.	Control granular y revocación selectiva.
Configuraciones inseguras o heredadas	Eliminar WEP/TKIP así como cualquier modo permisivo o servicios innecesarios	Aislar equipos heredados que no se pueden actualizar y planear migración controlada.	WPA3/WPA2-AES; PMF; actualización; políticas de acceso.	Crítico en Wi-Fi 5 y entornos mixtos; preventivo en Wi-Fi 6/7.	Menor superficie de ataque y se evita que la seguridad se degrade con el tiempo.

Nota. Compilación de estrategias frente a los ataques estudiados con respuestas defensivas aplicables según la situación.

Como muestra la Tabla 14, se infiere que la prevención baja la probabilidad de compromiso mediante autenticación robusta, protección criptográfica y validación de infraestructura; la mitigación limita el impacto mediante revocación, aislamiento, segmentación, monitoreo y un restablecimiento controlado del acceso.

Tabla 15

Recomendaciones técnicas alineadas con IEEE 802.11 y controles complementarios para fortalecer redes Wi-Fi modernas

Criterio	Base técnica	Recomendación	Condición	Riesgo	Complemento
Selección por compatibilidad real	IEEE 802.11; perfiles WPA2/WPA3.	Elegir mecanismos según capacidades verificadas de AP, controladores y clientes.	Inventario actualizado y pruebas de interoperabilidad.	Configuraciones inoperantes o degradadas.	Define el marco técnico antes de aplicar respuestas defensivas.
Priorización de WPA3/SAE	WPA3-Personal; SAE.	Adoptar WPA3/SAE cuando el ecosistema soporte operación estable y segura.	Evitar transiciones permisivas no controladas.	Ataques a contraseñas y degradación de autenticación.	Convierte la estrategia de autenticación en una política de arquitectura.
Uso controlado de WPA2	WPA2 con AES-CCMP.	Mantener WPA2 solo donde la compatibilidad lo exija y con parámetros criptográficos vigentes.	Excluir WEP, TKIP y claves débiles.	Exposición por mecanismos heredados.	Permite continuidad sin normalizar configuraciones obsoletas.
Protección del plano de administración	PMF / IEEE 802.11w integrado en IEEE 802.11.	Establecer PMF como obligatorio cuando todos los clientes lo soporten.	Verificar comportamiento de asociación y roaming.	Falsificación y manipulación de tramas robustas.	Fortalece estructuralmente la continuidad del enlace.
Control de acceso empresarial	IEEE 802.1X; EAP-TLS; AAA/RADIUS.	Aplicar autenticación individual basada en certificados y políticas centralizadas.	PKI gestionada, validación de certificados y alta disponibilidad.	Claves compartidas, suplantación y baja trazabilidad.	Traslada el control desde la contraseña común hacia la identidad.
Separación de dominios WLAN	VLAN, roles y políticas de acceso asociadas a WLAN.	Separar redes corporativas, invitados, IoT y administración.	Reglas de mínimo privilegio y control entre segmentos.	Movimiento lateral y exposición de recursos internos.	Reduce el alcance de los incidentes identificados en la Tabla 15.

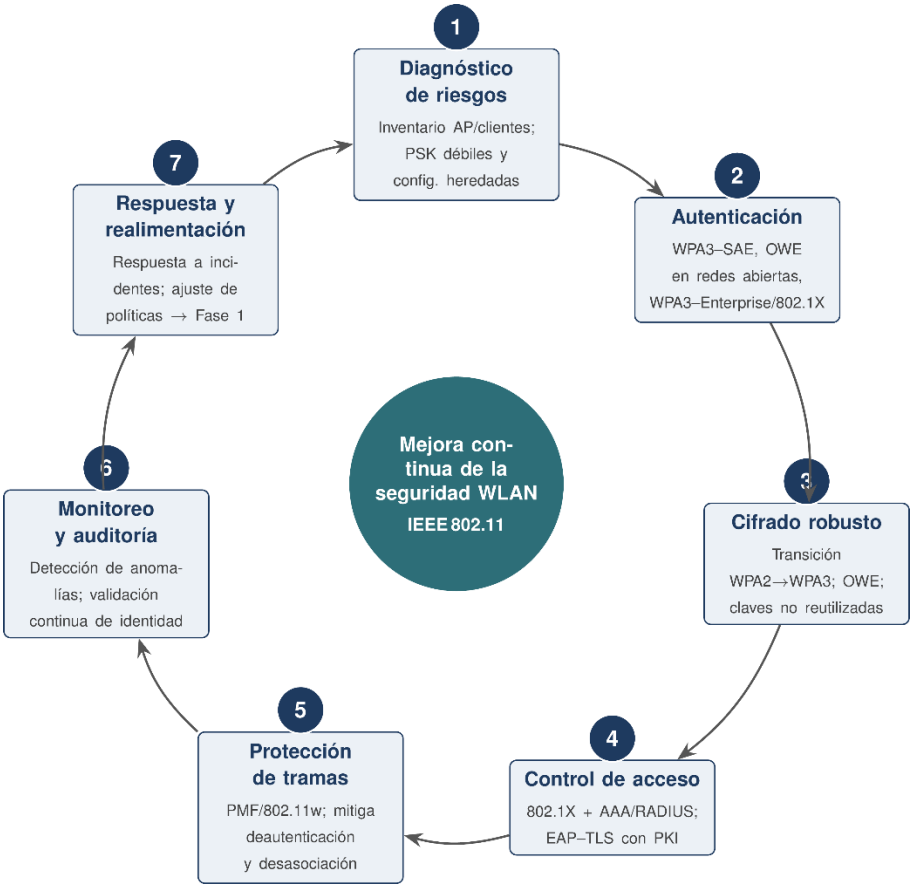
Criterio	Base técnica	Recomendación	Condición	Riesgo	Complemento
Retiro gradual de configuraciones heredadas	Compatibilidad IEEE 802.11 y perfiles de seguridad.	Planificar la eliminación de clientes y modos que obliguen a reducir el nivel de protección.	Migración por etapas y segmento temporal aislado.	Downgrade y dependencia de controles obsoletos.	Evita que la compatibilidad debilite la arquitectura completa.
Gestión de firmware y compatibilidad	AP, controladores y clientes IEEE 802.11.	Mantener versiones soportadas y evaluar cambios antes de desplegarlos.	Inventario, ventanas de mantenimiento y capacidad de reversión.	Vulnerabilidades conocidas y fallas de interoperabilidad.	Sostiene la eficacia de los mecanismos preventivos.
Supervisión del entorno inalámbrico	Monitoreo WLAN; WIDS/WIPS.	Detectar AP no autorizados, cambios anómalos y patrones de asociación inusuales.	Cobertura de monitoreo y criterios de alerta definidos.	Rogue AP, evil twin y actividad no autorizada.	Aporta visibilidad continua a las acciones de mitigación.
Revisión de acceso y trazabilidad	AAA, registros WLAN y políticas de identidad.	Revisar periódicamente cuentas, certificados, privilegios y eventos de acceso.	Registros íntegros, sincronización temporal y responsables definidos.	Persistencia de accesos y falta de atribución.	Mantiene vigentes las decisiones de autorización.
Criterios diferenciados por generación	IEEE 802.11ac, 802.11ax y 802.11be.	Ajustar los controles a capacidades, bandas, densidad y coexistencia de cada generación.	No asumir que una generación nueva garantiza seguridad por sí sola.	Aplicación uniforme de controles incompatibles o insuficientes.	Contextualiza las estrategias para Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7.
Administración integrada de seguridad	Autenticación, cifrado, PMF, segmentación y monitoreo.	Gestionar los controles como una arquitectura coordinada y revisable.	Gobernanza, responsables, métricas y ciclo de mejora.	Controles aislados y brechas entre configuración y operación.	Integra prevención, detección y mitigación en un mismo modelo.

Nota. Se entregan recomendaciones aplicables para entornos personales como empresariales y redes abiertas o cerradas

La Tabla 15 nos ayuda a comprender que aplicar estas alternativas de forma diferenciada permite mantener controles adecuados en Wi-Fi 5 y, a la vez, sacar provecho de los mecanismos modernos en Wi-Fi 6 y Wi-Fi 7. Combinar autenticación robusta, cifrado vigente, PMF, control empresarial, segmentación y monitoreo reduce la exposición a credenciales débiles, infraestructura fraudulenta, accesos no autorizados y configuraciones heredadas, sin depender de una sola medida de seguridad.

Figura 15

Modelo cíclico de fortalecimiento continuo de la seguridad de acceso WLAN en redes IEEE 802.11



Nota. Elaboración propia del autor. Síntesis del proceso de mejora contínua propuesta por el autor para redes wifi-modernas.

El ciclo mostrado en la figura 15 nos permite partir de la identificación de la exposición de los riesgos tanto administrativos como del usuario y posteriormente el ciclo continúa con el aseguramiento de la autenticación mediante mecanismos actuales y robustos.

En el ciclo de mejora continua del aseguramiento de la red wifi el tercer paso consiste saber elegir el mecanismo robusto de cifrado considerando su versión más actual, posteriormente luego de asegurar los aspectos criptográficos es necesario establecer mecanismos de vigilia de la autenticación para garantizar que el servidor confirme que el suplicante es quien realmente dice ser y no se trate de una suplantación.

La fase final del ciclo consiste en el monitoreo constante y auditoria permanente de los usuarios que acceden y los intentos no exitosos, una red sin principios de gestión es un blanco fácil de los atacantes, por ello es

necesaria la configuración de protocolos de alertas temprana, sensores que eleven el incidente al terminal de gestión de riesgos.

Esta secuencia garantizará la mejora continua y la preparación del personal ante eventos que puedes ser un positivo verdadero o en su defecto identificar los falsos positivos.

3.6. Discusión de resultados y validación de hipótesis

El peligro en figura de amenazas y vulnerabilidades se puede afirmar con certeza que no provienen de una fuente única, sino que a lo largo del estudio se ha determinado que se originan por muchas causas probables estudiadas y a su vez identificadas, ante ello se establecieron buenas prácticas y controles sin perder el horizonte del del análisis de la causa efecto.

La figura 14 nos amplía el panorama para identificar el vector de amenazas que se amplifican por las debilidades existentes y ante esto se proponen medidas y controles de mitigación, esto resume la intención del autor de analizar los principales actores, que, aunque pueden ampliarse a muchos elementos más, estos terminan siendo los más relevantes en las redes inalámbricas contemporáneas.

La revisión bibliográfica fue la base para la construcción de modelo cíclico de aplicación de mecanismos de aseguramientos, se optó por priorizar artículos de alto impacto donde se analicen las fuentes de problemas de seguridad en redes wifi-modernas y los mecanismos idóneos para mitigarlas.

En cada una de las tablas que se muestran en los resultados se encuentra el resumen de los hallazgos más importantes que permiten el cumplimiento de los objetivos de la investigación, donde podrán encontrar resumido y sintetizado aspectos relevantes como las amenazas y debilidades identificadas, la comparación de los mecanismos de autenticación actuales, las estrategias de prevención y mitigación y sobre todo las recomendaciones técnicas, controles para fortalecer los mecanismos de autenticación frente a las amenazas actuales cumpliendo sobremanera los objetivos planteados.

La hipótesis se fundamenta y cumple con la aseveración de que ningún control aislado cubre todas las amenazas, sino que es necesario implementar

un conjunto de estrategias complementarias para mejora la autenticación, la confidencialidad, la integridad, la disponibilidad y la trazabilidad. Eso sí, la hipótesis queda sustentada desde lo documental y lo técnico, condicionada a que haya compatibilidad, configuración correcta, administración continua y monitoreo.

CONCLUSIONES

La presente revisión utilizo una revisión sistemática basada en el método PRISMA que obtuvo como resultante 53 fuentes únicas y dejó una base documental trazable para poder asociar los mecanismos de autenticación y cifrado, versus las amenazas y debilidades más relevantes caracterizadas en el documento. Los factores predominantes son la debilidad en credenciales, el uso de protocolos heredados y las configuraciones vulnerables e inseguras. Otro elemento que afecta es la no protección de las tramas de control y la carente administración del versionamiento del firmware.

Un hallazgo importante ha sido determinar que la autenticación, el cifrado y el acceso rara vez nacen de una sola vulnerabilidad sino del conjunto de elementos y por ello se establecen una serie de mecanismos que permiten identificar como se interrelacionan para afrontarlos y proponer alternativas de mitigación cumpliendo con el objetivo de analizar los principales mecanismos de prevención y mitigación.

Se elaboró una tabla para proponer alternativas de fortalecimiento de seguridad, así como buenas prácticas administrativas y técnicas para los responsables de la configuración de los equipos y para los usuarios finales afín de que se evite cometer errores comunes descritos en los resultados.

Se puede confirmar el cumplimiento de los objetivos trazados al inicio de estudio siguiendo un camino evidenciado en los soportes documentales de la trazabilidad de la investigación y de la validación de las hipótesis que se describen en capítulos previos.

RECOMENDACIONES

Se sugiere que el presente estudio migre a la fase de exploración y se elaboren escenarios de simulación donde se pongan a prueba las teorías y se afinen y validen las mejores estrategias propuestas confirmando lo planteado para ofrecer una guía manual de configuraciones seguras genéricas independiente de los fabricantes.

Se recomienda a todo administrador en primera instancia realizar una auditoria de los algoritmos y mecanismos propuestos afín de detectar las vulnerabilidades y amenazas a las que están expuestos, puntualmente analice los tipos de ataques propuesto para identificar posibles debilidades y en función de aquello plantear las estrategias o buenas prácticas propuestas.

Es importante distinguir a las redes residenciales, corporativas tipo hot spot y las redes itinerantes que ofrecen en indoor las empresas para garantizar la movilidad de los usuarios y segmentar posibles alternativas y estrategias de mitigación como casos de estudios independientes que puedan ser evaluados a futuro para establecer estrategias de hardening basado en el usuario y el tipo de servicio wifi.

REFERENCIAS BIBLIOGRÁFICAS

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

Ali, A. M., Hassan, M. R., al-Qerem, A., Hamarsheh, A., Al-Qawasmi, K., Aljaidi, M., Abu-Khadrah, A., Kaiwartya, O., & Lloret, J. (2023). Towards a Smart Environment: Optimization of WLAN Technologies to Enable Concurrent Smart Services. *Sensors*, *23*(5), 2432. https://doi.org/10.3390/s23052432

Al-Saggaf, Y., Nguyen, L., & Sanderson, P. (2020). The Ethics of Lamers: The Use of Publicly Available Hacking Tools by Cybercriminals. *Journal of Business Ethics*.

Bispham, M., Creese, S., Dutton, W. H., Esteve-Gonzalez, P., & Goldsmith, M. (2021). Cybersecurity in Working from Home: An Exploratory Study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3897380

Burbano, K. V. (2015). *Incidencia de las herramientas de repaso en los resultados de la evaluación de competencias específicas de los alumnos de 10mo nivel*.

Chalyi, O. (2025). Assessing Wi-Fi Security Protocols: A Study of Dictionary Attack Performance. *Baltic Journal of Modern Computing*, *13*(3). https://doi.org/10.22364/bjmc.2025.13.3.03

Chatzisofroniou, G., & Kotzanikolaou, P. (2022). Exploiting WiFi usability features for association attacks in IEEE 802.11: Attack analysis and mitigation controls1. *Journal of Computer Security*, *30*(3), 357–380. https://doi.org/10.3233/JCS-210036

Chen, C., Chen, X., Das, D., Akhmetov, D., & Cordeiro, C. (2022). Overview and Performance Evaluation of Wi-Fi 7. *IEEE Communications Standards Magazine*, *6*(2), 12–18. https://doi.org/10.1109/MCOMSTD.0001.2100082

Cisco Systems, I. (2009). *Fundamentos de Redes Inalámbricas* (Pearson, Ed.; 2nd ed.).

Cisco Systems, Inc. (2023). *Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide*. 1–36. https://www.cisco.com/c/en/us/td/docs/wireless/outdoor_industrial/iw6300/software/config/guide/b-cos-wgb-deploy-guide.html?utm_source=chatgpt.com

Cybersecurity Ventures. (2022, September 30). *El costo global del cibercrimen en 2025 ascenderá a un total de US$10,5 billones*. Https://Www.Larepublica.Co/Empresas/El-Costo-Global-Del-Cibercrimen-En-2025-Ascendera-a-Un-Total-de-Us-10-5-Billones-3458183.

Dalal, N., Akhtar, N., Gupta, A., Karamchandani, N., Kasbekar, G. S., & Parekh, J. (2022). A Wireless Intrusion Detection System for 802.11 WPA3 Networks. *2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 384–392. https://doi.org/10.1109/COMSNETS53615.2022.9668542

de Curtò, J., de Zarzà, I., Cano, J.-C., & Calafate, C. T. (2024). Enhancing Communication Security in Drones Using QRNG in Frequency Hopping Spread Spectrum. *Future Internet*, *16*(11), 412. https://doi.org/10.3390/fi16110412

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. Https://Www.Enisa.Europa.Eu/Topics/Cyber-Threats/Threat-Landscape.

Farej, Z. K., & Ali, O. M. (2021). On the evaluation of the IEEE 802.11ac WLAN performance with QoS deployment. *Indonesian Journal of Electrical Engineering and Computer Science*, *24*(3), 1618. https://doi.org/10.11591/ijeecs.v24.i3.pp1618-1627

Ficara, D., Garroppo, R. G., & Henry, J. (2024). A Tutorial on Privacy, RCM and Its Implications in WLAN. *IEEE Communications Surveys & Tutorials*, *26*(2), 1003–1040. https://doi.org/10.1109/COMST.2023.3345746

Fortinet. (2026). *INFORME GLOBAL PANORAMA DE AMENAZAS 2025*. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf

Halbouni, A., Ong, L. Y., & Leow, M. C. (2023a). Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access*, *11*, 112438–112450. https://doi.org/10.1109/ACCESS.2023.3322931

Halbouni, A., Ong, L.-Y., & Leow, M.-C. (2023b). Wireless Security Protocols WPA3: A Systematic Literature Review. *IEEE Access*, *11*, 112438–112450. https://doi.org/10.1109/ACCESS.2023.3322931

Harkat, H., Monteiro, P., Gameiro, A., Guiomar, F., & Farhana Thariq Ahmed, H. (2022). A Survey on MIMO-OFDM Systems: Review of Recent Trends. *Signals*, *3*(2), 359–395. https://doi.org/10.3390/signals3020023

Hasan, M., Thakur, J. M., & Podder, P. (2015). Design and Implementation of FHSS and DSSS for Secure Data Transmission. *International Journal of Signal Processing Systems*, *4*(2). https://doi.org/10.12720/ijsps.4.2.144-149

Hsu, F.-H., Wu, M.-H., Hwang, Y.-L., Lee, C.-H., Wang, C.-S., & Chang, T.-C. (2022). WPFD: Active User-Side Detection of Evil Twins. *Applied Sciences*, *12*(16), 8088. https://doi.org/10.3390/app12168088

Hucaby, Dave. (2016). *CCNA wireless 200-355 official cert guide* (Official Cert Guide). Cisco Press.

Institute of Electrical and Electronics Engineers [IEEE]. (2021). *IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. IEEE. https://doi.org/10.1109/IEEESTD.2021.9363693

Joseph, G., Osamor, J., & Olajide, F. (2024). A Systematic Review of Network Packet Sniffing Tools for Enhancing Cybersecurity in Business Applications. *International Journal of Intelligent Computing Research*, *15*(1), 1292–1307. https://doi.org/10.20533/ijicr.2042.4655.2024.0157

Karamyshev, A., Levitsky, I., Bankov, D., & Khorov, E. (2025). A Tutorial on Wi-Fi 8: The Journey to Ultra High Reliability. *Problems of Information Transmission*, *61*(2), 164–210. https://doi.org/10.1134/S003294602502005X

Kasana, H. (2021). Top 10 WiFi Security Risks You Must Know About. *Https://Resources.Infosecinstitute.Com/*.

Ko, K., & Wang, H. (2024). Noise-Canceling Channel Estimation Schemes Based on the CIR Length Estimation for IEEE 802.11p/OFDM Systems. *Electronics*, *13*(6), 1110. https://doi.org/10.3390/electronics13061110

Lin, C.-H., Cheng, M.-H., Hwang, W.-S., Shieh, C.-K., & Wei, Y.-H. (2023). A Rapidly Adaptive Collision Backoff Algorithm for Improving the Throughput in WLANs. *Electronics*, *12*(15), 3324. https://doi.org/10.3390/electronics12153324

Louca, C., Peratikou, A., & Stavrou, S. (2023). A novel Evil Twin MiTM attack through 802.11v protocol exploitation. *Computers & Security*, *130*, 103261. https://doi.org/10.1016/j.cose.2023.103261

Lounis, K., Ding, S. H. H., & Zulkernine, M. (2022). *Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3* (pp. 235–252). https://doi.org/10.1007/978-3-031-08147-7_16

Mortágua, D., Zúquete, A., & Salvador, P. (2024). Enhancing 802.1X authentication with identity providers using EAP-OAUTH and OAuth 2.0. *Computer Networks*, *244*, 110337. https://doi.org/10.1016/j.comnet.2024.110337

MyCert. (2026). *Reported Incidents based on General Incident Classification Statistics 2026*. 1. https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169-66677d694932&id=17e4d4cf-1ce2-4ceb-85d2-6cdf484b9faa

Mykhaylova, O., & Nakonechny, T. (2024). SECURITY ANALYSIS OF MODERN WI-FI NETWORK PROTECTION PROTOCOLS: ASSESSMENT OF WPA3 PROTOCOL RESISTANCE DURING ATTACKS BASED ON DRAGONBLOOD UTILITY. *Computer Systems and Network*, *6*(1), 133–147. https://doi.org/10.23939/csn2024.01.133

National Security Agency. (2023). *Best Practices for Securing Your Home Network*. https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICES_FOR_SECURING_YOUR_HOME_NETWORK.PDF

Qadri, Y. A., Zulqarnain, Nauman, A., Musaddiq, A., Garcia-Villegas, E., & Kim, S. W. (2022). Preparing Wi-Fi 7 for Healthcare Internet-of-Things. *Sensors*, *22*(16), 6209. https://doi.org/10.3390/s22166209

Qureshi, I. A., & Asghar, S. (2023a). A Systematic Review of the IEEE-802.11 Standard's Enhancements and Limitations. *Wireless Personal Communications*, *131*(4), 2539–2572. https://doi.org/10.1007/s11277-023-10553-7

Qureshi, I. A., & Asghar, S. (2023b). A Systematic Review of the IEEE-802.11 Standard's Enhancements and Limitations. *Wireless Personal Communications*, *131*(4), 2539–2572. https://doi.org/10.1007/s11277-023-10553-7

Ramón, L. (2015). *Sistema de Radiocomunicaciones* (Paraninfo, Ed.).

Rasool, M. B., Shah, U. M., Imran, M., Minhas, D. M., & Frey, G. (2025). Invisible eyes: Real-time activity detection through encrypted Wi-Fi traffic without machine learning. *Internet of Things*, *31*, 101602. https://doi.org/10.1016/j.iot.2025.101602

Rosales, J., Martínez, R., & Castro, E. (2022). Análisis del fenómeno del hacking en México. *Revista Científica de Seguridad Informática*, 1–14.

Sayago-Heredia, J. (2022). Ciberseguridad en Ecuador y Latinoamérica. *Killkana Técnica*, *5*(1). https://doi.org/10.26871/killkanatecnica.v5i1.957

Sethi, M., Preuß Mattsson, J., & Turner, S. (2022). *Handling Large Certificates and Long Certificate Chains in TLS-Based EAP Methods*. https://doi.org/10.17487/RFC9191

Soltani, M., Othman, Z., & Ibrahim, R. (2021). Cybersecurity awareness among social media users: A conceptual model. Journal of Information Privacy and Security. *Journal of Information Privacy and Security*, 49–63.

Tanenbaum, A. S. ., Wetherall, D. J. ., & Romero Elizondo, A. Vidal. (2012). *Redes de computadoras*. Pearson Educación.

Tareef, A., Allawi, Y. M., Alkasasbeh, A. A., Abadleh, A., Alamro, W., Alghamdi, M., Zreikat, A. I., & Kang, H. (2025). A machine learning approach for detecting WPA3 downgrade attacks in next-generation Wi-Fi systems. *PLOS One*, *20*(9), e0331443. https://doi.org/10.1371/journal.pone.0331443

TechNadu. (2023, April 1). *8 Common Wi-Fi Security Vulnerabilities and How to Avoid Them*. Https://Www.Technadu.Com/Common-Wifi-Security-Vulnerabilities-How-to-Avoid-Them/80166/.

Telco. (2015, February). *how does mimo work*. Https://Www.Telcoantennas.Com.Au/Site/How-Does-Mimo-Work.

Tleuberdin, S., Issainova, A., Adamova, A., Aidynov, T., Samashova, G., & Satybaldina, D. (2025). Analysis of Vulnerabilities and Practical Attacks on WPA3-Enterprise in Corporate Wireless Networks. *Procedia Computer Science*, *272*, 613–618. https://doi.org/10.1016/j.procs.2025.10.256

Trînc, E.-C., Ancuți, C., Vesa, A., Simu, C., Niță, V.-A., & Stolojescu-Crişan, C. (2026). 3D Urban Outdoor WiFi 7 Network Planning and Analysis Using Ray-Tracing and Machine Learning: Transformer-Based Surrogate Modeling for High-Resolution Digital Twin. *Sensors*, *26*(7), 2223. https://doi.org/10.3390/s26072223

Trochim, W., Donnely, J., & Arora, K. (2015). *Research Methods - The Essentials Knowledge Base* (Cengage Learning, Ed.; 2nd ed., Vol. 1).

Veroni, E., Ntantogian, C., & Xenakis, C. (2022). A large-scale analysis of Wi-Fi passwords. *Journal of Information Security and Applications*, *67*, 103190. https://doi.org/10.1016/j.jisa.2022.103190

Wang, R., Lin, Z., Du, J., Wu, J., & He, X. (2017). Direct Sequence Spread Spectrum-Based PWM Strategy for Harmonic Reduction and Communication. *IEEE Transactions on Power Electronics*, *32*(6), 4455–4465. https://doi.org/10.1109/TPEL.2016.2597005

WE ARE SOCIAL. (2022, October 28). *THE GLOBAL STATE OF DIGITAL EN OCTUBRE 2022*. Https://Wearesocial.Com/Es/Blog/2022/10/the-Global-State-of-Digital-in-October-2022/.

Xiao, M., Cheng, W., Fan, H., Shao, H., Li, Z., & Zhong, Y. (2025). Formal Analysis of EAP-TLS Protocol Based on Logic of Events. *Symmetry*, *17*(9), 1456. https://doi.org/10.3390/sym17091456

GLOSARIO DE TÉRMINOS

WLAN.- Red de área local que utiliza comunicación inalámbrica.

IEEE 802.11.- Familia de estándares que regula el funcionamiento de las redes Wi-Fi.

Wi-Fi 5.- Generación inalámbrica basada en el estándar IEEE 802.11ac.

Wi-Fi 6.- Generación inalámbrica basada en IEEE 802.11ax, orientada a mayor eficiencia.

Wi-Fi 7.- Generación inalámbrica basada en IEEE 802.11be, de alta capacidad y baja latencia.

Access Point.- Dispositivo que permite conectar equipos inalámbricos a una red.

WPA2.- Perfil de seguridad Wi-Fi que utiliza autenticación y cifrado robusto.

WPA3.- Perfil de seguridad Wi-Fi que fortalece la autenticación y protección criptográfica.

SAE.- Mecanismo de autenticación utilizado en WPA3-Personal.

OWE.- Mecanismo que cifra el tráfico en redes Wi-Fi abiertas.

PSK.- Clave precompartida utilizada para autenticar dispositivos en una WLAN.

AES-CCMP.- Mecanismo de cifrado e integridad empleado en redes Wi-Fi seguras.

IEEE 802.1X.- Marco de control de acceso basado en autenticación por identidad.

EAP-TLS.- Método de autenticación mutua basado en certificados digitales.

RADIUS/AAA.- Servicio centralizado de autenticación, autorización y registro.

PMF.- Mecanismo de protección de determinadas tramas de administración WLAN.

Evil Twin.- Punto de acceso falso que imita una red Wi-Fi legítima.

Rogue AP.- Punto de acceso no autorizado conectado o presente en una red.

Man-in-the-Middle.- Ataque en el que un tercero intercepta la comunicación entre dos entidades.

Downgrade.- Ataque que fuerza el uso de un mecanismo de seguridad menos robusto.

DECLARACIÓN Y AUTORIZACIÓN

Yo, **DARIO FERNANDO HUILCAPI SUBÍA**, con C.C: # **0920375177** autor del trabajo de titulación: **"Análisis de los mecanismos de prevención y mitigación de ataques contra la autenticación y el cifrado en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 para el fortalecimiento de la seguridad de acceso"**. previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 14 de julio de 2026

f. _____

Ing. Darío Fernando Huilcapi Subía

C.C: 0920375177

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	Análisis de los mecanismos de prevención y mitigación de ataques contra la autenticación y el cifrado en redes Wi-Fi 5, Wi-Fi 6 y Wi-Fi 7 para el fortalecimiento de la seguridad de acceso		
AUTOR(ES)	Darío Fernando Huilcapi Subía		
REVISOR(ES)/TUTOR(ES)	Tutor: Ph.D. Celso Bayardo Bohórquez Escobar Revisores: Mgtr. Nestor Armando Zamora Cedeño, Mgtr. Ronnie Alexander Bonilla Sánchez		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Subsistema de Posgrado		
CARRERA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	14 de julio de 2026	**No. DE PÁGINAS:**	81
ÁREAS TEMÁTICAS:	Redes Inalámbricas 802.11, Seguridad en redes wlan. Prevención y mitigación de amenazas,		
PALABRAS CLAVES/ KEYWORDS:	Seguridad WLAN, IEEE 802.11, WPA3, autenticación inalámbrica, cifrado, control de acceso, revisión sistemática PRISMA, Wi-Fi 6.		

RESUMEN/ABSTRACT:

Las redes Wi-Fi permiten la conexión universal de dispositivos inalámbricos en diferentes ámbitos, pero su evolución no eliminó las amenazas de autenticación, cifrado y control de acceso. El problema abarca diferentes aspectos que afecta a factores como credencias débiles, protocolos heredados, tramas de administración desprotegidas, firmware desactualizado, segmentación deficiente e identidad de acceso limitada. El presente estudio analiza estrategias actuales para prevención y mitigación de amenaza en las redes WiFi, para recomendar alternativas que fortalezcan la seguridad de acceso. La metodología de investigación empleó un enfoque descriptivo y explicativo, además de un diseño documental, utilizando el método PRISMA para la revisión sistemática que se complementó con un análisis documental, técnico y comparativo. Se obtuvieron 53 fuentes bibliográficas que caracterizan tanto las amenazas, como las vulnerabilidades, además de los mecanismos y condiciones adecuados para su implementación. Posteriormente los resultados sugieren que WPA2, WPA3, SAE, OWE, IEEE 802.1X, EAP-TLS y PMF cumplen funciones distintas y pero que a su vez complementarias permitiendo inferir que ningún control aplicable aislado permitiría cubrir la variedad de escenarios susceptibles de riesgos. Se comprendió y determinó que las diversas generaciones de redes Wi-Fi no son la causa principal por la cual están expuestas a vulnerabilidades y amenazas, sino que son un conjunto de factores como la compatibilidad, la configuración, la gestión de credenciales, la actualización, la segmentación y un monitoreo sostenido que permiten contar con un esquema relativamente seguro. El aporte del estudio consiste en establecer una gama de estrategias que confronta las amenazas y debilidades desembocando en mecanismos de prevención, mitigación y fortalecimiento estructural. Se concluye que una arquitectura de defensa en profundidad, con autenticación robusta, cifrado vigente, protección de tramas, control de identidad, hardening y supervisión, reduce la superficie de exposición y mejora la seguridad operativa.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** 0994915543	E-mail: **dario.huilcapi@gmail.com**
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE):	**Nombre: Ph.D. Celso Bayardo Bohórquez Escobar**	
	Teléfono: +593-995147293	
	E-mail: celso.bohorquez@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	