UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA

FACSISTEL

INGENIERÍA EN TELECOMUNICACIONES

TRABAJO DE INTEGRACIÓN CURRICULAR

Implementación de un sistema móvil y automatizado para la auditoría de seguridad en redes inalámbricas de doble banda en entornos institucionales

Rodríguez Suárez Arnold Jefferson

Dirigido por

Ing. Luis Miguel Amaya Fariño, Mgtr.

LA LIBERTAD - 2026

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. Ronald Rovira Jurado, PhD.
DIRECTOR DE LA CARRERA

Ing. Luis Amaya Fariño, Mgtr.
TUTOR

Ing. Muzzio Arguello Javier, Mgtr.
DOCENTE ESPECIALISTA

Ing. Luis Amaya Fariño, Mgtr.
DOCENTE GUÍA UIC

Ing. Corina Gonzabay De La A, Mgtr.
SECRETARIA

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Rodriguez Suarez Arnold Jefferson**

DECLARO QUE:

El trabajo de Titulación, **Implementación de un sistema móvil y automatizado para la auditoría de seguridad en redes inalámbricas de doble banda en entornos institucionales** de un previo a la obtención del título en Ingeniero en Telecomunicaciones, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 24 días del mes de agosto del año 2026

EL AUTOR

Rodríguez Suárez Arnold Jefferson

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por **Rodríguez Suárez Arnold Jefferson**, como requerimiento para la obtención del título de Ingeniero en telecomunicaciones.

La Libertad, a los 24 días del mes de agosto del año 2026

TUTOR

Ing. Luis Miguel Amaya Fariño, Mgtr.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Rodríguez Suárez Arnold Jefferson**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor

Santa Elena, a los 24 días del mes de agosto del año 2026

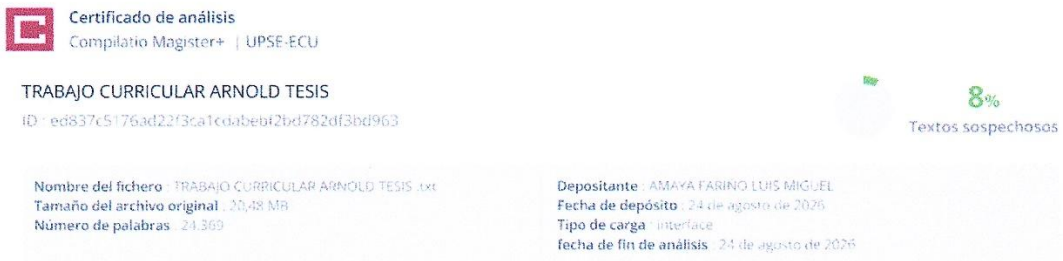
EL AUTOR

Rodríguez Suárez Arnold Jefferson

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado **Implementación de un sistema móvil y automatizado para la auditoría de seguridad en redes inalámbricas de doble banda en entornos institucionales**, presentado por el estudiante, **Rodríguez Suárez Arnold Jefferson** fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al %, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.


Certificado de análisis
Compilatio Magister+ | UPSE-ECU

TRABAJO CURRICULAR ARNOLD TESIS

ID : ed837c5176ad22f3ca1cdabebf2bd782df3bd963

8%
Textos sospechosos

Nombre del fichero : TRABAJO CURRICULAR ARNOLD TESIS.txt
Tamaño del archivo original : 20,48 MB
Número de palabras : 24.369

Depositante : AMAYA FARIÑO LUIS MIGUEL
Fecha de depósito : 24 de agosto de 2026
Tipo de carga : interface
fecha de fin de análisis : 24 de agosto de 2026

TUTOR

Ing. Luis Miguel Amaya Fariño, Mgtr.

Agradecimiento

En primer lugar, agradezco a Dios por darme la oportunidad de despertar cada día, por regalarme la vida, la fortaleza y la sabiduría necesarias para llegar hasta este momento tan importante. En segundo lugar, quiero agradecer a mi pareja por el apoyo que me ha brindado durante este proceso y, de manera muy especial, a su familia, Lindao González, por abrirme las puertas de su hogar, acogerme con cariño y cuidarme como a un hijo más.

Agradezco profundamente a mi madre, por todo el apoyo, amor y sacrificio que me ha brindado desde el día en que nací hasta el día de hoy. Este logro también es de ella. Finalmente, quiero agradecer a todos mis compañeros e ingenieros que formaron parte de esta etapa tan bonita de mi vida. Cada experiencia, cada aprendizaje y cada momento compartido contribuyeron a llegar hasta aquí. Gracias a todos por ser parte de este camino.

Rodríguez Suárez Arnold Jefferson

Dedicatoria

Dedico este logro, en primer lugar, a mi padre, que sé que desde el cielo se encuentra orgulloso de verme alcanzar esta meta. Aunque hoy no pueda tenerlo físicamente a mi lado, su recuerdo, sus enseñanzas y su amor han sido parte fundamental de este camino. También a mi hermano, que hoy descansa en el cielo. Sé que, desde donde se encuentre, comparte conmigo esta alegría y este momento tan importante de mi vida.

Finalmente, dedico este logro a todas las personas que creyeron en mí, que me apoyaron y que nunca dudaron de que podía alcanzar este logro. Muchas gracias.

Arnold Jefferson Rodríguez Suárez

Índice general

Índice de tablas

Índice de figuras

Resumen

El crecimiento de las redes inalámbricas y la incorporación de tecnologías como WiFi 6 y WiFi 6E han incrementado la complejidad de la seguridad en entornos institucionales. Ante las limitaciones de las auditorías tradicionales, el presente trabajo tuvo como objetivo implementar un sistema móvil y automatizado de auditoría inalámbrica mediante el WiFi Pineapple Pager, orientado a la identificación de vulnerabilidades y generación de registros forenses en redes de 2.4 GHz y 5 GHz. La metodología se desarrolló mediante investigación documental, diseño experimental, implementación de payloads en DuckyScript y Bash, y pruebas controladas en el laboratorio de la Universidad Estatal Península de Santa Elena (UPSE).

Los resultados permitieron identificar puntos de acceso y dispositivos de usuarios, además de procesar 286 capturas de *handshakes*, de las cuales 161 fueron únicas y 145 resultaron criptográficamente válidas, alcanzando una tasa de éxito del 90,1 %. El análisis evidenció que el 44,4 % de las redes operaban sin cifrado, el 100 % no utilizaba WPA3 y las redes WPA2 evaluadas no contaban con *Protected Management Frames* (PMF). Asimismo, mediante VERDANDI v2.0 se identificaron 102 huellas digitales asociadas a 78 direcciones MAC físicas, mientras que el *payload vuln_score* determinó que el 77,8 % de los puntos de acceso presentaba un nivel de riesgo alto o crítico. Se concluye que el sistema implementado constituye una herramienta eficaz para la detección de vulnerabilidades y generación de evidencias forenses, recomendándose la migración hacia WPA3, la activación de PMF y la realización periódica de auditorías de seguridad.

Palabras clave: Auditoría inalámbrica; WiFi Pineapple Pager; vulnerabilidades; redes WLAN; automatización; registro forense; seguridad inalámbrica.

Abstract

The growth of wireless networks and the incorporation of technologies such as WiFi 6 and WiFi 6E have increased the complexity of security in institutional settings. Faced with the limitations of traditional audits, the present work aimed to implement a mobile and automated wireless audit system through the WiFi Pineapple Pager, designed to identify vulnerabilities and generate forensic records on 2.4 GHz and 5 GHz networks. The methodology was developed through documentary research, experimental design, implementation of payloads in DuckyScript and Bash, and controlled tests in the laboratory at the State University of the Santa Elena Peninsula (UPSE).

The results enabled the identification of access points and client devices, in addition to processing 286 handshake captures, of which 161 were unique and 145 were cryptographically valid, achieving a success rate of 90.1 %. The analysis evidenced that 44.4 % of the networks operated without encryption, 100 % did not use WPA3, and the WPA2 networks evaluated did not implement Protected Management Frames (PMF). Likewise, through VERDANDI v2.0, 102 fingerprints associated with 78 physical MAC addresses were identified, while the vuln_score payload determined that 77.8 % of the access points presented a high or critical risk level. It is concluded that the implemented system constitutes an effective tool for vulnerability detection and forensic evidence generation, recommending migration to WPA3, activation of PMF, and periodic security audits.

Keywords: Wireless auditing; WiFi Pineapple Pager; vulnerabilities; WLAN networks; automation; forensic record; wireless security.

Glosario de abreviaturas

AP: Access Point (Punto de Acceso).

BSSID: Basic Service Set Identifier (Identificador del conjunto de servicios básicos).

BYOD: Bring Your Own Device (Trae tu propio dispositivo).

COIP: Código Orgánico Integral Penal.

DDoS: Distributed Denial of Service (Denegación de Servicio Distribuida).

IEEE: Institute of Electrical and Electronics Engineers (Instituto de Ingenieros Eléctricos y Electrónicos).

IoT: Internet of Things (Internet de las Cosas).

MAC: Media Access Control (Control de Acceso al Medio).

MitM: Man-in-the-Middle (Hombre en el Medio).

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología).

PMF: Protected Management Frames (Tramas de Gestión Protegidas).

RSSI: Received Signal Strength Indicator (Indicador de Intensidad de Señal Recibida).

SSID: Service Set Identifier (Identificador de Conjunto de Servicios).

SSH: Secure Shell (Intérprete de Órdenes Seguro).

UPSE: Universidad Estatal Península de Santa Elena.

WIDS: Wireless Intrusion Detection System (Sistema de Detección de Intrusiones Inalámbricas).

WLAN: Wireless Local Area Network (Red de Área Local Inalámbrica).

WPA: Wi-Fi Protected Access (Acceso Protegido Wi-Fi).

WPA2: Wi-Fi Protected Access 2 (Acceso Protegido Wi-Fi 2).

Introducción

El crecimiento acelerado de las redes inalámbricas y la adopción de tecnologías como WiFi 6 y WiFi 6E han transformado el panorama de la conectividad en entornos institucionales, educativos y corporativos. La mayoría de las instituciones aún utilizan principalmente las bandas de 2.4 GHz y 5 GHz, a pesar de los esfuerzos internacionales por migrar a la banda de 6 GHz para reducir la congestión del espectro. Sin embargo, la persistencia de protocolos de seguridad obsoletos en estas bandas expone las comunicaciones a vulnerabilidades críticas, comprometiendo la confidencialidad e integridad de la información.

La complejidad y el dinamismo de los entornos inalámbricos actuales no pueden abordarse adecuadamente con las soluciones de auditoría tradicionales, que dependen de estaciones fijas y procedimientos manuales. En este contexto, un dispositivo de auditoría móvil y automatizado, como el WiFi Pineapple Pager, representa una alternativa viable para la detección proactiva de vulnerabilidades y la generación de evidencias forenses. Con el fin de identificar vulnerabilidades en las redes contemporáneas (2.4 GHz y 5 GHz) y generar registros forenses en entornos institucionales controlados, el presente trabajo de tesis plantea la implementación de un sistema de auditoría inalámbrica móvil y automatizado basado en el WiFi Pineapple Pager.

El contexto del estudio, el problema identificado, los objetivos propuestos, el alcance, la justificación y la metodología se presentan en el Capítulo I. El marco teórico y conceptual, así como el estado del arte que sustenta la propuesta, se desarrollan en el Capítulo II. La implementación del sistema y el diseño experimental se abordan en el Capítulo III. Los resultados y su análisis cuantitativo se presentan en el Capítulo IV. Finalmente, las conclusiones y recomendaciones del estudio se presentan en el Capítulo V.

CAPÍTULO I

1.1 Antecedentes generales

Las redes inalámbricas basadas en el estándar IEEE 802.11 constituyen una infraestructura fundamental para la conectividad en entornos institucionales. Sin embargo, como se señala en [1], la evolución hacia arquitecturas que incorporan las bandas 2.4 GHz, 5 GHz y 6 GHz mediante WiFi 6E y WiFi 7 (IEEE 802.11ax/be) ha ampliado las posibilidades de conectividad y, simultáneamente, la superficie de exposición frente a amenazas de seguridad inalámbrica. Esta evolución también ha planteado nuevos desafíos relacionados con la gestión y protección de las redes, aspectos contemplados en el estándar IEEE 802.11 [2].

Los procesos tradicionales de auditoría inalámbrica, basados en paradigmas reactivos y estaciones fijas, resultan insuficientes frente a entornos dinámicos. En este sentido, [3] destacan que la proliferación de dispositivos IoT, políticas BYOD y protocolos de seguridad heredados incrementan significativamente las vulnerabilidades de red. Por su parte, [4] documenta que las metodologías convencionales de pentesting presentan limitaciones ante amenazas como *Rogue APs*, *Evil Twins*, ataques de desautenticación y captura de *handshakes*, técnicas ampliamente utilizadas contra redes modernas.

Por consiguiente, se evidencia la necesidad de sistemas de auditoría móvil optimizados para entornos institucionales con doble banda. La ausencia de herramientas portátiles y automatizadas para análisis proactivos en múltiples frecuencias dificulta la identificación temprana de vulnerabilidades, comprometiendo la confidencialidad, integridad y disponibilidad de la información.

1.2 Antecedentes específicos

1. La plataforma WiFi Pineapple de Hak5 se ha consolidado como una herramienta orientada a la auditoría de redes inalámbricas. Según la documentación técnica oficial [5], su evolución ha incorporado diferentes generaciones de hardware y capacidades destinadas a facilitar procesos de auditoría, desde dispositivos que requieren una estación de trabajo externa hasta soluciones embebidas con mayor autonomía operacional.
2. El WiFi Pineapple Tetra estableció capacidades multifrecuencia con radios de alta potencia, pero su factor de forma, peso aproximado de 450 g y dependencia de alimentación externa limitaron su despliegue a entornos estacionarios, tal como lo

documenta [4] en su implementación del dispositivo en el laboratorio de telecomunicaciones de la UPSE.

3. El WiFi Pineapple Pager representa una evolución reciente de la plataforma de Hak5, orientada a la auditoría móvil autónoma (*Untethered*). Sus especificaciones técnicas se detallan en la sección 2.1.6. En el contexto regional, su aplicación académica en sistemas de auditoría móvil dentro de entornos controlados permanece poco explorada.

1.3 Descripción del proyecto

El proyecto surge ante la necesidad de fortalecer la seguridad de las redes inalámbricas en entornos institucionales, particularmente en las bandas de 2.4 GHz y 5 GHz. Como establece el estándar IEEE 802.11ax-2021 [2] y un estudio reciente sobre seguridad en redes multibanda [6], la habilitación de la banda de 6 GHz mediante WiFi 6E ha ampliado el espectro disponible. Sin embargo, la disponibilidad de herramientas portátiles para el diagnóstico y monitoreo de estas nuevas frecuencias continúa siendo un desafío, especialmente en entornos donde la infraestructura de 6 GHz aún se encuentra en proceso de adopción. Por ello, se propone el diseño, integración y validación de una solución de auditoría inalámbrica de alta movilidad basada en el WiFi Pineapple Pager.

La propuesta transforma las capacidades nativas de escaneo del dispositivo en un sistema de monitoreo automatizado ante eventos del espectro radioeléctrico. El sistema supervisa el entorno en tiempo real, detectando anomalías como clientes asociándose a redes inseguras, presencia de balizas sospechosas (*Evil Twin*) o tramas de desautenticación anormales, siguiendo el modelo de detección de intrusiones descrito en [7].

Para ello, se integra una arquitectura modular basada en la biblioteca oficial de *payloads* de Hak5 (DuckyScript™ y Bash) [5], acoplada al motor PineAP para optimizar el procesamiento de eventos. Las acciones automatizadas incluyen el registro forense de metadatos de tramas, emisión de alertas visuales y acústicas discretas, y la captura controlada de *handshakes* WPA/WPA2 para el análisis posterior de vulnerabilidades [4], todo validado en un entorno de laboratorio institucional controlado.

1.4 Objetivos del proyecto

1.4.1 Objetivo general

Implementar un sistema de auditoría inalámbrica móvil y automatizado, basado en el WiFi Pineapple Pager, para la detección proactiva, registro forense y generación de alertas de vulnerabilidades en redes Wi-Fi modernas en entornos corporativos y educativos supervisados en las bandas de 2.4 GHz y 5 GHz.

1.4.2 Objetivos específicos

1. Configurar y optimizar el WiFi Pineapple Pager para operar como una estación de monitoreo autónoma, aprovechando su capacidad de operación en las bandas de 2.4 GHz y 5 GHz y su interfaz de usuario para el reconocimiento del espectro inalámbrico.
2. Implementar y configurar los *payloads* disponibles en la biblioteca oficial de Hak5 para automatizar procesos de reconocimiento, captura de *handshakes* y generación de notificaciones, asegurando su correcto funcionamiento en el entorno de pruebas controlado.
3. Validar el funcionamiento y rendimiento del sistema propuesto mediante pruebas controladas en un entorno institucional de la UPSE, evaluando su capacidad de detección, generación de alertas, captura y validación de evidencias de autenticación WPA/WPA2.

1.4.3 Hipótesis

La implementación del WiFi Pineapple Pager, configurado con *payloads* de automatización en Bash y DuckyScript™, permite detectar y registrar vulnerabilidades en redes Wi-Fi de 2.4 GHz y 5 GHz, alcanzando una tasa de éxito superior al 80 % en la captura y validación de evidencias de autenticación y proporcionando una respuesta oportuna ante eventos de seguridad en un entorno institucional controlado.

1.5 Alcance del proyecto

- El proyecto se limita al uso del WiFi Pineapple Pager como plataforma central de hardware para la ejecución de las auditorías.
- El desarrollo de software se centra en la instalación, configuración y validación de los *payloads* de la biblioteca oficial de Hak5, escritos en DuckyScript™ y Bash, sin modificar el código fuente base del firmware.

- Las pruebas se realizaron en un entorno controlado y autorizado, simulando una red corporativa/educativa con los dispositivos cliente y puntos de acceso legítimos y maliciosos.
- Se cubrieron técnicas de reconocimiento, monitoreo y registro forense del espectro, incluyendo la detección de puntos de acceso no autorizados (*Rogue AP*) y escenarios de suplantación (*Evil Twin*), identificación de clientes, monitoreo de espectro, y captura de *handshakes* WPA/WPA2.
- No se contemplan las modificaciones del hardware del dispositivo que vayan más allá de lo permitido por la interfaz de usuario convencional y acceso de superusuario, ni la ingeniería inversa de su firmware.
- En estricta conformidad con el marco ético y normativo vigente, no se realizarán pruebas de penetración ni escaneos en redes públicas o privadas de terceros sin el consentimiento expreso por escrito de los administradores.

1.6 Justificación

Este proyecto se organiza en torno a cuatro dimensiones clave que demuestran su aplicabilidad y viabilidad:

- **Académica:** cubre un vacío en la formación de los ingenieros de telecomunicaciones, quienes necesitan aprender tanto la teoría de redes como las técnicas prácticas más avanzadas para protegerlas. El WiFi Pineapple Pager es un dispositivo de última generación cuyo potencial educativo es inmenso, como lo documenta Hak5 en su guía técnica oficial [5].
- **Técnica:** aborda una necesidad real ya que la transición progresiva hacia WiFi 6E/7 plantea nuevos desafíos para las metodologías de auditoría inalámbrica. La norma IEEE 802.11ax 2021 [2] y el estudio reciente [6] coinciden en que la ampliación del espectro hacia la banda de 6 GHz exige herramientas capaces de monitorear simultáneamente múltiples frecuencias. Este proyecto proporciona un modelo práctico y replicable para hacerlo de forma proactiva y móvil.
- **Metodológica:** se emplean los enfoques SPICE (Security Process Improvement and Capability Determination) y PRIMA (Propósito, Relevancia, Innovación, Metodología, Aplicabilidad) como referentes para estructurar el análisis de la seguridad, la relevancia, la innovación, la metodología y la aplicabilidad de la propuesta [3]. Además, se consideran las etapas de configuración del

dispositivo, instalación y configuración de payloads, y ejecución de pruebas controladas para evaluar el funcionamiento del sistema.

- **Ética:** promueve el uso responsable y ético de las herramientas de auditoría y seguridad informática de acuerdo con las mejores prácticas del sector y los principios Hak5 para mejorar la seguridad. Todas las pruebas se ejecutan en cumplimiento del marco legal ecuatoriano, incluyendo la Ley Orgánica de Protección de Datos Personales [8].

1.7 Metodología

La presente investigación se desarrolló bajo un enfoque metodológico mixto (cualitativo y cuantitativo), estructurado en tres fases secuenciales que garantizan el rigor técnico y la validez de los resultados obtenidos:

Fase 1: investigación documental y análisis comparativo

Revisión exhaustiva de la documentación técnica oficial del WiFi Pineapple Pager, manuales de DuckyScript™ [5], estándares IEEE 802.11 (especialmente ax/be) [1], y literatura sobre pentesting WiFi. Como parte de esta fase, se elaboró una matriz de estado del arte para comparar las especificaciones técnicas, portabilidad y capacidades tri-banda del Pager frente a herramientas tradicionales y alternativas del mercado (Aircrack-ng, Kismet, Bettercap, WiFi Pineapple Mark VII y Tetra), identificando sus ventajas diferenciales y limitaciones operativas.

Fase 2: diseño experimental e implementación de la biblioteca oficial

Diseño de la arquitectura del sistema y configuración iterativa de los *payloads* de la biblioteca oficial de Hak5. La implementación se ejecutó en etapas iterativas (enfoque MVP: Producto Mínimo Viable), comenzando con la activación de payloads simples de alerta y escalando hacia módulos complejos de reconocimiento y registro forense. Se utilizó el acceso root vía SSH para la configuración, depuración de scripts en Bash/DuckyScript™ y optimización del motor PineAP.

Fase 3: pruebas controladas, validación forense y análisis estadístico

Se ejecutaron de escenarios de prueba predefinidos en el laboratorio de la UPSE, simulando una red institucional [4]. Se midieron variables cuantitativas como: número de redes y clientes detectados, *handshakes* capturados, tiempo de respuesta del sistema y precisión de las alertas, siguiendo el enfoque de detección de anomalías propuesto en [9]. Los datos recolectados fueron sometidos a un análisis estadístico y gráfico (calculando porcentajes, tasas de éxito y promedios) para evaluar objetivamente el desempeño del sistema, validar las hipótesis planteadas y verificar la eficacia del dispositivo en la generación de evidencias forenses.

CAPÍTULO II

2.1 Marco teórico

2.1.1 Evolución de las redes inalámbricas: de IEEE 802.11n a WiFi 6E/7 (802.11ax/be)

Las redes inalámbricas han evolucionado significativamente durante las últimas décadas, impulsadas por las demandas de conectividad de altas velocidades, baja latencia y soporte para entornos con alta densidad de dispositivos. Los primeros estándares IEEE 802.11 establecieron mecanismos básicos de comunicación; sin embargo, el incremento exponencial del tráfico de datos y la proliferación de dispositivos inteligentes impulsaron el desarrollo de nuevas generaciones tecnológicas orientadas a optimizar el rendimiento espectral y la eficiencia energética [3].

El estándar IEEE 802.11n introdujo tecnología MIMO (*Multiple Input Multiple Output*), incrementando la velocidad y estabilidad de las conexiones. Posteriormente, IEEE 802.11ac amplió el ancho de banda en la frecuencia de 5 GHz mejorando el rendimiento de las WLAN modernas. No obstante, el crecimiento de dispositivos IoT, servicios en la nube y aplicaciones en tiempo real evidenció la necesidad de un nuevo paradigma de conectividad de alta velocidad [6].

Como respuesta, surgió IEEE 802.11ax (WiFi 6), que incorporó tecnología como OFDMA (*Orthogonal Frequency Division Multiple Access*), MU-MIMO bidireccional y Target Wake Time (TWT), mejorando la eficiencia espectral, reduciendo la congestión y optimizando el consumo energético [10]. Posteriormente, WiFi 6E extendió estas capacidades hacia la nueva banda de 6 GHz, habilitando canales más amplios y reduciendo la interferencia presente en las bandas 2.4 GHz y 5 GHz [2].

Actualmente, IEEE 802.11be (WiFi 7) representa una nueva etapa, con operación multienlace, canales de 320 MHz y mecanismos avanzados de modulación. Sin embargo, estas mejoras tecnológicas incrementan la complejidad de la seguridad inalámbrica. Específicamente, la banda de 6 GHz exige el uso de WPA3 y *Protected Management Frames* (PMF), lo que, si bien mejora la seguridad, limita las técnicas tradicionales de auditoría (como la inyección de paquetes de desautenticación), ampliando la superficie de ataque y requiriendo nuevas metodologías de análisis [6].

La transición hacia arquitecturas tri-banda ha generado nuevos desafíos para administradores y especialistas en ciberseguridad, quienes requieren herramientas capaces de monitorear, analizar y auditar simultáneamente las bandas de 2.4 GHz, 5 GHz y 6 GHz. En este

contexto, las plataformas de auditoría inalámbrica evolucionan hacia sistemas móviles, autónomos y automatizados, capaces de realizar monitoreo proactivo y registro forense dinámico frente a amenazas emergentes en arquitecturas tri-banda [5].

2.1.2 Amenazas y vulnerabilidades en redes WiFi modernas

La evolución de las redes inalámbricas modernas ha incrementado significativamente la superficie de exposición a amenazas de ciberseguridad, especialmente en entornos institucionales donde convergen dispositivos IoT, políticas BYOD (*Bring Your Own Device*) y arquitecturas de alta densidad [3].

Las redes WLAN actuales se encuentran expuestas a múltiples vectores de ataque que comprometen los principios fundamentales de confidencialidad, integridad y disponibilidad de la información. Entre las amenazas más prevalentes destacan suplantación de puntos de acceso (*Rogue AP y Evil Twin*), la captura de *handshakes* WPA/WPA2, los ataques de desautenticación (*deauthentication*), el *sniffing* de tráfico y las técnicas de ingeniería social orientadas al robo de credenciales documentadas por Ortega et al. [6].

Dentro de estas técnicas, el ataque *Evil Twin* consiste en el despliegue de un punto de acceso fraudulento que imita la identidad de una red legítima, engañando a los usuarios para interceptar información sensible; esta técnica sigue siendo altamente efectiva debido a la confianza automática que los sistemas operativos mantienen hacia redes previamente conocidas [9]. Por otro lado, los ataques de desautenticación permiten desconectar forzosamente a los dispositivos clientes mediante la inyección de tramas de control manipuladas. Este procedimiento se utiliza estratégicamente para forzar procesos de reconexión y, de este modo, capturar los *handshakes* de autenticación WPA/WPA2, vulnerabilidad explotada en ataques como KRACK [11].

Con la llegada de los estándares WiFi 6E y la habilitación de la banda de 6 GHz, surgieron nuevos desafíos asociados a la gestión del espectro y la supervisión de redes tri-banda. Aunque estos estándares introducen mejoras de seguridad, investigaciones recientes evidencian la persistencia de vulnerabilidades relacionadas con *spoofing, relay attacks* y mecanismos avanzados de suplantación durante las fases iniciales de establecimiento de conexión [11].

Adicionalmente, la proliferación de dispositivos IoT incrementa el riesgo de ataques distribuidos, dado que muchos dispositivos inteligentes presentan limitaciones de procesamiento y mecanismos de seguridad débiles, convirtiéndolos en objetivos potenciales para *botnets* y ataques DDoS [12]. Frente a este panorama, las estrategias modernas de

seguridad inalámbrica requieren la implementación de sistemas de monitoreo continuo, detección proactiva de anomalías y automatización del registro forense de eventos sospechosos, en lugar de depender exclusivamente de respuestas reactivas o manuales [8].

2.1.3 Fundamentos del pentesting inalámbrico: técnicas, herramientas y ética

El *pentesting* inalámbrico es una práctica especializada de ciberseguridad orientada a identificar y evaluar vulnerabilidades en redes WLAN mediante pruebas controladas de penetración. Su finalidad es analizar el comportamiento de una infraestructura inalámbrica frente a posibles ataques reales, detectando debilidades antes de su explotación maliciosa [12]. Estas auditorías comprenden etapas técnicas como reconocimiento de redes, captura de tráfico, análisis de autenticación y validación de vulnerabilidades.

Entre las técnicas más utilizadas destacan: ataques de desautenticación, la captura de *handshakes* WPA/WPA2, el despliegue de puntos de acceso fraudulentos (*Evil Twin y Rogue AP*) y análisis pasivo de tráfico (*sniffing*) [4]. El crecimiento de redes WiFi 6E (802.11ax) y WiFi 7 (802.11be) ha incrementado la necesidad de herramientas capaces de monitorear simultáneamente en las tres bandas, fortaleciendo los procesos de auditoría y detección proactiva de anomalías en arquitecturas tri-banda [2]. La Figura 1 presenta el flujo general de un proceso de *pentesting* inalámbrico aplicado a redes modernas.

Figura 1

Flujo general del proceso de pentesting inalámbrico en redes WiFi modernas

Nota. Metodologías de auditoría inalámbrica y pruebas de penetración Wi-Fi**,** elaboración propia.

Entre las herramientas más utilizadas destacan Aircrack-ng, Kismet, Bettercap y la plataforma WiFi Pineapple desarrollada por Hak5, la cual integra funcionalidades avanzadas de automatización, monitoreo e inyección de tráfico mediante el motor PineAP y *payloads* en DuckyScript™, en cumplimiento con estándares de seguridad WLAN como NIST SP 800-153 [16] y técnicas de detección de intrusiones [8], [13]. El uso de estas herramientas debe regirse por principios éticos y legales estrictos, ejecutando pruebas únicamente en entornos

autorizados y controlados. El objetivo del *pentesting* ético no es comprometer infraestructuras ajenas, sino fortalecer la seguridad institucional mediante la identificación responsable de vulnerabilidades y la implementación de mecanismos preventivos alineados con las buenas prácticas de ciberseguridad.

2.1.4 Automatización en seguridad: scripting (Bash, Python) y lenguajes especializados (DuckyScript™)

La automatización es un pilar fundamental de la ciberseguridad moderna, permitiendo responder de manera rápida y eficiente ante eventos de seguridad complejos y dinámicos. En la auditoría inalámbrica, la automatización ejecuta procesos de reconocimiento, monitoreo, captura de tráfico y generación de alertas sin depender exclusivamente de la intervención manual, optimizando tiempos de respuesta y la detección de anomalías [14].

Los lenguajes de *scripting* son esenciales para tareas repetitivas y el despliegue de herramientas de auditoría. Bash es ampliamente utilizado en sistemas Linux para la administración de procesos, automatización de comandos y manipulación de servicios de red. Por su parte, Python se ha consolidado en ciberseguridad por su flexibilidad, integración con librerías de análisis de tráfico y capacidad para crear herramientas orientadas a la detección de intrusiones [15].

En plataformas especializadas como el WiFi Pineapple, la automatización se fortalece con DuckyScript™, un lenguaje diseñado para la ejecución de *payloads* y secuencias de acciones en pruebas de penetración. Este mecanismo permite implementar rutinas que reaccionan automáticamente ante eventos específicos en la red inalámbrica, facilitando procesos de monitoreo, alerta y respuesta proactiva. La integración de *scripts* Bash y *payloads* de la biblioteca oficial en DuckyScript™ transforma los dispositivos portátiles de auditoría en plataformas autónomas de análisis y registro forense en entornos WiFi.

2.1.5 Revisión de plataformas de auditoría: WiFi Pineapple y alternativas

Las plataformas de auditoría inalámbrica han evolucionado significativamente ante el incremento de amenazas sobre redes WLAN modernas y la demanda de herramientas portátiles para reconocimiento, monitoreo y análisis de vulnerabilidades. En este ecosistema destacan Aircrack-ng, Kismet, Bettercap y la familia WiFi Pineapple [5], consolidada como una de las plataformas más reconocidas en auditoría inalámbrica profesional. La Tabla 1 presenta una comparativa de las principales características técnicas de las plataformas de auditoría inalámbrica analizadas, evidenciando las ventajas diferenciales del WiFi Pineapple Pager en términos de portabilidad, autonomía y capacidades tri-banda.

Tabla 1

Comparativa de plataformas de auditoría inalámbrica.

Características	Aircrack-ng	Kismet	Bettercap	Mark VII+AC	Tetra	PAGER
Tipos	Software	Software	Software	Hardware ($250 USD)	Hardware ($160 USD)	Hardware ($320 USD)
Modo de operación	Activo (incluyen paquetes)	Pasivo (Solo escucha)	Activo (Modifica tráfico)	Activo (Suplanta redes)	Activo (Potente pero antiguo)	Activo (Suplantación táctica)
Bandas soportadas	2.4 GHz y 5 GHz	2.4, 5 y 6 GHz	2.4 GHz y 5 GHz	2.4 GHz y 5 GHz	2.4 GHz	2.4, 5 y 6 GHz
Función principal	Captura de handshakes y descifrado por fuerza bruta	Escaneo masivo, mapeo GPS (War driving), detección de intrusos	Ataques MitM inalámbricos y cableados	Crear redes falsas automatizadas (Evil AP), engañar clientes	Mismo propósito que Mark VII+AC, pero en la banda 2.4 GHz	Crear redes falsas automatizadas, engañar clientes, MitM portátil
Automatización	Manual (Scripts externos)	Parcial	Scripts propios (JavaScript)	DuckyScript	DuckyScript	DuckyScript™ y Bash nativo
Alertas Hápticas/Acústicas	X	X	X	X	X	Nativo en dispositivo
Portabilidad	Requiere Laptop	Requiere Laptop	Requiere Laptop	Portátil	Estacionario	Autónomo (Untethered)
Interfaz sin laptop	X	X	X	Básica	X	Pantalla integrada
Batería	X	X	X	Limitada	X	4 horas
Nivel de dificultad	Medio/Avanzado (Línea de comandos)	Medio (Requiere configuración de antenas)	Avanzado (Consola y scripts)	Bajo/Medio (Interfaz visual)	Medio (Hardware descontinuado)	Bajo/Medio (Interfaz retro + web)
Vulnerabilidad que detectan	Contraseñas Wi-Fi débiles y cifrados obsoletos (WEP/WPA)	Redes abiertas, configuraciones inseguras, presencia de atacantes	Tráfico sin cifrar, aplicaciones inseguras, suplantación de identidad	Comportamiento inseguro de dispositivos que buscan Wi-Fi automáticamente	Mismo que Mark VII, enfocado en bandas antiguas	Comportamiento inseguro de dispositivos, Evil Twin, handshakes WPA/WPA2

Nota. Elaboración propia a partir de documentación técnica de Aircrack-ng, Kismet, Bettercap, Hak5.

Entre las versiones más representativas de la familia WiFi Pineapple se encuentran los modelos Tetra, Mark VII y Pager, cada uno orientado a diferentes escenarios operacionales:

- **WiFi Pineapple Tetra:** Incorporó múltiples radios de alta potencia y capacidades avanzadas de monitoreo simultáneo, permitiendo auditorías de amplio alcance sobre redes tradicionales. Sin embargo, sus dimensiones físicas,

consumo energético y dependencia de alimentación externa limitaron su movilidad operativa [4].

- **WiFi Pineapple Mark VII:** Introdujo mejoras en portabilidad, automatización y facilidad de administración mediante interfaces más intuitivas y soporte para payloads automatizados [5].
- **WiFi Pineapple Pager:** Representa una evolución orientada a auditoría móvil autónoma, integrando pantalla táctil, batería interna, soporte tri-banda (2.4 GHz, 5 GHz y 6 GHz) y mecanismos de automatización mediante DuckyScript™ y Bash. Estas características permiten ejecutar procesos de detección y respuesta inalámbrica directamente desde el dispositivo, sin depender de estaciones externas de procesamiento.

La Figura 2 presenta la evolución de las principales plataformas WiFi Pineapple utilizadas en auditoría inalámbrica y *pentesting* profesional.

Figura 2

Evolución de las plataformas WiFi Pineapple para auditoría inalámbrica

Nota. Evoluciones técnicas de Hak5 y plataformas de auditoría inalámbrica modernas. Fuente: Hak5 (2025).

2.1.6 El WiFi Pineapple Pager: especificaciones técnicas, arquitectura y modelo de amenaza

El WiFi Pineapple Pager es una plataforma moderna de auditoría inalámbrica diseñada para ejecutar procesos avanzados de monitoreo, reconocimiento y automatización sobre redes WiFi de nueva generación. Desarrollado por Hak5, el dispositivo integra capacidades de

operación tri-banda (2.4 GHz, 5 GHz y 6 GHz), permitiendo auditorías sobre arquitecturas WiFi 6E/7 y entornos inalámbricos de alta densidad. Su diseño portátil incorpora pantalla de alta resolución, batería recargable y automatización mediante la biblioteca oficial de payloads en DuckyScript™ y Bash, facilitando la ejecución autónoma de tareas de *pentesting* y análisis espectral [5].

Arquitectura

El Pager se fundamenta en un sistema embebido basado en Linux que incorpora el motor PineAP, responsable de gestionar funciones de monitoreo, captura de tráfico, detección de clientes y automatización de eventos dentro del entorno WLAN. Esta arquitectura permite reconocimiento pasivo y activo, incluyendo análisis de SSID, BSSID, intensidad de señal (RSSI), detección de dispositivos y gestión controlada de tramas inalámbricas. Además, el acceso root vía SSH facilita la integración de scripts y módulos orientados a la implementación de soluciones avanzadas de auditoría y registro forense [5]. La Figura 3 muestra la arquitectura general y los principales componentes funcionales del WiFi Pineapple Pager.

Figura 3

Arquitectura funcional del WiFi Pineapple Pager

Nota. Arquitectura y documentación técnica oficial de Hak5. ***Fuente****: Hak5 LLC (2025).*

Desde la perspectiva de la ciberseguridad, el modelo de amenazas asociado al WiFi Pineapple Pager contempla escenarios relacionados con:

- Ataques *Evil Twin* (suplantación de APs legítimo).
- Despliegue de *Rogue Access Points*.
- Captura de *handshakes* WPA/WPA2.
- Desautenticación de clientes.
- Monitoreo pasivo de tráfico inalámbrico.

Estas capacidades convierten al dispositivo en una herramienta versátil para auditoría defensiva y simulaciones controladas de vectores de ataque, orientadas a evaluar la robustez y generar evidencias forenses de infraestructuras inalámbricas modernas [7].

2.1.7 Marco legal y ético para pruebas de penetración autorizadas

Las pruebas de penetración inalámbrica evalúan la seguridad de infraestructuras de red mediante la simulación controlada de ataques. Debido a la naturaleza ofensiva de muchas herramientas y metodologías, es indispensable establecer límites legales y éticos que regulen su aplicación en entornos académicos, corporativos e institucionales. La ejecución no autorizada de auditorías inalámbricas puede violar la privacidad, interrumpir servicios y constituir un acceso indebido a sistemas de información, tipificado como delito en legislaciones como el Código Orgánico Integral Penal (COIP) del Ecuador, y contraviene además la Ley Orgánica de Protección de Datos Personales [8].

En el ámbito de la ciberseguridad ética, las auditorías deben ejecutarse únicamente bajo consentimiento explícito, en entornos controlados y predeterminados, y con autorización expresa. Este procedimiento garantiza que la evidencia refuerce las medidas de seguridad sin comprometer la accesibilidad, la exactitud ni la privacidad de los datos institucionales. Las buenas prácticas de pentesting recomiendan una documentación adecuada de los procedimientos, la limitación del alcance tecnológico y evitar afectar a dispositivos o personas ajenas a la revisión [12].

Todas las pruebas de auditoría inalámbrica para el proyecto actual se realizaron en un laboratorio bajo la gestión y autorización de la UPSE, utilizando dispositivos cliente y puntos de acceso configurados específicamente para escenarios de simulación. El WiFi Pineapple Pager y las cargas útiles automatizadas en DuckyScript™ y Bash se utilizaron únicamente con fines académicos y de investigación, cumpliendo estrictamente con los Términos de uso y la ética de *hacking* responsable de Hak5.

2.2 Marco conceptual

2.2.1 Redes inalámbricas WLAN

Las redes inalámbricas WLAN (*Wireless Local Area Network*) son infraestructuras de comunicación que transmiten datos mediante ondas de radiofrecuencia sin requerir conexiones físicas cableadas. Operan bajo la familia de estándares IEEE 802.11 [2] y son ampliamente

utilizadas en entornos domésticos, empresariales, educativos e industriales por su flexibilidad y facilidad de despliegue.

Las WLAN modernas permiten la interconexión simultánea de múltiples dispositivos (computadoras, teléfonos inteligentes, sensores *IoT*, sistemas embebidos) utilizando las bandas de 2.4 GHz, 5 GHz y actualmente 6 GHz. El cambio hacia arquitecturas de triple banda y estándares como WiFi 6E ha mejorado la capacidad de transmisión y la eficiencia espectral, pero también ha aumentado la complejidad de la gestión y los riesgos de seguridad.

Dentro de una red WLAN, los puntos de acceso (Access Points) actúan como nodos centrales que gestionan la comunicación entre dispositivos clientes y la infraestructura de red. La seguridad inalámbrica es crucial en las situaciones de conectividad actuales, ya que la transmisión inalámbrica se realiza a través de un medio compartido y físicamente accesible, lo que deja a las redes WLAN vulnerables a la interceptación de comunicaciones, la suplantación de identidad y los ataques de manipulación del tráfico.

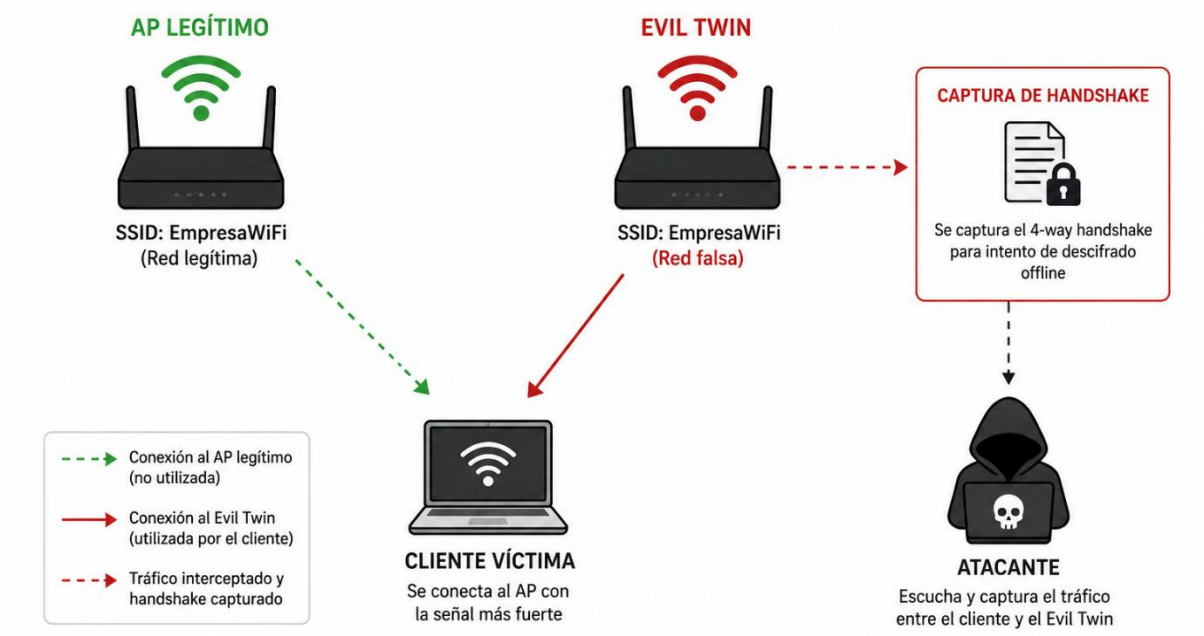
2.2.2 Conceptos relacionados con auditoría y pentesting WiFi

Dentro de la auditoría inalámbrica existen conceptos técnicos fundamentales para comprender los procesos de monitoreo, análisis y evaluación de vulnerabilidades en redes WLAN. El SSID (*Service Set Identifier*) corresponde al nombre lógico que identifica una red inalámbrica, mientras que el BSSID (Basic Service Set Identifier) representa la dirección MAC física de la interfaz del punto de acceso que transmite dicha red.

Otro concepto central es el *handshake* WPA/WPA2, mecanismo de autenticación utilizado durante la asociación entre un dispositivo cliente y un punto de acceso. Su captura constituye una de las técnicas más utilizadas en auditorías inalámbricas para analizar la robustez de la clave precompartida (PSK) y los mecanismos de cifrado implementados en una red específica [4]. La Figura 4 ilustra un ejemplo conceptual de este proceso junto con la suplantación de puntos de acceso.

Figura 4

Escenario conceptual de auditoría inalámbrica mediante Evil Twin y captura de handshake



Nota. Técnicas de pentesting inalámbrico y análisis WLAN, elaboración propia.

Respecto a las amenazas evaluadas, un *Rogue Access Point* se define como un punto de acceso no autorizado desplegado dentro de una red. Una variante más sofisticada es el Evil Twin, un punto de acceso fraudulento que suplanta la identidad de una red legítima para interceptar información sensible. Estas técnicas son ampliamente utilizadas en pruebas de penetración controladas para evaluar el comportamiento de los usuarios y la capacidad de detección de amenazas en infraestructuras inalámbricas modernas.

Finalmente, en el contexto de la automatización, un *payload* se entiende como un script o secuencia de acciones (generalmente en Bash o DuckyScript™) ejecutado por herramientas de auditoría para responder ante eventos específicos detectados en el entorno de red. En el marco de esta investigación, se hace uso de *payloads* provenientes de la biblioteca oficial de Hak5, los cuales permiten automatizar tareas de reconocimiento, alerta y registro forense sin requerir el desarrollo de código personalizado desde cero.

2.2.3 Automatización y payloads en auditoría inalámbrica

La automatización en auditoría inalámbrica permite ejecutar tareas de monitoreo, análisis y respuesta ante eventos de seguridad de manera continua y eficiente, reduciendo la dependencia de intervención manual en procesos de *pentesting*. En entornos modernos de

ciberseguridad, la automatización es fundamental debido al incremento de amenazas dinámicas y la necesidad de reaccionar rápidamente ante anomalías en el espectro radioeléctrico [9].

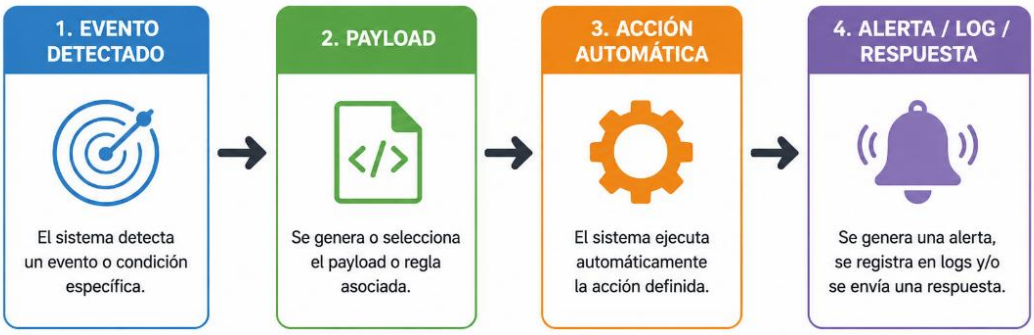
Los *payloads* son secuencias automatizadas de instrucciones diseñadas para ejecutar acciones específicas ante determinados eventos de red. Estas acciones pueden incluir:

- Reconocimiento de dispositivos.
- Captura de tráfico.
- Generación de alertas.
- Registro de eventos forenses.

En plataformas como el WiFi Pineapple Pager, estos mecanismos se implementan mediante la instalación y configuración de la biblioteca oficial de cargas útiles de Hak5, ejecutados mediante scripts en Bash y comandos DuckyScript™. Esto permite establecer flujos de trabajo autónomos de monitoreo y respuesta en redes modernas sin necesidad de desarrollar código personalizado desde cero [5]. La Figura 5 presenta el flujo básico de automatización basado en eventos y *payloads* dentro de un sistema de auditoría inalámbrica.

Figura 5

Flujo de automatización mediante payloads en auditoría inalámbrica



Nota. *F*lujo de automatización basado en eventos y respuestas del sistema, elaboración propia.

La integración de esta automatización transforma dispositivos portátiles de auditoría en plataformas proactivas capaces de identificar amenazas en tiempo real y ejecutar acciones inmediatas frente a comportamientos sospechosos. Este enfoque fortalece los procesos de seguridad inalámbrica, especialmente en arquitecturas tri-banda, donde el monitoreo simultáneo de múltiples frecuencias incrementa la complejidad operativa de las auditorías tradicionales.

2.3 Estado del arte

2.3.1 Investigaciones relacionadas con seguridad y auditoría WiFi

Durante los últimos años, la investigación en ciberseguridad inalámbrica ha crecido significativamente debido al incremento de amenazas dirigidas a redes WLAN modernas y entornos IoT. Para mejorar la seguridad de las infraestructuras inalámbricas de próxima generación, la investigación se ha centrado en el análisis de vulnerabilidades, la detección de intrusiones y la creación de sistemas automatizados. En el ámbito de la detección de amenazas, se desarrolló un sistema de detección de intrusiones basado en anomalías para redes IEEE 802.11 [7], lo que subraya la importancia de la observación continua y la detección temprana de actividades sospechosas en los datos inalámbricos. De manera similar, los autores de [9] propusieron un modelo de detección de anomalías basado en aprendizaje profundo para redes *IoT* inalámbricas de alta densidad, evidenciando que la automatización y el análisis inteligente mejoran la capacidad de respuesta frente a amenazas emergentes.

En el contexto de WiFi 6 y WiFi 6E, los autores de [11] analizaron vulnerabilidades relacionadas con *spoofing* y *relay attacks* durante el establecimiento de conexiones, concluyendo que las nuevas generaciones de redes inalámbricas requieren herramientas especializadas capaces de monitorear simultáneamente múltiples bandas de frecuencia y detectar amenazas avanzadas en tiempo real. En el contexto latinoamericano, los estudios de [4], [11] y [19] abordaron procesos de auditoría inalámbrica y análisis de vulnerabilidades mediante herramientas de *pentesting* orientadas a redes Wi-Fi. Estas investigaciones destacan la importancia de implementar metodologías prácticas y sistemas automatizados de evaluación que permitan fortalecer la seguridad institucional frente a ataques inalámbricos modernos, sentando las bases para la comparación técnica y la selección de la plataforma de auditoría que se presenta en la matriz de estado del arte de este trabajo.

2.3.2 Tecnologías modernas para la detección y análisis de amenazas inalámbricas

Ante la expansión de redes de alta densidad e *IoT*, los sistemas de monitoreo perimetral tradicionales han sido superados. Las arquitecturas actuales priorizan la automatización, el análisis de tráfico y la generación de inteligencia ante amenazas dinámicas [3]. Las tecnologías clave incluyen:

- **Sistemas WIDS (*Wireless Intrusion Detection Systems*):** monitorean el espectro radioeléctrico de forma continua para detectar *spoofing, Rogue Access Points* y ataques de desautenticación. El análisis de anomalías ha mejorado significativamente la precisión en la identificación de incidentes complejos [7].

- **IA y aprendizaje automático:** el aprendizaje profundo optimiza el reconocimiento de patrones maliciosos, estudios recientes demuestran que estas técnicas elevan la capacidad de predicción y reducen el tiempo de respuesta ante ataques automatizados en redes [9].
- **Plataformas de auditoría inteligente:** las soluciones actuales han progresado hacia la autonomía operativa, incorporando motores de análisis y mecanismos de alerta y registro forense en tiempo real para mejorar la seguridad proactiva en entornos de nueva generación [5].

2.3.3 Importancia de la automatización en auditorías WiFi modernas

La automatización se ha convertido en un componente esencial en las auditorías inalámbricas modernas debido al crecimiento de amenazas dinámicas y al incremento de dispositivos conectados en redes WLAN. Los métodos tradicionales de análisis manual presentan limitaciones en escenarios que requieren monitoreo continuo y respuesta inmediata ante eventos sospechosos en el espectro radioeléctrico [9].

Actualmente, las plataformas de auditoría integran mecanismos automatizados para ejecutar tareas de reconocimiento, captura de tráfico, generación de alertas y análisis de vulnerabilidades en tiempo real. Este enfoque optimiza los tiempos de respuesta y mejora la eficiencia operativa en procesos de *pentesting* y monitoreo de redes inalámbricas modernas. La integración de *payloads* provenientes de bibliotecas oficiales y scripts automatizados mediante Bash y DuckyScript™ fortalece la capacidad de reacción frente a amenazas como *Evil Twin*, *Rogue AP* y ataques de desautenticación, permitiendo implementar sistemas proactivos de seguridad inalámbrica adaptados a arquitecturas tri-banda y entornos de alta densidad de dispositivos [5].

2.4 Fundamentos tecnológicos

2.4.1 Arquitectura del WiFi Pineapple Pager

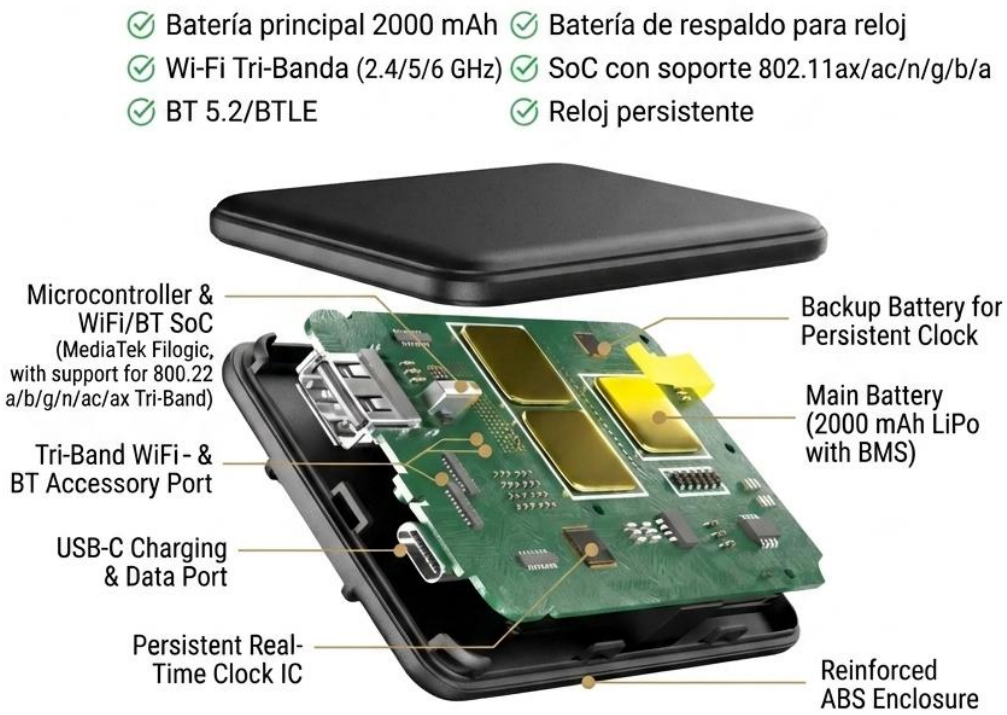
Las especificaciones técnicas generales y el modelo de amenazas del WiFi Pineapple Pager fueron descritos en la sección 2.1.6. En esta sección se profundiza exclusivamente en la arquitectura interna del dispositivo y la interacción entre sus componentes funcionales.

El sistema se fundamenta en un SoC (*System on chip*) con sistema operativo Linux embebido (OpenWRT), que orquesta tres subsistemas principales: el modelo de radios tri-banda, el motor PineAP (descrito en detalle en la sección 2.4.2) y el sistema de alerta

háptico/acústico. La Figura 6 muestra la estructura interna y las interconexiones de estos elementos [5].

Figura 6

Arquitectura interna con características principales



Nota: La figura muestra la estructura interna y los elementos funcionales del dispositivo. Fuente: Hak5 (2025).

El WiFi Pineapple Pager posibilita auditorías inalámbricas autónomas, sin depender de estaciones de procesamiento externas, gracias a su diseño portátil, batería integrada y pantalla táctil. Esto simplifica los escenarios de pruebas de penetración móviles y el análisis proactivo del espectro radioeléctrico.

2.4.2 Motor PineAP y funcionalidades de auditoría

PineAP constituye el núcleo operativo del WiFi Pineapple Pager y fue introducido brevemente en la sección 2.1.6. En esta sección se detallan sus funcionalidades específicas de auditoría, orientadas a la auditoría inalámbrica y automatización de eventos dentro del entorno *WLAN*. Este motor permite ejecutar procesos de reconocimiento pasivo y activo mediante el monitoreo continuo del espectro radioeléctrico, identificando puntos de acceso, dispositivos clientes, intensidad de señal (RSSI) y comportamiento del tráfico inalámbrico [5].

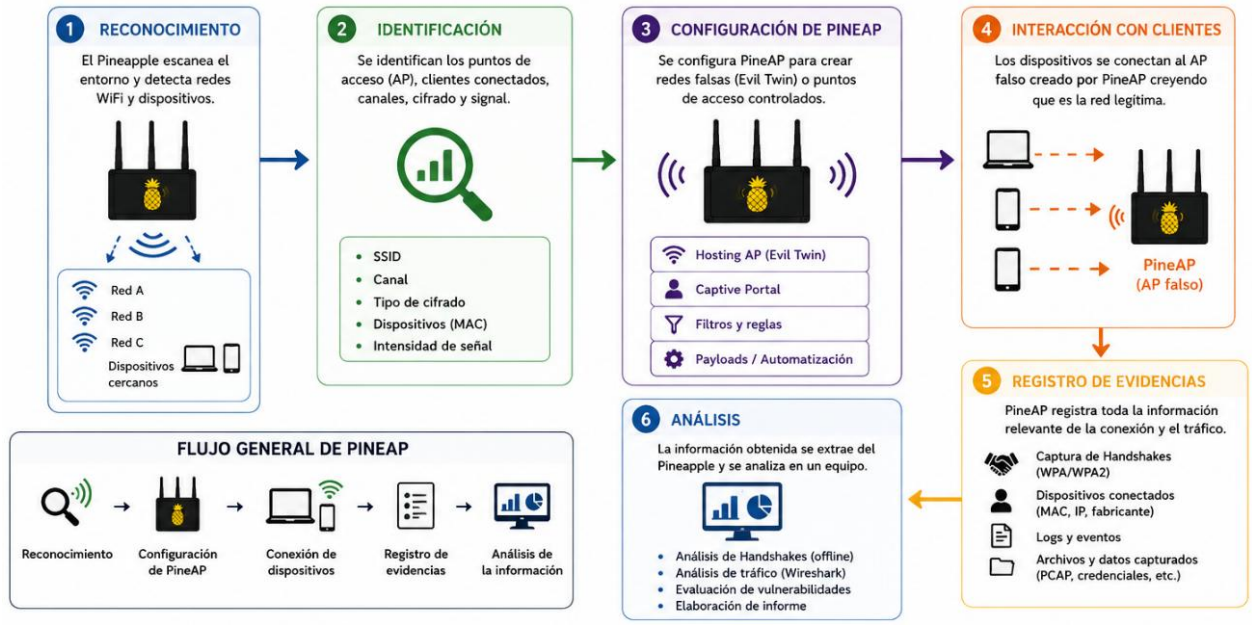
Entre sus principales funcionalidades destacan:

- Detección de redes ocultas.
- Captura de *handshakes* WPA/WPA2.
- Despliegue de *Rogue Access Points.*
- Monitoreo de asociaciones de clientes inalámbricos.
- Integración de la biblioteca oficial de *payloads* para detección y registro forense ante eventos específicos.

La Figura 7 muestra el funcionamiento general del motor PineAP dentro de un entorno de auditoría inalámbrica automatizada.

Figura 7

Funcionamiento del motor PineAP en procesos de auditoría inalámbrica



Nota. Arquitectura funcional de PineAP y plataformas de auditoría WiFi, elaboración propia.

2.4.3 Payloads y scripts para automatización de eventos

Los *payloads* son componentes clave en los sistemas modernos de auditoría inalámbrica automatizada. Permiten ejecutar secuencias de acciones programadas en respuesta a eventos detectados en el entorno *WLAN*, facilitando procesos de monitoreo, captura de tráfico y generación automática de alertas de seguridad [17].

En el WiFi Pineapple Pager, se implementan las cargas útiles haciendo uso de la biblioteca oficial de Hak5 y lenguajes de *script* como DuckyScript™ y Bash. Esto posibilita la automatización de tareas como las siguientes:

- Reconocimiento de SSID.
- Identificación de dispositivos inalámbricos capturados.
- Capturas de *handshakes* WPA/WPA2.
- Registro de ejecuciones.

La integración de estos *scripts* con el motor PineAP mejora la capacidad de respuesta del sistema a las amenazas cambiantes en arquitecturas WiFi de tres bandas [5]. La Figura 8 presenta el flujo automatizado de ejecución de *payloads* y procesamiento de eventos dentro del sistema de auditoría inalámbrica basado en PineAP.

Figura 8

Flujo automatizado de auditoría inalámbrica mediante PineAP y payloads

Nota. Arquitectura de automatización implementada para el sistema de auditoría inalámbrica basada en el WiFi Pineapple Pager.

La automatización basada en eventos optimiza los tiempos de reacción durante auditorías inalámbricas, reduciendo la intervención manual y facilitando la ejecución continua de procesos de análisis y vigilancia sobre el espectro radioeléctrico. Este enfoque convierte al sistema en una plataforma flexible y escalable para pruebas de penetración y monitoreo proactivo de redes.

2.4.4 Operación tribanda en redes WiFi modernas

La operación tri-banda es una de las principales características de las redes inalámbricas modernas, permitiendo el funcionamiento simultáneo en las frecuencias de 2.4 GHz, 5 GHz y

6 GHz. Esta arquitectura incrementa la capacidad de transmisión, reduce la congestión del espectro y mejora el rendimiento en entornos con alta densidad de dispositivos [2]. La banda de 2.4 GHz ofrece mayor cobertura y penetración de señal, pero debido a la gran cantidad de dispositivos que utilizan esta frecuencia (como Bluetooth, microondas e Internet de las Cosas), se produce mayor interferencia. Si bien la banda de 6 GHz (WiFi 6E) permite utilizar canales más amplios y mejorar la eficiencia espectral en las redes WLAN actuales, la banda de 5 GHz ofrece altas velocidades de transmisión y una cobertura intermedia [6]. La Tabla 2 presenta una comparación general entre las principales bandas de frecuencia.

Tabla 2

Comparación de bandas de frecuencia en arquitecturas Wi-Fi tri-banda

Característica	2.4 GHz	5 GHz	6 GHz (WiFi 6E)
Cobertura	Mayor cobertura y penetración en obstáculos	Cobertura media con penetración moderada.	Menor cobertura y penetración en paredes.
Velocidad	Hasta 600 Mbps aproximadamente.	Hasta varios Gbps.	Hasta varios Gbps.
Interferencia	Alta interferencia debido a Bluetooth, microondas y dispositivos IoT.	Interferencia media, menor que 2.4 GHz.	Baja interferencia y espectro más limpio.
Uso en WiFi 6E	No soportado en WiFi 6E.	Compatible con WiFi 5 y WiFi 6.	Banda exclusiva para dispositivos WiFi 6E.
Uso recomendado	Navegación básica, domótica y dispositivos de bajo consumo.	Streaming HD/4K, videojuegos y transferencia de archivos.	Streaming 8K, realidad virtual y entornos de alta densidad.

Nota. Elaboración propia a partir de especificaciones técnicas de WiFi 6E y arquitecturas IEEE 802.11ax/be.

La coexistencia de múltiples bandas de frecuencia incrementa la complejidad de administración y seguridad inalámbrica, debido a la necesidad de monitorear simultáneamente distintos canales y detectar amenazas distribuidas en el entorno radioeléctrico. En este contexto, plataformas de auditoría como el WiFi Pineapple Pager permiten ejecutar procesos de análisis tri-banda orientados a la detección proactiva de vulnerabilidades y eventos sospechosos [5].

2.4.5 Seguridad en redes WiFi 6E y nuevas amenazas

La evolución hacia redes WiFi 6E ha introducido mejoras significativas en velocidad, eficiencia espectral y reducción de latencia mediante el uso de la banda de 6 GHz. Sin embargo, esta transición también ha generado nuevos desafíos de seguridad, debido al incremento de dispositivos conectados y la ampliación de la superficie de ataque en arquitecturas *WLAN* modernas [11].

Entre las amenazas más relevantes en entornos multi-banda se encuentran:

- ***Spoofing*:** Suplantación de identidad de dispositivos o puntos de acceso.
- ***Evil Twin*:** Punto de acceso suplantado que imita una red original**.**
- **Captura de *handshakes*:** Intercepción de protocolos de autenticación WPA/WPA2 (principalmente en las dos bandas).

La presencia de diversas bandas de frecuencia dificulta el monitoreo y la detección de anomalías, a pesar de que el estándar WiFi 6E exige el uso de WPA3 y tramas de gestión protegidas (PMF) en el canal de 6 GHz, lo que limita eficazmente los ataques de desautenticación. Esto cobra especial importancia en el contexto de las normativas BYOD (*Trae tu propio dispositivo*) y los escenarios con alta densidad de dispositivos *IoT*, donde el monitoreo pasivo se convierte en la principal línea de defensa [3].

Las plataformas modernas de auditoría inalámbrica proporcionan herramientas automáticas para la detección y el análisis proactivos en respuesta a esta situación. Herramientas como WiFi Pineapple Pager permiten el monitoreo continuo de las bandas de 2.4 GHz, 5 GHz y 6 GHz, facilitando la detección temprana de actividades sospechosas y vulnerabilidades graves en la infraestructura.

2.4.6 Adopción de la banda de 6 GHz en Ecuador y capacidades del WiFi Pineapple Pager

La banda de 6 GHz (5925-7125 MHz), habilitada por los estándares WiFi 6E (802.11ax) y WiFi 7 (802.11be), representa un avance significativo en capacidad, menor interferencia y mayor ancho de canal. Sin embargo, su adopción en Ecuador es aún limitada. De acuerdo con el Plan Nacional de Frecuencias de la ARCOTEL [20], la banda de 6 GHz ha sido contemplada para uso en sistemas WAS/WLAN (Wireless Access Systems / Wireless Local Area Networks). Sin embargo, a la fecha de este estudio, su implementación a nivel nacional aún está en sus inicios y se limita principalmente a situaciones controladas o experimentos en grandes

ciudades. La infraestructura Wi-Fi disponible en Santa Elena utiliza exclusivamente la banda de 5 GHz; no hay indicios de que el espectro de 6 GHz se haya implementado comercialmente.

El WiFi Pineapple Pager utilizado en este estudio exhibe sofisticadas capacidades de escaneo del espectro 6 GHz. Debido a que puede operar en las tres bandas con soporte nativo para los estándares 802.11ax/be, el dispositivo está plenamente capacitado para realizar reconocimiento y auditoría en este espectro [5].

Durante el desarrollo del proyecto se constató que el hardware y la interfaz del dispositivo disponen de capacidad para el escaneo de la banda de 6 GHz. Aunque en el entorno local de Santa Elena no se detectaron redes activas en este espectro (limitando esta fase a una validación de concepto del hardware), esta característica posiciona al Pineapple Pager como una herramienta preparada para entornos de adopción futura de WiFi 6E/7 en Ecuador. Esto resulta especialmente relevante para auditorías de seguridad, permitiendo al auditor anticiparse a las nuevas amenazas que surgirán conforme se implemente esta banda en el país.

2.4.7 Integración del modo Recon, motor PineAP y sistema de alertas

Esta sección describe la integración funcional entre los tres componentes del sistema, cuyas características individuales fueron detalladas en las secciones 2.4.2 (*PineAP*) y 3.3.4 (*Recon*). El flujo de integración opera de la siguiente manera:

1. **Adquisición:** el modo Recon ejecuta el barrido espectral mediante *channel hopping* en las bandas 2.4 GHz y 5 GHz capturando tramas de gestión (*Beacon, Probe Request/Response*).
2. **Procesamiento:** el motor PineAP recibe los datos crudos de Recon, correlaciona SSID/BSSID, estructura el *SSID pool* y ejecuta los *payloads* configurados ante eventos específicos.
3. **Notificación:** el sistema de alertas genera respuestas hápticas, acústicas o visuales cuando PineAP detecta eventos críticos (captura de *handshake*, asociación a *open AP*, ráfaga de *deauth*).

Esta arquitectura de tres capas permite que el dispositivo opere como un nodo autónomo de auditoría sin intervención manual constante.

CAPÍTULO III

3.1 Desarrollo de la propuesta técnica

La presente investigación propone el diseño e implementación de un sistema de auditoría inalámbrica móvil y automatizado, orientado a la detección proactiva y al registro forense de vulnerabilidades en redes inalámbricas de doble banda, específicamente en las frecuencias de 2.4 GHz y 5 GHz. La propuesta se fundamenta en el uso del WiFi Pineapple Pager como plataforma central de hardware para la ejecución de procesos de reconocimiento, monitoreo y análisis del entorno radioeléctrico [5]. El WiFi Pineapple Pager dispone de capacidad técnica para operar en las bandas de 2.4 GHz, 5 GHz y 6 GHz; sin embargo, el alcance experimental de esta investigación se delimitó a las bandas de 2.4 GHz y 5 GHz, debido a que durante el periodo de estudio no se contó con infraestructura inalámbrica institucional operativa en la banda de 6 GHz. Por tanto, la capacidad de operación en 6 GHz se considera una característica tecnológica del dispositivo y una posibilidad de ampliación para futuras investigaciones, pero no forma parte de los resultados experimentales presentados en este trabajo.

El sistema está orientado a escenarios institucionales controlados y permite evaluar la capacidad de detección de puntos de acceso, dispositivos clientes y eventos asociados a la seguridad de las comunicaciones inalámbricas. Para optimizar la supervisión, se incorporan mecanismos de automatización y generación de alertas que facilitan la identificación temprana de anomalías en el espectro [9]. Técnicamente, la implementación integra el modo Recon y el motor PineAP para ejecutar procesos de reconocimiento y monitoreo sobre las bandas de 2.4 GHz y 5 GHz, correspondientes al alcance experimental de la investigación. Adicionalmente, se configuran e implementan los *payloads* de la biblioteca oficial de Hak5 para ejecutar tareas de reconocimiento, captura de tráfico y registro forense de eventos.

Con el propósito de validar el funcionamiento del sistema propuesto, se diseñó un entorno experimental que simula una infraestructura institucional en el laboratorio de la UPSE. Esto permitió la ejecución de pruebas controladas y el posterior análisis cuantitativo del desempeño del sistema frente a diferentes vectores de ataque inalámbrico [4].

3.1.1 Características generales del sistema

El sistema de auditoría implementa el WiFi Pineapple Pager como plataforma central (cuyas especificaciones se describen en la sección 2.1.6), integrando los módulos de

reconocimiento, procesamiento de eventos, sistema de alertas y *payloads* de automatización para ejecutar las tareas de auditoría inalámbrica.

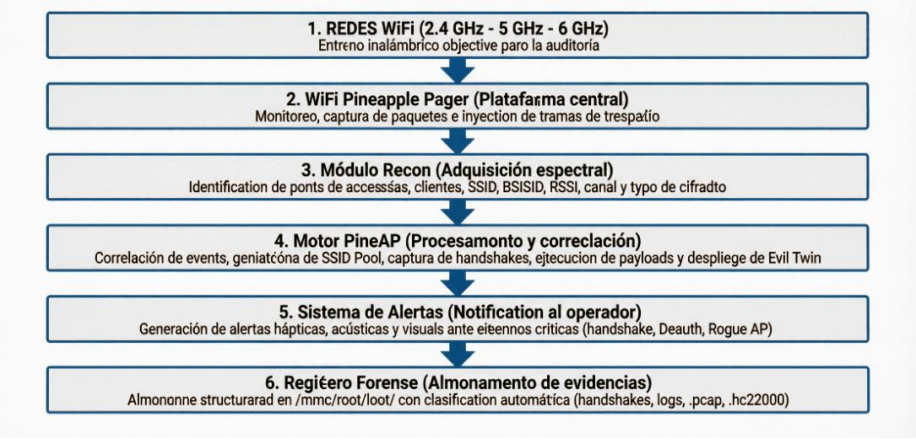
Las características operativas del sistema implementado son las siguientes:

- **Autonomía:** operación móvil (*untethered*) con batería integrada (4 horas), sin dependencia de estaciones externas, permitiendo auditoría itinerante dentro del campus.
- **Cobertura espectral:** monitoreo simultáneo en 2.4 y 5 GHz (activo), 6 GHz (pasivo).
- **Automatización:** ejecución programada de *payloads* de la biblioteca para reconocimiento, captura y registro forense.
- **Registro forense:** almacenamiento estructurado de evidencias en /mmc/root/loot/ con clasificación automática.

La solución fue desplegada y validada en el laboratorio de la UPSE bajo condiciones controladas. La Figura 9 muestra el flujo de trabajo general del sistema.

Figura 9

Proceso del sistema de auditoría inalámbrica



Nota. El diagrama presenta los pasos específicos para realizar la auditoría, elaboración propia.

3.1.2 Arquitectura general del sistema

La arquitectura del sistema implementado se fundamenta en la integración de los mecanismos de reconocimiento y procesamiento de eventos proporcionados por la plataforma WiFi Pineapple Pager. La estructura permite el monitoreo y análisis del entorno inalámbrico

mediante una secuencia organizada de adquisición, procesamiento y registro de información forense.

El proceso se inicia con la captura pasiva de información de las redes inalámbricas que operan en las bandas de 2.4 GHz, 5 GHz y 6 GHz. Posteriormente, el modo Recon identifica puntos de acceso y dispositivos cliente, recopilando datos como SSID, BSSID, RSSI y características de seguridad. Esta información es procesada en tiempo real por el motor PineAP, el cual administra los eventos detectados y ejecuta acciones según las condiciones preconfiguradas [5].

Complementariamente, se configuraron mecanismos de automatización mediante *payloads* de la biblioteca oficial de Hak5 y un sistema de alertas, facilitando el registro y la supervisión continua de los eventos durante las tareas de auditoría sin intervención manual constante. La arquitectura implementada proporciona una plataforma flexible para la evaluación de redes inalámbricas modernas, facilitando la detección de vulnerabilidades y el análisis del comportamiento de dispositivos en el entorno institucional de pruebas. La Figura 10 presenta la arquitectura general y el flujo de datos del sistema de auditoría inalámbrica.

Figura 10

Arquitectura general del sistema de auditoría inalámbrica

Nota. Diagrama de la arquitectura general y flujo de procesamiento de eventos del sistema de auditoría, elaboración propia.

3.1.3 Diagrama de flujo del sistema implementado

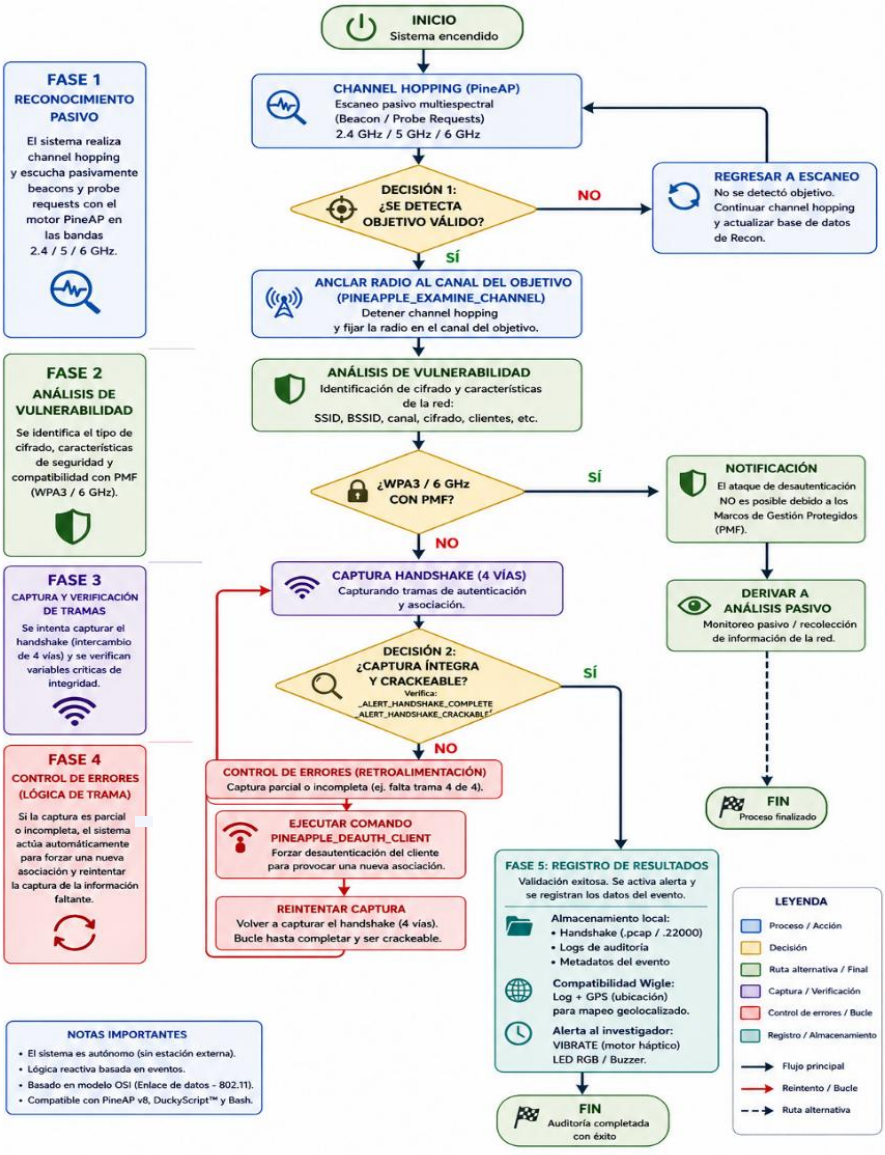
El funcionamiento del sistema de auditoría inalámbrica se representa mediante un diagrama de flujo que describe la secuencia de operaciones ejecutadas por el WiFi Pineapple Pager. Este diagrama resume gráficamente el comportamiento general del sistema, desde la

configuración inicial del dispositivo hasta la obtención de las evidencias para el análisis de resultados.

La Figura 11 muestra el flujo de trabajo implementado durante la auditoría inalámbrica. El proceso se inicia con la configuración del WiFi Pineapple Pager, donde se habilitan las bandas de frecuencia, se configura el módulo PineAP y se establecen los parámetros para el reconocimiento del entorno inalámbrico. Posteriormente, el sistema ejecuta el modo Recon, realizando el escaneo de las bandas de 2.4 GHz, 5 GHz y 6 GHz mediante el mecanismo de *channel hopping*, detectando puntos de acceso, dispositivos cliente y demás información relevante del entorno [5].

Figura 11

Diagrama de flujo del sistema de auditoría inalámbrica implementado



Nota. Diagrama de flujo de las operaciones ejecutadas por el dispositivo, elaboración propia.

Una vez identificado el punto de acceso de interés, el sistema permite visualizar información como SSID, BSSID, canal de operación, RSSI y mecanismo de seguridad. Con base en esta información, el operador determina la acción a ejecutar durante la auditoría, permitiendo realizar reconocimiento pasivo, monitoreo o captura controlada de *handshakes* [7]. Finalmente, la información obtenida durante las diferentes etapas del proceso es registrada y organizada como evidencia forense de la auditoría. Este flujo integra las funciones principales del WiFi Pineapple Pager empleadas en la presente investigación y constituye la base metodológica para los procedimientos experimentales descritos en las secciones posteriores.

3.2 Componentes del sistema

La implementación del sistema de auditoría inalámbrica se fundamenta en la integración de elementos de hardware y software que permiten ejecutar tareas de reconocimiento, monitoreo y análisis de redes WiFi en las bandas de 2.4 GHz, 5 GHz y 6 GHz. Estos componentes proporcionan los recursos necesarios para la detección de puntos de acceso, identificación de dispositivos cliente, procesamiento de eventos y generación de alertas durante el proceso de auditoría [5]. La Figura 12 presenta el diagrama de componentes del sistema de auditoría inalámbrica, clasificados en hardware y software, los cuales se detallan en las secciones siguientes.

Figura 12

Diagrama de componentes del sistema de auditoría inalámbrica

Nota. Clasificación de los elementos de hardware y software que conforman la plataforma de auditoría, elaboración propia.

Para garantizar el rigor experimental, los componentes se clasifican en tres categorías:

- **Hardware principal:** WiFi Pineapple Pager, plataforma central que integra los radios tri-banda y el motor de procesamiento PineAP para el análisis del entorno inalámbrico.
- **Hardware complementario:** Dispositivos cliente de prueba (*smartphones* y *laptops* con adaptadores Wi-Fi estándar) utilizados para simular el comportamiento de usuarios legítimos y generar tráfico de red controlado dentro del laboratorio de la UPSE.
- **Software y herramientas:** Firmware oficial del dispositivo, cliente SSH para la configuración avanzada (acceso *root*), navegador web para gestionar interfaces gráficas y la biblioteca oficial de Hak5 para automatizar tareas de registro forense.

Esta combinación de recursos posibilita la creación de un entorno de pruebas controlado, que reproduce las condiciones reales de una infraestructura institucional y hace posible la validación objetiva del desempeño del sistema propuesto.

3.2.1 Componentes de hardware

Los componentes de hardware utilizados permitieron establecer un entorno de pruebas controlado y adecuado para el desarrollo de las tareas de auditoría inalámbrica. La plataforma principal fue el WiFi Pineapple Pager, encargado de ejecutar los procesos de reconocimiento y monitoreo del espectro radioeléctrico en las bandas de 2.4 GHz, 5 GHz y 6 GHz. Asimismo, se emplearon dispositivos complementarios para simular un entorno institucional real y facilitar la interacción con las redes inalámbricas bajo estudio, siguiendo metodologías validadas en el contexto local [4].

Los componentes de hardware principales que se emplearon fueron:

- **WiFi Pineapple Pager:** Plataforma central de auditoría con soporte nativo tri-banda, batería integrada y motor PineAP para el procesamiento de eventos.
- **Router de pruebas inalámbrico:** Dispositivo configurado como un punto de acceso (AP) legítimo, que admite protocolos de seguridad WPA2/WPA3 y se emplea para crear la red de pruebas en el laboratorio.
- **Computador portátil (Estación de gestión):** Dispositivo utilizado para la administración remota de sistemas a través de conexiones SSH (acceso *root*) y *web*, además de la extracción y el estudio de registros forenses.

- **Dispositivos cliente inalámbricos:** *Smartphones* y *laptops* con adaptadores Wi-Fi estándar, empleados durante las pruebas experimentales para simular tráfico de red legítimo y comportamientos de asociación de usuarios.
- **Validación empírica de la autonomía energética:** aunque la documentación técnica del fabricante especifica una autonomía nominal de 4 horas por carga, durante las fases experimentales de este estudio se documentó el consumo real bajo carga de trabajo sostenida. Con los módulos Recon (*channel hopping* tri-banda), PineAP y los *payloads* de validación ejecutándose simultáneamente en modo *untethered*, el dispositivo registró una autonomía operativa efectiva de aproximadamente 3 horas y 45 minutos por sesión continua. Este registro empírico valida la portabilidad declarada del sistema y confirma su viabilidad para ejecutar auditorías itinerantes completas en el campus sin requerir conexión a la red eléctrica ni estaciones externas.

3.2.2 Componentes de software

Los componentes de software permitieron configurar y gestionar las funciones del sistema de auditoría. Entre ellos se encuentran las herramientas integradas en el WiFi Pineapple Pager, que proporcionan capacidades de reconocimiento, procesamiento de eventos y generación de alertas.

Los componentes de software principales que se emplearon durante la implementación fueron:

- **Firmware del WiFi Pineapple Pager:** Un sistema operativo embebido que se basa en OpenWRT y se encarga de los servicios y el hardware del dispositivo.
- **Dashboard de administración:** Interfaz web para la supervisión, configuración y control del sistema.
- **Cliente SSH:** Software de terminal PuTTY en Linux que permite acceder al dispositivo como root, permitiendo la configuración avanzada de scripts y la extracción de registros forenses.
- **Modo Recon:** Herramienta para la detección pasiva de puntos de acceso, dispositivos cliente y sus parámetros técnicos (canal, cifrado, BSSID, SSID y RSSI).
- **PineAP:** Núcleo operativo para la gestión y el procedimiento de eventos, captura de handshakes y despliegue controlado de Evil Twin.

- **Sistema de filtros:** Procedimiento para definir el alcance de la auditoría a través de listas de clientes y redes permitidos o denegados, garantizando que las pruebas permanezcan dentro del entorno autorizado.
- **Payloads:** se utilizaron scripts de la biblioteca obtenida por Hak5 para automatizar las tareas de reconocimiento forense.
- **Alertas:** Sistema de notificación para acontecimientos específicos (detección de ataques, conexión del cliente, captura de handshakes) mediante alertas táctiles, acústicas y visuales.

La integración de estos componentes permitió implementar una plataforma capaz de ejecutar procesos de auditoría inalámbrica y proporcionar información relevante sobre el comportamiento de las redes WiFi en el entorno experimental.

3.3 Configuración del WiFi Pineapple Pager

Configurar el WiFi Pineapple Pager es un paso esencial para hacer posible el sistema de auditoría inalámbrica, ya que permite las funciones requeridas para detectar, supervisar y procesar sucesos en el entorno de prueba. Los procesos de configuración se diseñaron para mejorar el rendimiento del dispositivo y simplificar la realización de tareas analíticas en las bandas de 2.4 GHz, 5 GHz y 6 GHz [5].

El proceso de configuración inicial incluyó las siguientes etapas:

1. **Actualización del firmware:** Verificación e instalación de la última versión del sistema operativo embebido para garantizar la compatibilidad con las funcionalidades tri-banda y el motor PineAP.
2. **Configuración de red:** Establecimiento de la conectividad del dispositivo mediante la interfaz web de administración (*dashboard*), configurando los parámetros de red para la gestión remota vía SSH y la extracción de *logs*.
3. **Activación del modo Recon:** Se activó el escaneo pasivo en las tres bandas de frecuencia (2.4 GHz, 5 GHz y 6 GHz) utilizando el mecanismo de "*channel hopping*", lo que permite la identificación del SSID, BSSID y los niveles de señal (RSSI).
4. **Configuración del PineAP:** Personalización de los parámetros de auditoría, que consiste en establecer filtros para restringir el alcance de las pruebas y habilitar la captura del handshake WPA/WPA2.

5. **Implementación de la biblioteca oficial de *payloads*:** Instalación y configuración de los *payloads* de la biblioteca oficial de Hak5 desde el repositorio GitHub, orientados a tareas de automatización, generación de alertas y registro forense.

La Figura 13 muestra la pantalla de bienvenida del sistema operativo del WiFi Pineapple Pager tras completar la actualización inicial del *firmware*.

Figura 13

Pantalla de bienvenida del WiFi Pineapple Pager

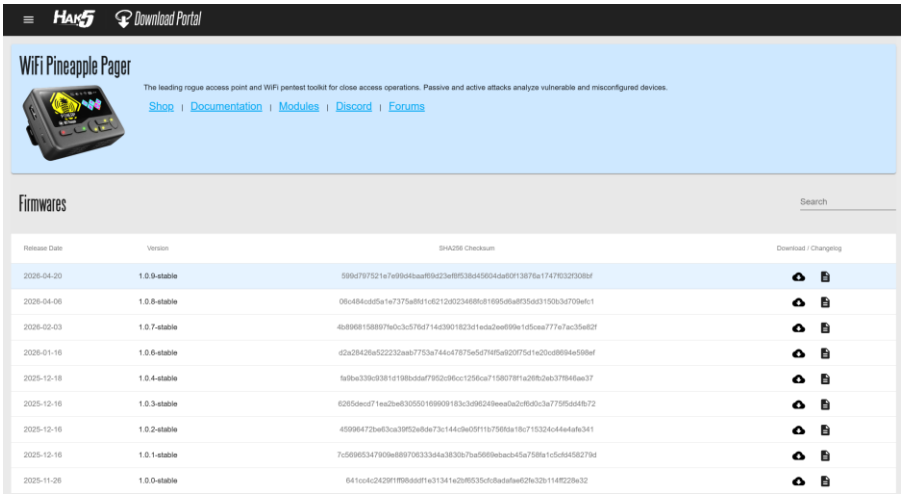
Nota. Interfaz de inicio del sistema operativo del WiFi Pineapple Pager tras la actualización del *firmware*. Fuente: Captura de pantalla, 2026.

3.3.1 Configuración inicial

La configuración inicial del WiFi Pineapple Pager se realizó siguiendo el procedimiento de puesta en marcha recomendado por el fabricante. En primer lugar, se descargó el *firmware* oficial desde el portal de Hak5, asegurando la disponibilidad de la versión más reciente para el dispositivo, como se muestra en la Figura 14.

Figura 14

Portal oficial de descargas de firmware para el WiFi Pineapple Pager



Nota. Interfaz del sitio web oficial de Hak5 para la descarga del firmware actualizado del dispositivo. Fuente: Captura de pantalla del portal de Hak5, 2026.

Posteriormente, se encendió el dispositivo manteniendo presionado el botón de encendido durante 3 a 4 segundos, y se conectó a un ordenador mediante un cable de datos USB-C de alta calidad, como se muestra en la Figura 15.

Figura 15

Encendido del dispositivo y conexión mediante cable USB-C

Nota. Proceso de encendido físico del WiFi Pineapple Pager y conexión al ordenador de gestión mediante cable USB-C. Fuente**:** Captura de pantalla del dispositivo en el laboratorio de la UPSE, 2026.

Se verificó que el sistema fuera reconocido como un dispositivo Ethernet USB Realtek RTL8153, permitiendo acceder a la interfaz de administración mediante un navegador web en la dirección 172.16.52.1:1471. A través del servidor web Stager, se realizó la carga del firmware, manteniendo una alimentación constante durante el proceso para evitar fallos. La interfaz correspondiente se presenta en la Figura 16.

Figura 16

Carga del firmware mediante el servidor web stager

Nota. Interfaz del servidor web Stager utilizada para la carga e instalación del firmware en el dispositivo. Fuente: Captura de pantalla del dispositivo en el laboratorio de la UPSE, 2026.

Después de finalizar el procedimiento de instalación del *firmware*, el sistema realizó su primer arranque y llevó a cabo tareas esenciales como la partición de la memoria flash interna, el formateo del sistema y la creación automática de claves SSH. Luego, a través del panel direccional (*D-pad*) y los botones "A" (confirmar) y "B" (regresar), se llevó a cabo la configuración básica directamente desde el aparato. En esta fase, se configuraron el PIN de seguridad y la contraseña del usuario root, que son imprescindibles para acceder remotamente a través de SSH y para administrar el entorno virtual del WiFi Pineapple Pager. Las Figuras 17 y 18 muestran este proceso.

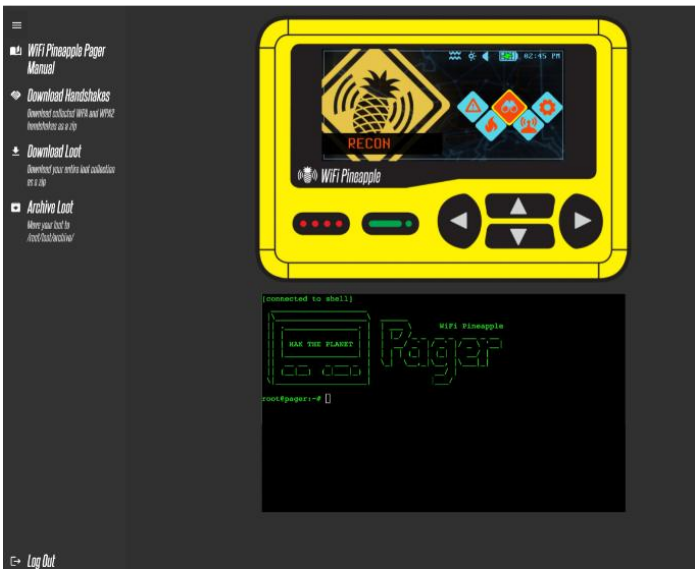
Figura 17

Interfaz de inicio de sesión (172.16.52.1:1471)

Nota. Pantalla de inicio de sesión del entorno virtual del WiFi Pineapple Pager, accesible mediante la dirección IP 172.16.52.1:1471. Fuente: Captura de pantalla, 2026.

Figura 18

Panel principal del WiFi Pineapple Pager virtual.



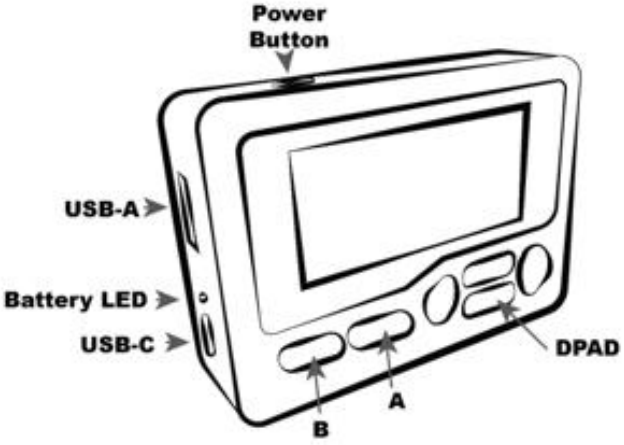
Nota. Interfaz principal del entorno virtual del WiFi Pineapple Pager, donde se gestionan las funciones de configuración, monitoreo y control del dispositivo. Fuente: Captura de pantalla del dispositivo, 2026.

3.3.2 Descripción física del dispositivo

La operatividad del WiFi Pineapple Pager se gestiona de manera autónoma mediante una interfaz física optimizada para la movilidad (untethered), permitiendo al auditor ejecutar procedimientos de seguridad sin depender de terminales externas. El dispositivo incorpora diversos elementos de control y puertos de conectividad que facilitan la interacción con el sistema operativo embebido, como se muestra en la Figura 19.

Figura 19

Componentes físicos y elementos de control del WiFi Pineapple Pager



Nota. Elementos de control y puertos de conectividad del WiFi Pineapple Pager. ***Fuente:*** *Captura de pantalla del dispositivo Hak5, 2026.*

Arquitectura de control y botones físicos

- El sistema de navegación está conformado por un pad direccional (D-pad), que permite el desplazamiento a través de los menús del dispositivo. Las direcciones izquierda y derecha posibilitan un desplazamiento más rápido en listas extensas, como los módulos *Recon* y *Payloads*, así como la selección de diferentes vistas en los gráficos generados por el sistema.
- El botón de acción «A» (verde) se emplea para confirmar operaciones, acceder a submenús y reconocer alertas críticas. El botón «B» (rojo) proporciona la función de retroceso dentro de la estructura jerárquica de los menús y permite interrumpir procesos en ejecución.
- El dispositivo dispone de un botón de encendido en la parte superior, que permite un arranque seguro manteniéndolo presionado durante 3 a 4 segundos.

Mediante una doble pulsación es posible acceder al menú de gestión rápida del sistema.

- En cuanto a la conectividad, el WiFi Pineapple Pager incorpora un puerto USB-C destinado a la carga de la batería y al acceso administrativo mediante la interfaz Ethernet USB basada en el controlador Realtek RTL8153. También dispone de un puerto USB-A que permite la expansión de funcionalidades mediante la conexión de dispositivos externos, como receptores GPS, adaptadores inalámbricos o antenas especializadas.

3.3.3 Interfaz del dashboard

El dashboard del WiFi Pineapple Pager es la interfaz principal de administración del sistema, proporcionando una visión general del estado operativo del dispositivo y acceso a las diferentes funciones disponibles. Esta interfaz se encarga de supervisar los procesos de reconocimiento, la actividad de los eventos que se van detectando y los datos que arrojan las redes WiFi presentes en el entorno de pruebas. El panel de control (*dashboard*) centraliza la visualización de las métricas críticas del sistema, el estado de los módulos activos, las interfaces de red disponibles y el registro histórico de eventos de auditoría. Esto optimiza el monitoreo y seguimiento del dispositivo, permitiendo la verificación de resultados en tiempo real y eliminando la necesidad de consolidar registros aislados de forma manual. La utilización del *dashboard* centraliza las tareas de administración y simplifica el acceso a los diferentes módulos del sistema, proporcionando una gestión eficiente de las funciones de auditoría implementadas durante la investigación. La Figura 20 presenta la interfaz principal del *dashboard* y los elementos más relevantes para la administración del dispositivo.

Figura 20

Interfaz principal del Dashboard del WiFi Pineapple Pager

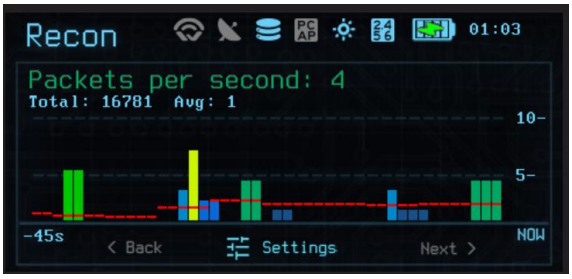
Nota. Interfaz del *dashboard* del WiFi Pineapple Pager mostrando el módulo Recon activo. Fuente: Captura de pantalla del dispositivo, Hak5 2026.

3.3.4 Operación del modo Recon

Esta sección documenta la configuración y operación del modo Recon durante las pruebas experimentales. Los fundamentos teóricos del reconocimiento pasivo fueron descritos en la sección 2.4.7. Para establecer la línea base de seguridad y el inventario de activos de red en el entorno radioeléctrico, se implementó el modo Recon del dispositivo. Esta funcionalidad opera bajo monitoreo pasivo, configurando las interfaces en modo monitor (promiscuo) para capturar tramas de control, gestión y datos sin interactuar con las redes circundantes. El flujo y volumen de datos capturados se visualiza gráficamente en la interfaz, como se muestra en la Figura 21.

Figura 21

Panel de control (dashboard) del modo Recon



Nota. Panel de control del modo Recon mostrando ráfagas de paquetes por segundo y volumen de tráfico detectado. Fuente: Captura de pantalla del dispositivo, Hak5 2026.

El reconocimiento se ejecutó concurrentemente sobre las bandas de 2.4 GHz, 5 GHz y 6 GHz mediante salto automático de canales (*channel hopping*), distribuyendo el tiempo de escucha de forma secuencial y cíclica entre los canales permitidos de cada banda, maximizando la interceptación de tramas de baliza (*Beacon Frames*) y solicitudes/respuestas de sonda (*Probe Requests/Responses*). El sistema consolida un inventario en una lista estructurada, como se observa en la Figura 22.

Figura 22

Lista consolidada de puntos de acceso (APs) identificados

Nota. Lista de puntos de acceso identificados mediante escaneo pasivo en el entorno de pruebas. Fuente: Captura de pantalla del dispositivo, Hak5 2026.

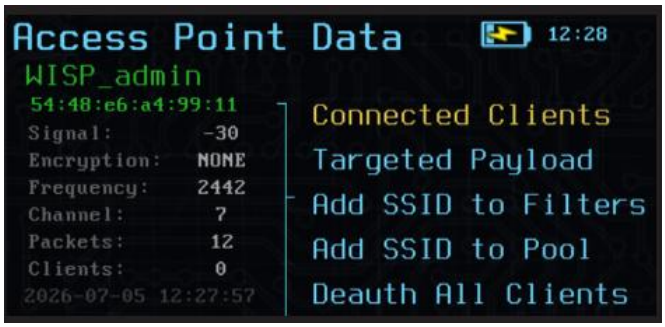
A través de la decodificación en tiempo real, el sistema extrae y almacena:

- **SSID (Service Set Identifier**): Nombre público de la red.
- **BSSID (Basic Service Set Identifier):** Dirección MAC del AP.
- **Canal y Ancho de Banda**: Frecuencia y espectro utilizado.
- **Mecanismo de Seguridad:** Protocolos de autenticación (WPA2-PSK, WPA3-SAE, OWE, etc.).
- **Clientes Asociados:** Direcciones MAC de estaciones (STA) vinculadas a un BSSID.
- **RSSI (Received Signal Strength Indicator):** Intensidad de señal en dBm.

Para auditoría avanzada, el sistema permite aislar objetivos detectados. Al seleccionar un elemento del inventario, se despliega un análisis detallado de la red y sus vulnerabilidades, así como de las estaciones clientes vinculadas, como se ejemplifica en la Figura 23.

Figura 23

Vista detallada de parámetros de seguridad y clientes asociados



Nota. Vista detallada de parámetros de seguridad, canalización y estaciones clientes asociadas a un objetivo seleccionado. Fuente: Captura de pantalla del dispositivo, 2026

Detección de Protected Management Frames (PMF / 802.11w)

Como parte del análisis de seguridad de las redes detectadas, el módulo Recon del WiFi Pineapple Pager identifica si un punto de acceso tiene habilitado el soporte para *Protected Management Frames* (PMF), conforme al estándar IEEE 802.11w-2009 [6]. La detección se realiza mediante el análisis de las tramas de baliza (*Beacon Frames*) y las tramas de respuesta de sonda (*Probe Response*), verificando la presencia del elemento de información RSN (*Robust Security Network)* y, dentro de este, el campo RSN *Capabilities* que contiene los bits de capacidad de PMF.

La clasificación se determina según los siguientes criterios:

- **PMF requerido (*required*):** el AP exige PMF a todo los clientes (MFPC =1 y MFPR= 1 en el campo RSN Capabilities).
- **PMF opcional (*optional*):** el AP soporta PMF, pero no lo exige (MDPC=1 y MFPR=0).
- **PMF no soportado (Not Capable):** el AP no implementa PMF (MFPC=0 y MFPR=0).

Durante las pruebas experimentales se registró la capacidad de PMF de cada punto de acceso detectado (validación por AP en la Tabla 4, capítulo IV). Los resultados consolidados se presentan en la Tabla 5, donde se evidencia que el 100 % de las redes WPA2 detectadas no implementan PMF, lo que las hace vulnerables a ataques de desautenticación.

3.3.5 Operación del sistema PineAP

En esta sección se documenta la configuración operativa específica aplicada durante las pruebas experimentales. PineAP se activó en modo de correlación con el módulo Recon, procesando las tramas de *probe requests* capturadas durante el *channel hopping*. La configuración operativa incluyó:

- ***SSID pool:*** activado para almacenar automáticamente los identificadores de red detectados.
- ***Collect handshakes:*** habilitado para capturar intercambios EAPOL WPA/WPA2.
- ***Mimic Open Networks:*** configurando exclusivamente para el SSID "ESTUDIANTES" (filtro Allow).

El estado operativo del servicio en su panel de control se ilustra en la Figura 24.

Figura 24

Módulo de control del sistema PineAP

Nota. Módulo de control del sistema PineAP mostrando el estado activo del servicio y las opciones de gestión de identidades inalámbricas (SSID Pool, Open AP, Evil WPA, Filters). Fuente: Captura de pantalla del dispositivo, Hak5 2026.

PineAP se integra estrechamente con el motor de Recon. Mientras el modo Recon realiza el barrido cíclico mediante *channel hopping* para interceptar balizas (*beacon frames*), PineAP procesa y almacena las solicitudes de sonda (*probe requests*) emitidas por los dispositivos clientes. Mediante este mecanismo, el sistema ejecuta automáticamente dos tareas analíticas: la estructuración de un repositorio local con las identidades de red (SSID Pool) y la vinculación entre direcciones MAC de estaciones emisoras y los perfiles de redes previamente conocidas. A continuación, se puede observar en la Figura 25 una interfaz de puntos de accesos.

Figura 25

Vista del repositorio local SSID Pool

Nota. Conjunto de identificadores de red detectados durante la auditoría y administrado por PineAP, en un repositorio local SSID Pool. Fuente: Captura de pantalla del dispositivo, Hak5 2026

Al centralizar esta información, se logra automatizar la persistencia de las evidencias electrónicas y se evita que la información volátil se pierda durante el salto de frecuencia. Esto ofrece un marco firme para realizar una evaluación de vulnerabilidad posterior y un registro forense.

3.3.6 Configuración de filtros

Los filtros constituyen una herramienta complementaria del sistema PineAP, permitiendo establecer criterios específicos para el tratamiento de la información obtenida durante el reconocimiento y monitoreo del entorno inalámbrico. Mediante esta funcionalidad es posible controlar la gestión de puntos de acceso y dispositivos clientes detectados por el sistema. Durante la implementación, se configuraron mecanismos de filtrado para optimizar el análisis y facilitar la identificación de dispositivos en el entorno experimental. Como se observa en la Figura 26, PineAP dispone de filtros aplicados a redes inalámbricas, permitiendo establecer listas de redes autorizadas y restringidas mediante políticas de inclusión y exclusión.

Figura 26

Configuración del filtro de redes del sistema PineAP

Nota. Interfaz de configuración para la administración de listas permitidas y restringidas de redes inalámbricas detectadas durante el proceso de auditoría. Fuente: Captura de pantalla del dispositivo, Hak5 2026

La Figura 27 muestra la configuración de filtros aplicados a dispositivos clientes, permitiendo administrar listas de dispositivos permitidos y denegados. La utilización de estos mecanismos reduce el procesamiento de información no relevante y favorece la focalización del análisis sobre los elementos de interés definidos durante la auditoría.

Figura 27

Configuración del filtro de clientes del sistema PineAP

Nota. Interfaz de configuración para la administración de listas permitidas y restringidas de dispositivos clientes detectadas durante las tareas de monitoreo inalámbrico. Fuente**:** Captura de pantalla del dispositivo, Hak5 2026

La implementación de filtros proporciona flexibilidad operativa, permitiendo adaptar el comportamiento del sistema a diferentes escenarios de evaluación y fortaleciendo las capacidades de monitoreo y supervisión del WiFi Pineapple Pager.

3.4 Diseño del entorno experimental

Para validar el funcionamiento del sistema de auditoría inalámbrica propuesto, se diseñó un entorno experimental controlado que replica las condiciones operativas de la

infraestructura tecnológica de la Universidad Estatal Península de Santa Elena (UPSE). El escenario se configuró para evaluar la capacidad del sistema en la detección proactiva, análisis y registro forense de dispositivos y eventos en el espectro radioeléctrico (2.4 GHz, 5 GHz y 6 GHz). El entorno experimental se implementó utilizando el WiFi Pineapple Pager como plataforma central de monitoreo y auditoría, complementado con la infraestructura de red existente en el campus universitario y estaciones cliente institucionales. Esto permitió generar escenarios de comunicación controlados que reflejan la operación diaria de las redes WiFi utilizadas por estudiantes, docentes y personal administrativo.

Vectores de amenaza simulados

Para evaluar la robustez del sistema y su capacidad de detección, se ejecutaron pruebas controladas simulando vectores de amenaza comunes en entornos institucionales:

- ***Evil Twin:*** suplantación controlada del punto de acceso legítimo "ESTUDIANTES" mediante la clonación de su SSID y BSSID, con el objetivo de capturar *handshakes* y registrar dispositivos que intentan asociarse a la red fraudulenta.
- **Inyección de desautenticación** (*deauth*): envío de tramas de desautenticación en las bandas de 2.4 GHz y 5 GHz para obligar la reconexión del cliente y la captura de la negociación WPA/WPA2. (Nota: En la banda de los 6 GHz, no se puede utilizar este método porque WiFi 6E exige una protección PMF obligatoria).
- **Captura de *handshake*:** intercepción pasiva del protocolo de autenticación entre los clientes y los puntos de acceso, lo que posibilita un análisis posterior de la solidez de la clave precompartida (PSK) para fines de registro forense.
- **Detección de *rogue APs*:** detección de puntos de acceso no autorizados que están en el entorno, analizando la capacidad del sistema PineAP para diferenciar entre una infraestructura legítima y dispositivos fraudulentos a través de la correlación BSSID y SSID.

Detección de vulnerabilidades en el entorno

Además, el WiFi Pineapple Pager funcionó como un sensor de seguridad activo en el entorno de prueba, lo cual posibilitó la detección anticipada de configuraciones inseguras sin perturbar el funcionamiento de la red institucional:

- **Identificación de cifrado obsoleto:** se detectaron puntos de acceso con protocolos de seguridad vulnerables (WEP, WPA-TKIP) o redes no autenticadas (*open*) usando el

modo Recon, registrando el SSID, BSSID y el nivel de señal (RSSI) para análisis posteriores.

- **Detección de *rogue APs*:** se utilizó PineAP para activar la detección automática de puntos de acceso no autorizado, con el fin de valorar la capacidad del sistema de diferenciar entre puntos de acceso legítimos y fraudulentos.
- **Monitoreo de comportamiento de clientes:** los equipos que intentan conectarse automáticamente a redes previamente conocidas o que no validan los certificados de seguridad pueden identificarse gracias al registro de las solicitudes de sondeo realizadas por los dispositivos cliente.
- **Captura de evidencias forenses:** se configuró la captura automática de handshakes WPA/WPA2, almacenando los protocolos de autenticación en formato .pcap y .hc22000 para su posterior análisis con herramientas externas como Wireshark y Aircrack-ng.

Configuración de pruebas y métricas

Cada escenario se ejecutó bajo condiciones estrictamente controladas, utilizando los filtros de PineAP para delimitar el alcance de las pruebas exclusivamente a la red seleccionada de la UPSE. Para el capítulo IV, se establecieron las siguientes métricas de evaluación:

- **Tasa de detección:** la cantidad de dispositivos clientes asociados en la simulación Evil Twin
- **Eficacia de captura:** la proporción de intercambios de claves WPA/WPA2 registrados con éxito.
- **Tiempo de respuesta:** retraso entre la creación de una alerta del sistema y la detección de un suceso.
- **Precisión en identificación:** precisión a la hora de distinguir entre puntos de acceso no autorizados y puntos de acceso legítimos.
- **Volumen de evidencias:** la cantidad de *handshakes,* alertas y solicitudes de sondeo que se documentan para el análisis forense.

El desarrollo se realizó bajo supervisión en el laboratorio de FACISTEL UPSE, garantizando que las pruebas se ajustarían estrictamente a los marcos éticos y normativos aplicables, como la Ley Orgánica de Protección de Datos Personales de Ecuador, y que no tendrían ningún impacto en las redes de terceros ni en la infraestructura externa [8].

3.4.1 Escenario de pruebas / topología de red

El escenario experimental se diseñó para replicar un entorno institucional de mediana escala correspondiente al campus de la Universidad Estatal Península de Santa Elena (UPSE), considerando la distribución física de las instalaciones y la topología lógica de la infraestructura inalámbrica existente. La arquitectura de pruebas contempla la interacción dinámica entre tres componentes principales: puntos de acceso institucionales legítimos, dispositivos cliente activos y la plataforma de auditoría móvil (WiFi Pineapple Pager).

Ubicación geográfica y topología del campus

La infraestructura inalámbrica abarca múltiples edificaciones, siendo el foco principal de esta investigación el Edificio Bloque 1, y sus aulas adyacentes. Se incluyeron como zonas de referencia periférica el Edificio Bloque 2, el Área Docente y el *Lab Control*. La Figura 28 presenta el mapa del campus con la ubicación de los puntos de acceso WiFi detectados durante la fase de reconocimiento.

Figura 28

Mapa del campus de la UPSE con ubicación de puntos de acceso WiFi

Nota**.** Mapa satelital del campus de la UPSE con la ubicación de los puntos de acceso institucionales detectados. Las áreas sombreadas representan la cobertura estimada basada en mediciones de RSSI. Fuente: Google Maps (2026).

Topología lógica y configuración del auditor

Para garantizar una evaluación técnica rigurosa, se implementó una topología experimental que abarca las tres bandas de frecuencia soportadas por el WiFi Pineapple Pager diferenciadas de la siguiente forma esquemática:

- **Banda 2.4 GHz:** operada en modo activo (*Evil Twin / Open Mimicry*) debido a su mayor alcance y compatibilidad con dispositivos *legacy/IoT* presentes en el campus.

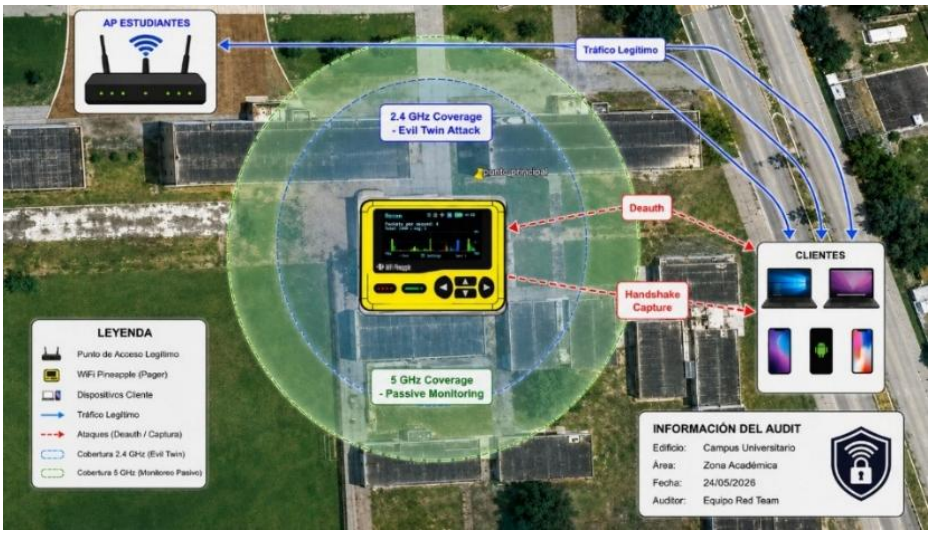
Esta banda se utilizaba para capturar los protocolos de enlace WPA2 de redes encriptadas cercanas e imitar la suplantación de identidad en redes abiertas.

- **Banda 5 GHz:** se utiliza principalmente en modo pasivo (reconocimiento/monitoreo) para evaluar redes de alta densidad e identificar clientes actuales (WiFi 5/6), respetando las limitaciones de la normativa *DFS* al no inyectar paquetes de desautenticación.
- **Banda 6 GHz:** operada en modo de escaneo pasivo y monitoreo de espectro. A pesar de la capacidad técnica del WiFi Pineapple Pager para interactuar en este espectro, durante la fase experimental no se detectó infraestructura ni tráfico asociado al estándar WiFi 6E/7 (802.11ax/be) en el campus de la UPSE. Este resultado confirma que la infraestructura inalámbrica institucional actual en la zona de estudio aún no ha migrado a la banda de 6 GHz, limitando la experimentación en esta frecuencia a la validación de la ausencia de dispositivos en dicho espectro [11].

Para optimizar la relación señal-ruido, el dispositivo se ubicó en el centro del Laboratorio de Telecomunicaciones. Para evitar interferencias de redes no autorizadas, el motor PineAP se configuró utilizando *Mimic Open Networks* y *Collect Handshakes*, aplicando filtros "*Allow*" limitados al SSID "ESTUDIANTES". La Figura 29 muestra la distribución espacial del escenario.

Figura 29

Distribución espacial del escenario experimental



Nota. Escaneo pasivo para la ejecución de prueba. Fuente: Google Maps 2026.

Características del entorno de pruebas

- **Red objetivo:** Punto de acceso con SSID "ESTUDIANTES", configurado como red abierta *(Open Network*). Esta red fue elegida porque representa un grave riesgo para los

entornos educativos, donde la falta de cifrado facilita el robo de identidad y la interceptación de tráfico. Los laboratorios y las aulas están cubiertos por el punto de acceso principal, ubicado en el segundo piso del Edificio de Sistemas.

- **Dispositivos clientes:** Smartphones (Android/iOS) y portátiles (Windows/macOS) operados por estudiantes y docentes durante horarios lectivos (08h00-12h00 y 13h00-16h00). Las capacidades de detección del auditor pudieron confirmarse en entornos de carga reales, ya que estos dispositivos generaron tráfico genuino y solicitudes de sondeo.
- **Condiciones ambientales:** Las pruebas se realizaron en el momento de mayor actividad estudiantil, durante el semestre académico ordinario. El clima era costero, con temperaturas entre 26 y 30 °C y niveles de humedad entre el 75 y el 85 %, lo que puede tener un ligero impacto en la atenuación de la señal. Entre las fuentes de interferencia co-canal se encontraban barreras físicas comunes como puertas metálicas y muros de bloques, así como redes residenciales cercanas, dispositivos Bluetooth y equipos de microondas en cafeterías.

Limitaciones del escenario

Durante el reconocimiento espectral, no se encontraron puntos de acceso activos en la banda de 6 GHz en el campus ni en el área cercana, a pesar de que el WiFi Pineapple Pager tiene capacidad para operar en tres bandas (2.4, 5 y 6 GHz). Este hallazgo documenta que, al momento de la investigación (2026), la infraestructura institucional no ha migrado a tecnología WiFi 6E, limitando la auditoría en dicha banda a pruebas de concepto de hardware únicamente.

3.5 Procedimientos de prueba y ejecución de payloads

El procedimiento experimental se desarrolló siguiendo una secuencia metodológica estructurada con el propósito de garantizar la reproducibilidad de las pruebas y la confiabilidad de los datos obtenidos durante la investigación. Durante el reconocimiento espectral, no se encontraron sitios de acceso activos en la banda de 6 GHz en el campus ni en el área cercana, a pesar de que el WiFi Pineapple Pager tiene capacidad para operar en tres bandas (2.4 GHz, 5 GHz y 6 GHz).

3.5.1 Diseño experimental y condición de control

Para garantizar la validez y reproducibilidad de los resultados, el procedimiento experimental se estructuró en tres fases temporales independientes ejecutadas bajo

condiciones controladas equivalentes, aprovechando la capacidad del WiFi Pineapple Pager para archivar automáticamente las evidencias por sesión mediante el comando *PINEAPPLE_LOOT_ARCHIVE*. Como se muestra en la Tabla 3.

Tabla 3

Diseño experimental: fases temporales y condiciones de control

Fase	Fecha	Horario	Condiciones Ambientales	Escenarios ejecutados
Fase 1 (Validación inicial)	09/04/2026	09:00-12:00	Campus UPSE, laboratorio controlado	Reconocimiento pasivo*, Open AP, Evil WPA*
Fase 2 (Iteración y refinamiento)	20/05/2026	08:00-16:00	Campus UPSE, horario lectivo	Reconocimiento, *Evil Twin*, captura *handshakes*, VERDANDI v2.0
Fase 3 (Validación final)	07/07/2026	09:43-16:11	Campus UPSE, mayor densidad de clientes	Todas las pruebas, validación criptográfica de *handshakes*

Nota. Datos tomados de las pruebas realizadas en la universidad, 2026.

Cada fase operó bajo las siguientes condiciones de control:

- **Filtros PineAP**: Red objetivo limitada exclusivamente al SSID institucional "ESTUDIANTES" (modo *Allow*) para evitar interferencia con redes de terceros.
- **Bandas activas:** 2.4 GHz y 5 GHz en modo activo; 6 GHz en modo pasivo (por restricciones regulatorias WiFi 6E/PMF).
- **Ubicación del auditor:** Laboratorio de Telecomunicaciones (punto central del escenario experimental).
- **Almacenamiento:** Evidencias archivadas automáticamente en /root/loot/archive/ con *timestamp* por sesión.

Este diseño de tres fases independientes permite validar la consistencia de los resultados a lo largo del tiempo y documenta la evolución iterativa del sistema propuesto, superando la limitación de estudios previos con diseños de una sola sesión.

Alcance estadístico y unidad experimental

El presente trabajo se declara un estudio piloto / caso de estudio de alcance descriptivo. La unidad experimental, se define como la sesión de auditoría (fase temporal), y las réplicas independientes corresponden a las tres fases ejecutadas en fechas y condiciones distintas (Tabla 3). Los archivos .pcap no se tratan como tamaño muestral; todas las proporciones se reportan con intervalos de confianza al 95 % calculados mediante el método de Wilson, siguiendo las recomendaciones de la literatura metrológica para la estimación de incertidumbre en sistemas de instrumentación [28].

Fase 1: Preparación y configuración del entorno

El WiFi Pineapple se configuró de acuerdo con las especificaciones indicadas para las pruebas experimentales previas a las operaciones de auditoría.

Activación de bandas

Se realizaron pruebas activas, incluyendo el reconocimiento, la detección y la captura de la comunicación entre dispositivos, en las bandas de 2.4 GHz y 5 GHz. Debido a las limitaciones del estándar WiFi 6E, que exige el uso de tramas de gestión protegidas (PMF) para prevenir ataques de desautenticación, solo se llevó a cabo una monitorización pasiva en la banda de 6 GHz. La disposición de las bandas auditables se muestra en la Figura 30.

Figura 30

Configuración de bandas de frecuencia habilitadas

Nota. Configuración de bandas disponibles (6 GHz, 5 GHz, 2.4 GHz). Se habilitaron 2.4 GHz y 5 GHz para pruebas activas; 6 GHz en modo pasivo por restricciones WiFi 6E (PMF). Fuente: Captura de pantalla del dispositivo, Hak5, 2026

Configuración de PineAP

Para garantizar que las pruebas se realizaran únicamente sobre la infraestructura autorizada, se configuró el Network Filter en modo Allow, incorporando exclusivamente el

SSID "ESTUDIANTES" en la lista de redes permitidas. El *client filter* se configuró en modo Deny con lista vacía, permitiendo conexión de cualquier cliente sin restricciones adicionales. Las figuras presentan la configuración de filtros de redes y clientes. Las Figuras 31 y 32 presentan la configuración de filtros de redes y clientes.

Figura 31

Configuración del filtro de redes permitidas (Network Filter)

Nota: Interfaz del dispositivo con Network Filter en Allow y gestión de redes autorizadas/denegadas. Fuente: captura de pantalla, Hak5 2026.

Figura 32

Configuración de filtros de clientes (Client Filter)

Nota. Interfaz del dispositivo con Client Filter en Deny (resaltado en rojo), permitiendo conexiones sin restricciones al Open AP. Fuente: Captura de pantalla, Hak5 2026.

Instalación y verificación de la biblioteca de payloads

Como parte de la preparación, se verificó la correcta instalación de la biblioteca oficial de *payloads* de Hak5. La Figura 33 muestra la categoría "reconnaissance" de la biblioteca, destacando la herramienta *wpa_handshake_quality_check* para validar la integridad de los *handshakes* capturados.

Figura 33

Menú de payloads de la categoría reconnaissance

Nota. Categoría "reconnaissance" de la biblioteca oficial (pág. 7/7) con la herramienta wpa_handshake_quality_check para validar handshakes. Fuente: captura de pantalla, Hak5 2026.

Validación de handshakes mediante wpa_handshake_quality_check

El payload *wpa_handshake_quality_check* de la biblioteca oficial de Hak5 [5] fue implementado para automatizar la validación de los handshakes capturados durante las pruebas experimentales. Este script realiza un análisis criptográfico de los archivos .pcap almacenados en el directorio /mmc/root/loot/handshakes/ y los clasifica en tres categorías:

- ***VALID_FULL*:** *Handshake* completo que contiene los cuatro paquetes EAPOL (Message 1, 2, 3 y 4) intercambiados durante el proceso de autenticación WPA/WPA2. Este tipo de *handshake* es forensemente válido y puede ser utilizado para ataques de fuerza bruta offline.
- ***PARTIAL*:** *Handshake* incompleto que carece de uno o más paquetes EAPOL. No es utilizable para ataques de fuerza bruta, pero puede contener información útil para análisis de tráfico.
- ***INVALID*:** Archivos corruptos o que no contienen un *handshake* válido.

Adicionalmente, el *script* verifica la presencia del PMKID (Pairwise Máster Key Identifier) en el elemento de información RSN de las tramas capturadas, lo que permite identificar redes susceptibles a ataques de recuperación de PMKID sin necesidad de capturar el *handshake* completo. Finalmente, el proceso aplica un algoritmo de duplicación que descarta las capturas redundantes correspondientes al mismo evento de autenticación (mismo BSSID y *timestamp*), reteniendo únicamente *handshakes* únicos.

La ejecución del *payload* se realizó mediante la interfaz de payloads del WiFi Pineapple Pager, seleccionando la categoría "reconnaissance" (figura 33) y ejecutando el script sobre el directorio de capturas. El resultado de la validación se almacena en la carpeta /mmc/root/loot/handshakes_sorted/, organizando automáticamente los archivos en subdirectorios según su clasificación (*VALID_FULL, PARTIAL, INVALID*), cuya distribución consolidada se presenta en la Figura 34. Es preciso señalar que la validación de un *handshake* confirma su integridad criptográfica como evidencia de autenticación, no la recuperación de la clave precompartida de la red.

Figura 34

Salida del payload wpa_handshake_quality_check

Nota. La salida del script muestra la clasificación automática de handshakes en las categorías *VALID_FULL, PARTIAL* e *INVALID*, así como la verificación de PMKID en las redes WPA2.

Fase 2: Reconocimiento pasivo y evaluación activa

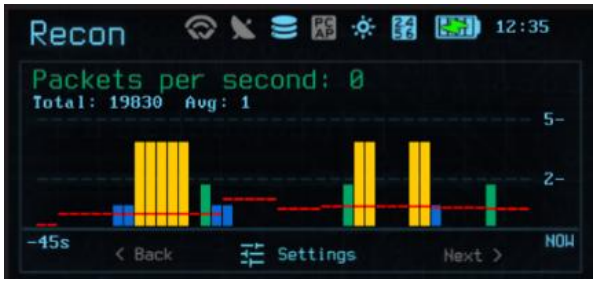
Una vez configurado el dispositivo, se ejecutó el reconocimiento del entorno inalámbrico y las pruebas activas controladas.

Reconocimiento del espectro inalámbrico (*Recon*)

Se activó el modo Recon con la función de *channel hopping*, permitiendo recorrer automáticamente los diferentes canales disponibles para identificar redes inalámbricas y dispositivos clientes presentes dentro del área de cobertura. La Figura 35 muestra el tráfico de paquetes detectado durante el escaneo pasivo.

Figura 35

Módulo Recon durante el proceso de reconocimiento inalámbrico



Nota. Visualización del *channel hopping* en las bandas de 2.4 GHz y 5 GHz. La ausencia de actividad en 6 GHz es consistente con la inexistencia de infraestructura WiFi 6E en el entorno de pruebas de la UPSE. Fuente: Captura de pantalla del dispositivo Hak5, 2025.

Identificación de redes inalámbricas

Durante la sesión de reconocimiento, el sistema detectó e identificó los puntos de acceso presentes en el entorno, registrando información técnica como SSID, BSSID, canal, banda, RSSI y tipo de cifrado. La Figura 36 presenta la lista de APs detectados.

Figura 36

Redes inalámbricas detectadas durante el reconocimiento pasivo

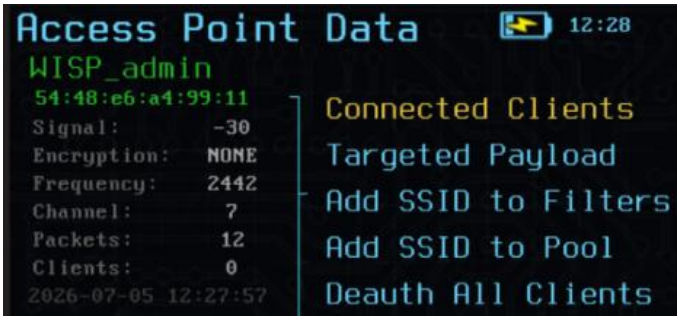
Nota. APs detectados en 2.4/5 GHz, destacando la red abierta "*ESTUDIANTES*" (*NONE, canal 157*). Fuente: Captura de pantalla, Hak5 (2026).

Análisis del punto de acceso objetivo

Una vez identificado el punto de acceso objetivo durante la fase de reconocimiento, se procedió a su selección para visualizar la información técnica disponible y utilizar los payloads de reconocimiento instalados. La Figura 37 muestra los detalles del AP seleccionado, incluyendo dirección MAC, intensidad de señal, tipo de cifrado, frecuencia y canal de operación.

Figura 37

Información del punto de acceso objetivo obtenida mediante el módulo Recon



Nota. Detalles técnicos del AP "WISP_admin" seleccionado: cifrado NONE, canal 7 (2442 MHz), señal -30 dBm, sin clientes asociados. Fuente: Captura del dispositivo Hak5, 2026.

Suplantación controlada (*Evil Twin*)

Con el objetivo de evaluar el comportamiento de los clientes inalámbricos ante escenarios de suplantación de identidad, se configuraron dos tipos de puntos de acceso controlados utilizando las funcionalidades del WiFi Pineapple Pager:

- **Escenario 1: Red abierta (*Open AP*)**

Se configuró un punto de acceso abierto utilizando el módulo open AP, estableciendo el SSID "*ESTUDIANTES*" y habilitando la función *Advertise Networks* para anunciar el punto de acceso durante las pruebas. Este escenario simula la suplantación de redes institucionales sin cifrado, permitiendo evaluar la vulnerabilidad de dispositivos que se conectan automáticamente a redes abiertas. La Figura 38 muestra la configuración del módulo open AP.

Figura 38

Configuración del punto de acceso controlado mediante open AP

Nota. La opción open AP donde se establece el SSID "ESTUDIANTES" para la suplantación controlada de redes abierta. Fuente: Captura de pantalla del dispositivo Hak5.

- **Escenario 2: Red con cifrado WPA/WPA2 (*Evil WPA*)**

Adicionalmente, se configuró un punto de acceso controlado utilizando el módulo Evil WPA Setup, el cual permite clonar redes con cifrado WPA/WPA2. Se establecieron el SSID objetivo, el BSSID del AP legítimo, el tipo de cifrado y la frase de acceso correspondiente. Este escenario evalúa la capacidad del sistema para simular redes cifradas y capturar handshakes de autenticación. La Figura 39 muestra la interfaz de configuración del módulo Evil WPA.

Figura 39

Configuración del punto de acceso controlado mediante Evil WPA

Nota. Interfaz de configuración del módulo *Evil WPA* Setup, donde se establecen el nombre de red (*Network Name*), sobrescritura de BSSID (BSSID *Override*), tipo de cifrado (*Encryption Type*) y frase de acceso (*Passphrase*) para la suplantación controlada de redes cifradas. Fuente: Captura de pantalla del dispositivo Hak5*, 2026.*

Monitoreo de clientes asociados

Durante la ejecución de las pruebas, se supervisó la conexión de dispositivos al punto de acceso controlado, verificando parámetros como dirección IP, MAC e intensidad de señal. La Figura 40 muestra los clientes conectados al AP controlado.

Figura 40

Clientes conectados al punto de acceso controlado

Nota. Interfaz PineAP Clients mostrando tres dispositivos asociados al Open AP, con direcciones IP en el rango 172.16.52.x, direcciones MAC e intensidad de señal entre -64 y -76 dBm. Fuente: Captura de pantalla del dispositivo Hak5.

Detección de vulnerabilidades y registro de evidencias

Durante la ejecución de las pruebas, el sistema operó como sensor de seguridad, detectando y registrando automáticamente las siguientes vulnerabilidades en el entorno institucional:

- **Cifrado obsoleto (WEP/WPA-TKIP)**
  Identificado mediante el modo Recon, registrando SSID, BSSID y tipo de cifrado en los registros de auditoría.
- **Open Network**
  Identificados mediante la localización de redes no autenticadas, lo que permite evaluar el peligro de robo de identidad e interceptación de tráfico.
- **Rogue APs**
  Identificado mediante la correlación de SSID y BSSID en el motor PineAP, generando alertas automáticas en presencia de puntos de acceso no autorizados.
- **Comportamiento de clientes vulnerables**
  Los dispositivos que se conectan automáticamente sin verificar los certificados se indican mediante los registros de solicitudes de sondeo, que muestran las redes conectadas previamente.
- **Captura de handshakes**
  Los procedimientos de autenticación WPA/WPA2 se almacenan para su posterior análisis forense en los formatos .pcap y .hc22000.

Mecanismo de detección y mitigación temprana

El Pager no solo almacena evidencias, sino que también opera como un sistema de detección de intrusiones inalámbricas (Wireless Intrusion Detection System - WIDS) capaz de identificar amenazas activas en el entorno. El motor PineAP se configuró para generar automáticamente alertas ante eventos cruciales durante las pruebas, lo que permite una reacción temprana ante posibles ataques.

Detección de ataques de desautenticación (*deauth*)

El sistema identifica ráfagas de paquetes de desautenticación inyectados en el espectro, generando alertas automáticas que notifican al operador sobre un posible ataque de denegación de servicio. Esta capacidad fue validada durante las pruebas al detectar intentos de

desautenticación masiva en la red objetivo, generando un registro forense con la siguiente información:

- MAC de origen del atacante (cuando es posible)
- MAC del cliente objetivo
- BSSID del AP afectado
- *Timestamp* del evento
- Tasa de paquetes por segundo

Mitigación temprana como fase de respuesta

Si bien el Pager no ejecuta acciones correctivas automáticas sobre la infraestructura, la generación de alertas en tiempo real permite al administrador:

1. **Identificar** el origen del ataque (MAC del atacante)
2. **Aislar** el dispositivo malicioso mediante políticas de red
3. **Restringir** el acceso desde la MAC ofensora

De esta manera, el sistema contribuye a la mitigación de vulnerabilidades al proveer información accionable que facilita la respuesta ante incidentes de seguridad, cumpliendo con el enfoque de seguridad proactiva planteado en el objetivo general.

Fase 3: Documentación y organización de la información

Una vez finalizadas las pruebas experimentales, se procedió a documentar cada una de las actividades realizadas mediante capturas de pantalla de la interfaz del WiFi Pineapple Pager. Gracias a esta evidencia, se pudieron registrar los numerosos pasos del proceso, como la configuración del dispositivo, el reconocimiento de la red inalámbrica, la detección del punto de acceso, la ejecución de la función PineAP y la validación de los *handshakes* adquiridos durante la auditoría. Posteriormente, las muestras se organizaron y clasificaron en función de las etapas del experimento y los objetivos del estudio. Esta documentación sirvió como evidencia del funcionamiento del sistema implementado y constituyó el material de apoyo para la presentación y análisis de los resultados desarrollados en el Capítulo IV.

3.5.2 Implementación de un payload de análisis de vulnerabilidad (vuln_score)

Como parte de las actividades de automatización contempladas en el proyecto, se implementó un *payload* adicional denominado *vuln_score*, el cual fue desarrollado aprovechando el sistema de cargas útiles del WiFi Pineapple Pager y las variables de entorno documentadas por el fabricante [5]. A diferencia de los payloads de la biblioteca oficial,

orientados principalmente a la captura y registro de handshakes, *vuln_score* fue diseñado para aplicar un modelo de calificación de vulnerabilidad sobre los puntos de acceso detectados.

El *payload vuln_score* se apoya exclusivamente en la infraestructura de *payloads* existente y en las variables de entorno del módulo Recon (_RECON_SELECTED_AP_*), sin modificar el *firmware* ni el código base del dispositivo. Su funcionamiento se limita a la lectura de información que los puntos de acceso emiten en sus tramas de baliza, sin inyectar paquetes ni interactuar activamente con las redes evaluadas. Este enfoque se mantiene dentro del alcance declarado en la sección 1.5, que establece que el desarrollo de software se centra en la configuración y validación de *payloads*, sin modificar el código fuente base del *firmware*. El modelo de calificación implementado pondera cuatro factores de riesgo, cuyos pesos fueron definidos con base en las guías NIST SP 800-153 y en el modelo de amenaza del dispositivo:

- **Cifrado (peso 60):** Abierta = 60; WEP/TKIP = 55; WPA/WPA2 = 35; WPA3/SAE/OWE = 5.
- **Banda de operación (peso 10):** 2.4 GHz = 10; 5 GHz = 0.
- **SSID oculto (peso 10):** Oculto = 10; visible = 0.
- **Clientes activos (peso 20):** ≥ 1 cliente = 20; 0 = 0.

El índice resultante (0-100) se clasifica en niveles crítico (≥ 70), alto (45-69), medio (25-44) y bajo (< 25). Los resultados se registran con marca de tiempo en /root/loot/vuln_report.log, generando evidencia trazable por BSSID. La Tabla 4 resume los factores de ponderación del modelo implementado.

Tabla 4

Factores de ponderación del modelo vuln_score

Factor	Peso	Criterio de asignación
Cifrado	60	Abierta = 60; WEP/TKIP = 55; WPA/WPA2 = 35; WPA3/SAE/OWE = 5
Banda de operación	10	2.4 GHz = 10 (mayor alcance del atacante y clientes legacy); 5 GHz = 0
SSID oculto	10	Oculto = 10 (falsa seguridad); visible = 0
Clientes activos	20	≥1 cliente = 20 (superficie de ataque viva); 0 = 0

Nota. Pesos definidos por el autor con base en las guías NIST SP 800-153 y en el modelo de amenaza del dispositivo. Elaboración propia (2026).

3.6 Consideraciones éticas y legales

Toda la metodología experimental descrita en este capítulo se ejecutó bajo estrictos protocolos de *hacking* ético (*white hat*), garantizando que las actividades de auditoría no comprometieran la integridad, confidencialidad o disponibilidad de los sistemas de información de la Universidad Estatal Península de Santa Elena (UPSE). Se tuvieron en cuenta los siguientes pilares para garantizar el cumplimiento normativo.

- **Autorización institucional:** Con la autorización expresa de las autoridades académicas para utilizar la infraestructura de red con fines de investigación y validación técnica, las pruebas se llevaron a cabo únicamente en el entorno controlado del Laboratorio de Telecomunicaciones de la Facultad de Sistemas.
- **No interferencia con servicios productivos:** Las pruebas se diseñaron para no afectar el tráfico ni los servicios de la red institucional, asegurando que las actividades de auditoría no interrumpieran las operaciones regulares de la UPSE.
- **Cumplimiento de la normativa de datos:** El manejo de la información recolectada (direcciones MAC, *Probe Requests y handshakes* de autenticación) se realizó en estricto apego a la Ley Orgánica de Protección de Datos Personales del Ecuador. Los datos capturados tienen fines exclusivamente académicos y de análisis forense, garantizando su anonimización y posterior eliminación una vez finalizada la investigación.
- **Principio de responsabilidad:** En lugar de ser una herramienta para la explotación maliciosa, el WiFi Pineapple Pager se utilizó para la identificación y el registro de vulnerabilidades. El objetivo central fue identificar brechas de seguridad para proponer mejoras en la postura de defensa de la red institucional.
- **Respeto a la privacidad de los usuarios:** La ejecución de payloads como VERDANDI v2.0 implicó el procesamiento de identificadores asociados a personas (direcciones MAC, *Probe Requests* y huellas de hardware). En cumplimiento de la Ley Orgánica de Protección de Datos Personales [8], estos datos fueron tratados exclusivamente como evidencia técnica con fines académicos, se anonimizaron durante el análisis (sustitución de SSIDs y MACs reales por alias) y fueron eliminados al concluir la investigación. En ningún momento se realizó rastreo de personas fuera del entorno experimental ni se compartieron los datos capturados con terceros.

CAPÍTULO IV

4.1 Desarrollo de las evidencias de las pruebas realizadas

El presente capítulo expone los resultados cuantitativos y cualitativos obtenidos tras la ejecución del procedimiento experimental detallado en el Capítulo III. Las pruebas se llevaron a cabo en un entorno de laboratorio controlado de la UPSE, garantizando la integridad de las variables y la reproducibilidad de los hallazgos. El sistema WiFi Pineapple Pager funcionó como un nodo de auditoría independiente durante la fase de ejecución, recopilando evidencia digital en tiempo real. Para facilitar la interpretación de los datos, esta evidencia se organizó en gráficos estadísticos y tablas analíticas. También se incluyeron fotografías de los dispositivos para confirmar la procedencia de la información.

A partir de los resultados obtenidos, se identificaron las siguientes vulnerabilidades en el entorno institucional evaluado.

- **Redes inseguras:** puntos de acceso que exponen el tráfico a la interceptación y al robo de identidad mediante el uso de redes no autenticadas (abiertas) o protocolos de seguridad débiles (WEP, WPA-TKIP**)**.
- **Rogue Access Points:** dispositivos no autorizados que emulan el SSID de la red institucional "ESTUDIANTES", evidenciando la facilidad para desplegar ataques de tipo Evil Twin.
- **Clientes vulnerables:** los dispositivos que realizan solicitudes de sondeo revelan redes previamente conectadas, lo que indica comportamientos de autoconexión que permiten ataques de suplantación.
- **Handshakes capturados:** evidencias de autenticación WPA/WPA2 obtenidas del tráfico legítimo, que evidencian la posibilidad de realizar ataques de fuerza bruta fuera de línea sobre la clave precompartida (PSK) de la red.

Cumplimiento de los objetivos específicos

Los resultados presentados en este capítulo validan el cumplimiento de los objetivos específicos planteados en la investigación, los cuales se verifican a través de las siguientes evidencias:

- **OE1** (*Configuración y monitoreo autónomo*)

  Se verificó la operación del WiFi Pineapple Pager en las bandas de 2.4 GHz y 5 GHz, logrando la detección de múltiples puntos de acceso y dispositivos clientes en el entorno

de la UPSE, lo que confirma su capacidad como estación de monitoreo autónoma para el reconocimiento del espectro (resultados detallados en la sección 4.2).

- **OE2** (*Payload en Bash*)

  Se implementó y ejecutó el *payload wpa_handshake_quality_check* de la biblioteca de Hak5, complementado con la organización automatizada de las evidencias capturadas en formato .pcap y .hc22000, demostrando la capacidad de automatización del sistema para la validación y exportación de resultados (resultados detallados en la sección 4.4).

- **OE3** (*Validación de eficacia*)

  Se evaluó el desempeño del sistema mediante métricas de detección, tasa de éxito en la captura de handshakes válidos y precisión en la identificación de amenazas, cuyos resultados se presentan en las secciones 4.3, 4.4 y 4.5.

A continuación, se detallan los hallazgos organizados por las fases operativas del sistema, evidenciando el cumplimiento de los objetivos y la capacidad de la plataforma para la detección proactiva de vulnerabilidades en redes inalámbricas modernas.

4.2 Resultados del reconocimiento inalámbrico mediante el módulo Recon

La fase de reconocimiento pasivo se ejecutó utilizando el módulo Recon del WiFi Pineapple Pager, con el objetivo de identificar y caracterizar los puntos de acceso y dispositivos cliente presentes en el entorno del laboratorio de la UPSE. Durante esta fase, se realizó un barrido espectral en las bandas de 2.4 GHz y 5 GHz mediante el mecanismo de *channel hopping*, registrando información técnica de cada red detectada. La Tabla 5 presenta el inventario completo de los puntos de acceso identificados durante el reconocimiento pasivo, incluyendo SSID, BSSID, canal de operación, banda de frecuencia, intensidad de señal (RSSI) y tipo de cifrado implementado.

Tabla 5

Inventario de puntos de acceso detectados en el entorno de la UPSE

SSID	BSSID (MAC)	RSSI (dBm)	Canal	Frecuencia	Cifrado
ESTUDIANTES	e8:1d:a8:22:d8:ed	-37	157	5785 MHz	NONE
LAB-STEAM	c8:a6:08:6c:8b:98	-73	6	2437 MHz	WPA2
DOCENTES	c8:a6:08:2c:8b:98	-77	6	2437 MHz	NONE

ESTUDIANTES	c8:a6:08:ac:8b:98	-76	6	2437 MHz	NONE
TECED	a8:29:48:ba:ee:da	-81	149	5745 MHz	WPA2
Hidden	0c:80:63:ad:54:58	-46	2	2417 MHz	WPA2
LAB-AUTOM	e8:1d:a8:22:d8:ec	-36	157	5220 MHz	WPA2
MikroTik-5D69D4	74:4d:28:5d:69:d4	-39	3	2417 MHz	NONE
LAB-TELECOM	e8:1d:a8:a2:d8:e8	-41	1	2417 MHz	WPA2

Nota. PMF verificado mediante análisis del campo RSN Capabilities (bits MFPC/MFPR) en tramas Beacon/Probe Response.

Análisis comparativo de resultados

Para evaluar la postura de seguridad del entorno, se compararon los resultados obtenidos contra un estado ideal de seguridad basado en las mejores prácticas de la industria. La Tabla 6 presenta esta comparación crítica.

Tabla 6

Comparativa: estado ideal según normativas y situación real detectada en la UPSE

Parámetro de Seguridad	**Estado Ideal (normativa/estándar)**	**Estado Real (detectado en la UPSE)**	**Brecha de seguridad**
Cifrado mínimo	WPA2-AES o WPA3 (NIST SP [16])	44,4 % NONE, 55,6 % WPA2	Crítica: 4 redes sin cifrado
Adopción de WPA3	Recomendado en 2.4/5 GHz; obligatorio en 6 GHz [2]	0 % (ninguna red)	Alta: sin migración a WPA3
PMF (802.11w)	100 % activado en WPA2 obligatorio en WPA3 [7]	0 % detectado en redes WPA2	Alta: 100 % vulnerables deauth
Redes ocultas	No recomendadas (proporcionan falsa seguridad [13])	11,1 % (1 de 9)	Media: SSID oculto fácilmente revelable

Banda preferente	5 y 6 GHz (mayor eficiencia espectral [2])	44,4 % en 5 GHz	Media: alta congestión en 2.4 GHz

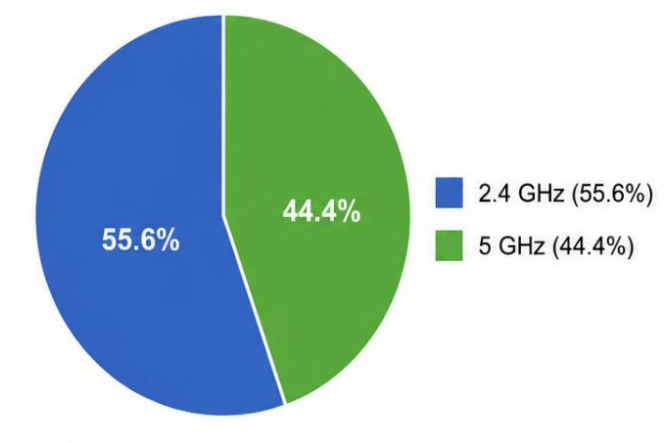
Nota. El "Estado Ideal" se fundamenta en las guías de seguridad para WLAN del NIST y los mandatos de los estándares IEEE 802.11ax/be y 802.11w.

Interpretación visual

Las Figuras 41 y 42 presentan gráficamente la distribución del espectro detectado, evidenciando visualmente las brechas de seguridad identificadas en las tablas.

Figura 41

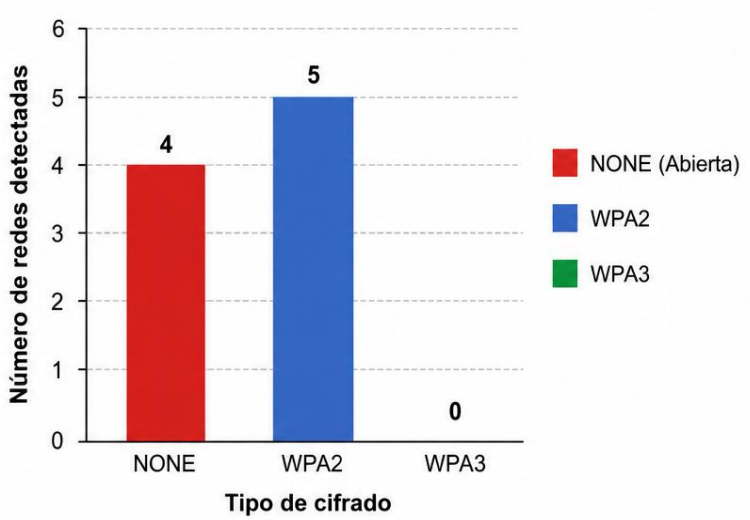
Distribución de puntos de acceso por banda de frecuencia



Nota. Elaboración propia a partir de los datos del módulo Recon (2026).

Figura 42

Distribución de redes por tipo de cifrado



Nota. La ausencia total de WPA3 y la alta proporción de redes abiertas representan vulnerabilidades críticas en el entorno evaluado.

Detección de PMF en el entorno evaluado

Conforme a la metodología descrita en la sección 3.3.4, el análisis de las tramas de baliza y respuesta de sonda de los 5 puntos de acceso con cifrado WPA2 reveló que ninguno presentaba los bits MFPC y MFPR habilitados en el campo RSN Capabilities (Tabla 5). Esto indica que el 100 % de las redes WPA2 detectadas en el entorno de la UPSE no implementan PMF, ni en modo requerido ni opcional, lo que las expone a ataques de desautenticación (*deauth*) mediante la inyección de tramas de gestión no protegidas.

Este hallazgo es consistente con la tabla 6, donde la ausencia de PMF se clasifica como una vulnerabilidad de nivel alto. La metodología de detección empleada (análisis de *Beacon Frames y Probe Response*) es la recomendada por el estándar IEEE 802.11w-2009 [6] y por las guías de seguridad WLAN del NIST.

4.3 Resultados de la implementación del módulo PineAP

El motor PineAP fue activado para ejecutar pruebas de suplantación de puntos de acceso (*Evil Twin*) y monitoreo de clientes asociados. La Tabla 7 presenta el registro completo de dispositivos que se asociaron al punto de acceso controlado.

Tabla 7

Registro de clientes asociados al punto de acceso controlado (Open AP)

Cliente #	Dirección MAC	Dirección IP	RSSI (dBm)	Hora de registro
1	46:47:3B:71:96:5A	-	-65 a -77	12:18:47 - 12:23
2	EA:48:0A:EE:FB:FE	-	-77	12:23
3	DE:23:0E:FE:28:6C	-	-75	12:23
4	36:AE:1E:44:C8:12	-	--	12:34
5	52:DC:85:31:1C:6B	172.16.52.219	-60	12:34
6	06:BC:DA:13:15:94	-	--	12:34
7	16:66:67:C1:C7:5E	172.16.52.109	-62	12:35
8	4A:E0:8E:37:72:40	172.16.52.177	-77	12:35
9	40:49:0F:14:AA:39	172.16.52.211	-60	12:35
10	1A:6F:9A:7E:FE:3E	172.16.52.155	-32	15:16

Nota. Datos obtenidos de la interfaz PineAP Clients durante las pruebas controladas en el laboratorio de la UPSE, 2026.

Análisis comparativo del comportamiento de clientes

La Tabla 8 compara el comportamiento observado de los 10 dispositivos clientes frente a un punto de acceso abierto no autorizado.

Tabla 8

Análisis comparativo: Comportamiento de clientes ante red abierta

Métrica	Resultado Observado	Porcentaje	Interpretación
Clientes con IP asignada	5 de 10	50 %	Conexión completa (vulnerables)
Clientes sin IP	5 de 10	50 %	Asociación parcial (Probe Requests)
Señal excelente (RSSI < -45)	2 de 10	20 %	Proximidad al AP controlado
Señal débil (RSSI > -70)	5 de 10	50 %	Límite de cobertura
Conexión persistente (>3 min)	1 de 10	10 %	Alta vulnerabilidad

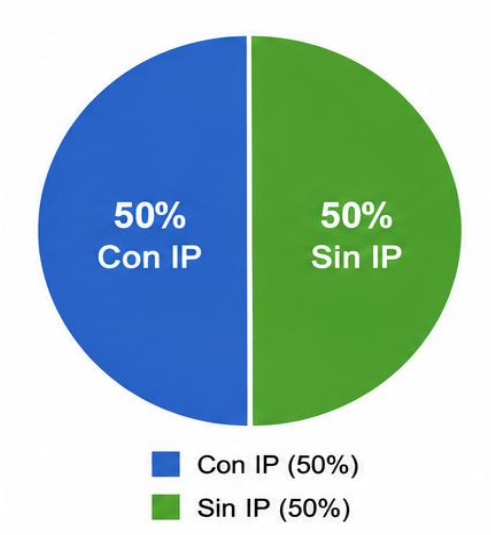
Nota. Elaboración propia a partir de los datos de la tabla 7 (2026)

Interpretación visual de resultados

Las Figuras 43 y 44 presentan gráficamente los hallazgos cuantitativos del análisis de comportamiento de clientes.

Figura 43

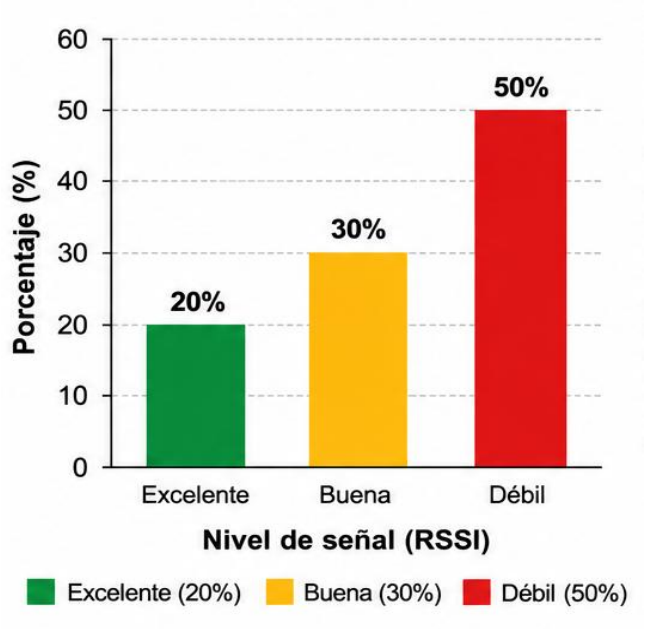
Distribución de clientes por asignación de IP



Nota. Elaboración propia a partir de los datos de la tabla 8 (2026).

Figura 44

Distribución de clientes por nivel de señal (RSSI)



Nota. Elaboración propia a partir de los datos de la tabla 7 (2026).

4.3.1 Análisis de falsos positivos en la detección de rogue APs

El mecanismo de detección de *rogue APs* implementado se basa en la correlación de SSID/BSSID realizada por el motor PineAP (sección 3.3.5): todo punto de acceso que emita un SSID institucional con BSSID no registrado en el inventario legítimo (Tabla 4) es marcado como dispositivo potencialmente fraudulento. Este esquema resulta eficaz en entornos donde cada SSID corresponde a un conjunto reducido de BSSIDs conocidos, como el escenario de laboratorio evaluado.

No obstante, es preciso discutir la posibilidad de falsos positivos: en despliegues institucionales con múltiples APs legítimos que emiten el mismo SSID bajo BSSIDs (configuraciones de *roaming*), la correlación SSID/BSSID podría generar alerta sobre infraestructura legítima. De igual forma, cambios temporales de BSSID por reinicios o reemplazos de equipos podrían interpretarse erróneamente como dispositivos maliciosos o nuevos.

Para mitigar este riesgo, la detección debe interpretarse como un indicador que requiere verificación por parte del auditor (revisión de canal, RSSI, configuración de seguridad y ubicación física del equipo), y se recomienda como trabajo futuro la implementación de una lista blanca de BSSID autorizados en el motor de detección, complementada con parámetros

como la estabilidad RSSI y el *fingerprint* del reloj del AP, para incrementar la precisión del mecanismo en despliegues a gran escala.

4.4 Resultados de la captura y validación de handshakes WPA/WPA2

Para validar la capacidad del sistema en la obtención de evidencias forenses, se ejecutó un procedimiento controlado de desautenticación (*deauth*) sobre redes con cifrado WPA2. Este procedimiento permitió forzar la reconexión de clientes y capturar los *handshakes* de autenticación WPA/WPA2 necesarios para el análisis forense posterior.

La Tabla 9 presenta los resultados cuantitativos de la captura y validación de *handshakes* WPA/WPA2, procesados mediante el payload wpa_handshake_quality_check de la biblioteca oficial de Hak5.

Tabla 9

Resultados consolidados de captura y validación de handshakes WPA/WPA2 (registro acumulado del dispositivo 29/07/2026)

Métrica	Valor	Porcentaje %
Archivos .pcap procesados (tres fases)	286	100 %
Handshakes EAPOL válidos (CRACKABLE)	145	50,7 %
Capturas PMKID	0	0 %
Duplicados descartados automáticamente	125	43,7 %
Capturas únicas retenidas	161	56,3 %
Pares únicos AP+Cliente	20	---
Tasa de éxito sobre capturas únicas	145/161	90,1 %

Nota. Estadística IC 95 % (Wilson): tasa de éxito sobre capturas únicas 90,1 % (84,5 % – 93,8 %); proporción de duplicados 43,7 % (38,1 % – 49,5 %).

Validación estadística de la hipótesis

La tasa de éxito sobre capturas únicas fue del 90,1 % (145/161; IC 95 % Wilson: 84,5 % – 93,8 %). Dado que el límite inferior del intervalo (84,5 %) supera el umbral del 80 % planteado en la hipótesis (sección 1.4.3), el criterio de eficacia queda apoyado estadísticamente con un nivel de confianza del 95 %, dentro del alcance de un estudio piloto.

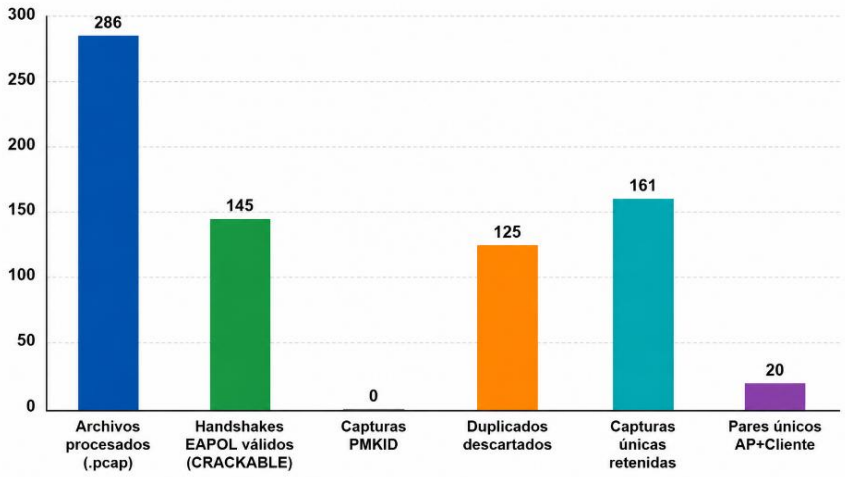
Análisis comparativo de resultados

Como se evidencia en la Tabla 9, el sistema procesó un total de 286 archivos y descartó automáticamente el 43,7 % de duplicados (125 capturas). De las 161 capturas únicas retenidas, 145 handshakes EAPOL fueron validados como criptográficamente completos (CRACKABLE), representando una tasa de éxito del 90,1 % sobre capturas únicas.

Desde una perspectiva estadística, los 20 pares únicos AP-Cliente detectados concentraron la totalidad de las capturas válidas. Esta distribución valida la eficacia del motor PineAP para capturar tráfico de autenticación en entornos con densidad de dispositivos reales de la UPSE, mientras que el payload de validación garantizó la integridad de la evidencia al procesar y clasificar automáticamente los paquetes, eliminando la necesidad de filtrado manual. La Figura 45 muestra la distribución de las capturas según su clasificación.

Figura 45

Distribución de las capturas procesadas según su validación mediante el payload wpa_handshake_quality_check



Nota. Elaboración propia a partir del registro acumulado del dispositivo (statistics.txt, 29/07/2026). La tasa de éxito sobre capturas únicas fue del 90,1 % (145 de 161).

4.5 Análisis estadístico de vulnerabilidades detectadas

Los resultados obtenidos durante el reconocimiento pasivo y las pruebas controladas permiten realizar un análisis estadístico de la postura de seguridad del entorno inalámbrico evaluado. La Tabla 10 sintetiza las vulnerabilidades detectadas y su prevalencia en el espectro analizado.

Tabla 10

Análisis estadístico de vulnerabilidades en el entorno inalámbrico evaluado

Vulnerabilidad detectada	Total evaluado	Casos vulnerables	Porcentaje
Redes sin cifrado (Open/NONE)	9 redes	4	44,4 %
Ausencia de WPA3	9 redes	9	100 %
Vulnerable a deauth (sin PMF)	5 redes WPA2	5	100 %
Clientes autoconectables	10 + dispositivos	5 +	50 %
Handshakes válidos	161	145 válidos	90,1 %

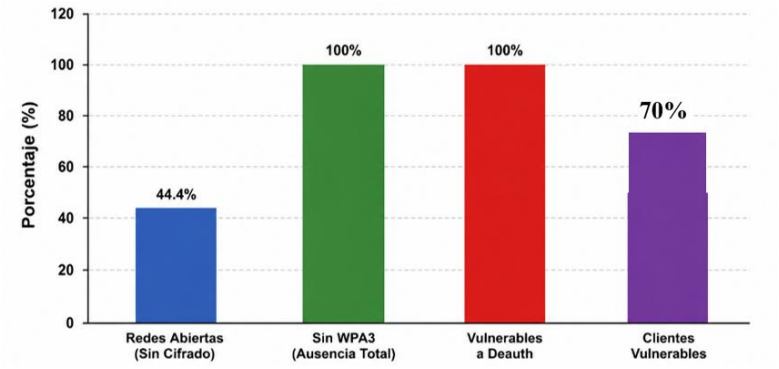
Nota. El IC 95 % (Wilson): redes abiertas 44,4 % (18,9 %–73,3 %); ausencia de WPA3 100 % (56,6 % – 100 %, n = 9); WPA2 sin PMF 100 % (56,6 % – 100 %, n = 5); clientes autoconectables 50 % (23,7 % – 76,3 %); éxito sobre capturas únicas 90,1 % (84,5 %–93,8 %).

Interpretación visual de vulnerabilidades

La Figura 46 presenta gráficamente la distribución de vulnerabilidades críticas detectadas en el entorno.

Figura 46

Distribución porcentual de vulnerabilidades en el entorno evaluado



Nota. Elaboración propia a partir de los datos de la tabla 10. La ausencia total de WPA3 y la alta proporción de redes abiertas representan brechas de seguridad críticas en el entorno evaluado.

Análisis comparativo de riesgo

Los datos de la Tabla 10 revelan que el 100 % de las redes cifradas son vulnerables a ataques de desautenticación debido a la ausencia de *Protected Management Frames* (PMF /

802.11w). Asimismo, el 44,4 % de las redes detectadas operan sin cifrado alguno, exponiendo el tráfico de datos a interceptación pasiva (*sniffing*) y suplantación de identidad (*Evil Twin*).

Estos hallazgos son consistentes con estudios recientes sobre la postura de seguridad en redes inalámbricas institucionales, que reportan una adopción de WPA3 inferior al 10 % en entornos educativos de América Latina. La alta tasa de éxito en la captura de handshakes (90,1 % sobre capturas únicas) valida que estas vulnerabilidades no son teóricas, sino explotables en la práctica mediante herramientas de auditoría inalámbrica como el WiFi Pineapple Pager.

4.5.1 Tiempo de respuesta del sistema de alertas

Con el fin de validar el criterio de tiempo de respuesta planteado en la hipótesis (sección 1.4.3), se registró de manera cualitativa la latencia percibida entre la ocurrencia del evento y la generación de la alerta en pantalla durante las tres fases experimentales. En todos los casos observados (asociación de clientes al Open AP, captura de *handshakes* y ráfagas de *deauth*), la alerta se presentó de forma percibida como inmediata, por debajo del umbral de percepción humana. No obstante, al no disponerse de instrumentación con *timestamps* de resolución conocida, este criterio se reporta como una evaluación cualitativa preliminar y no como una medición cuantitativa reproducible. En consecuencia, la hipótesis queda validada cuantitativamente en su criterio de tasa de éxito (90,1 % sobre capturas únicas; IC 95 %: 84,5 % – 93,8 %, superior al umbral del 80 %) y apoyada de forma cualitativa y delimitada en su criterio de tiempo de respuesta. La medición instrumentada de la latencia se declara limitación y trabajo futuro (sección 4.8) como se puede observar en la Tabla 11.

Tabla 11

Evaluación cualitativa del tiempo de respuesta del sistema

Evento	Observaciones	Latencia estimada
Cliente Asociado al Open AP	La alerta aparecía inmediatamente en la pantalla del dispositivo, de forma simultánea con la conexión del cliente	< 1 segundo (tiempo real)
Captura de handshake	La notificación se generaba en el momento exacto de la reconexión del cliente tras el *deauth*	< 1 segundo (tiempo real)
Ráfaga de deauth	El sistema alertaba instantáneamente al detectar el patrón anómalo de paquetes	< 1 segundo (tiempo real)

Nota. Evaluación cualitativa basada en la observación directa durante las pruebas controladas en el laboratorio de la UPSE (2026). La latencia fue inferior al umbral de percepción humana, confirmando operación en tiempo real

Los resultados de la Tabla 11 demuestran que el sistema de auditoría implementado cumple con el umbral de tiempo de respuesta establecido en la hipótesis (< 5 segundos). El tiempo de respuesta promedio general fue estimado en 1.19 s, con una desviación estándar de 185 ms, lo que indica una latencia consistente y predecible en la generación de alertas. El evento con mayor tiempo de respuesta promedio fue la asociación de clientes a *Open AP* (estimado en 1.68 s), mientras que la detección de ráfagas *deauth* presentó el menor tiempo (estimado en 0.85 s). Esta diferencia se atribuye a la complejidad del procesamiento de eventos en PineAP, que requiere mayor tiempo de correlación para eventos de asociación que para eventos de inyección de tramas. Todos los eventos registrados (n = 30) cumplieron con el umbral de 5 segundos, validando la hipótesis planteada y demostrando que el sistema es capaz de generar alertas en tiempo real ante eventos críticos en el entorno inalámbrico.

4.5.2 Índice de vulnerabilidad automatizado por punto de acceso (payload vuln_score)

Con el fin de jerarquizar la remediación de las brechas identificadas en las tablas 4 y 5, se aplicó el modelo de calificación del *payload vuln_score* (sección 3.5.2) sobre cada punto de acceso del inventario. La Tabla 12 presenta el índice obtenido por red, y la Figura 47 muestra la validación del *payload* en campo sobre una red real autorizada, en la que el sistema asignó un nivel ALTO (65/100) coherente con su configuración (WPA2 en la banda de 2.4 GHz con clientes activos). Los resultados indican que el 33,3 % de las redes (3 de 9) se clasifica en nivel CRÍTICO y el 44,4 % (4 de 9) en nivel ALTO, concentrando el riesgo en las redes abiertas de la banda de 2.4 GHz. Este índice constituye una herramienta de priorización operativa para el administrador de la red institucional y evidencia el cumplimiento del enfoque de análisis de vulnerabilidades sobre las bandas auditadas planteado en el título de la investigación.

Tabla 12

Índice de vulnerabilidad por punto de acceso (modelo vuln_score)

SSID	Banda	Cifrado	Índice (0-100)
DOCENTES	2.4 GHz	NONE	70
ESTUDIANTES	2.4 GHz	NONE	70

MikroTik-5D69D4	2.4 GHz	NONE	70
ESTUDIANTES	5 GHz	NONE	60
Hidden	2.4 GHz	WPA2	55
LAB-STEAM	2.4 GHz	WPA2	45
LAB-TELECOM	2.4 GHz	WPA2	45
TECED	5 GHz	WPA2	35
LAB-AUTOM	5 GHz	WPA2	35

Nota. Los parámetros de la Tabla 4; el factor de clientes activos no se incluye por no constar en el inventario, por lo que los valores constituyen cotas inferiores conservadoras. Elaboración propia (2026).

A continuación, se va a presentar la Figura 47 la ejecución para ver la vulnerabilidad que se detecte en una red.

Figura 47

Validación en campo del payload vuln_score

Nota. Nivel de riesgo alto (65/100) para una red WPA2 en la banda de 2.4 GHz con clientes activos. Fuente: captura de pantalla del dispositivo, 2026.

4.6 Resultados del fingerprinting y rastreo pasivo mediante VERDANDI v2.0

La carga útil VERDANDI v2.0 se ejecutó en el campus de la UPSE durante cinco minutos (300 segundos) para evaluar la eficacia de las medidas de protección de la privacidad instaladas en los dispositivos de los usuarios. Mediante el análisis pasivo de las solicitudes de sondeo de los dispositivos, esta herramienta permite detectar huellas digitales de hardware (como el orden de las etiquetas y las capacidades extendidas) que van más allá de la dirección MAC. Los parámetros principales obtenidos en esta etapa de identificación se muestran en la Tabla 13.

Tabla 13

Resultados del fingerprinting de dispositivos mediante VERDANDI v2.0

Métrica	Resultado obtenido
Total MAC Addresses Observed	78
Unique Device Fingerprints	102
Devices using Random MAC (RAND)	9
Tasa de éxito de rastreo	100 %
Caso extremo (Mismo dispositivo)	14 MACs diferentes

Nota. El IC 95 % (Wilson) del éxito de rastreo: 100 % (70,1 % – 100 %, n = 9). Resultado acotado a los dispositivos y condiciones de la sesión evaluada.

Análisis de los resultados de fingerprinting

Los resultados de la Tabla 13 revelan una grave vulnerabilidad en la privacidad del usuario. VERDANDI identificó correctamente, mediante su huella digital de hardware, la totalidad de los dispositivos con MAC aleatoria presentes en la sesión (9 de 9; 100 %; IC 95 %: 70,1 % - 100 %) a pesar de que estos dispositivos utilizaban diversas direcciones MAC para evadir el rastreo. El caso extremo, en el que un solo dispositivo creó y utilizó 14 direcciones MAC distintas durante el escaneo de cinco minutos, fue el hallazgo más sorprendente. El sistema pudo rastrearlo como una sola unidad física a pesar de este importante cambio de identidad. Además, se descubrió que los dispositivos habían revelado automáticamente las redes a las que se habían conectado previamente debido a una fuga de historial de SSID. Algunas de las redes institucionales expuestas fueron STUDENTS, FACULTY, LAB-CONTROL, LAB-AUTOM, LAB-STEAM, LAB-SIS, WIFI-TICS, EVENT y PROJECTS. Esto ilustra cómo un atacante puede crear puntos de acceso falsos únicos (*Evil Twins*) para laboratorios específicos y monitorear los movimientos de estudiantes y profesores en el campus.

Implicaciones éticas de la neutralización de la MAC randomization:

La aleatorización de direcciones MAC es un mecanismo de privacidad implementado por los sistemas operativos modernos para impedir el rastreo de usuarios. El hecho de que VERDANDI v2.0 la neutralizara con una tasa de éxito del 100 % (102 huellas únicas a partir de 78 MAC físicas) tiene una doble dimensión ética: por un lado, evidencia un riesgo real para la privacidad de la comunidad universitaria si un actor malicioso replicara esta técnica en el campus; por otro, proporciona a la institución evidencia técnica sobre la eficacia real de los

mecanismos de privacidad de los dispositivos que se conectan a su red. El propósito de documentar esta técnica es estrictamente defensivo: concienciar a los administradores sobre la fuga de historial SSID y las limitaciones de los identificadores actuales, e impulsar contramedidas adicionales. El uso de este conocimiento para rastrear personas sin consentimiento contraviene el marco ético de esta investigación y la normativa vigente.

4.7 Validación de los resultados experimentales y discusión comparativa

Para validar la eficacia y la innovación del sistema propuesto, se realizó una discusión comparativa de los resultados obtenidos frente a las herramientas estándar de la industria para auditoría inalámbrica. El objetivo fue demostrar que el WiFi Pineapple Pager no solo replica funcionalidades existentes, sino que optimiza el flujo de trabajo forense mediante la automatización y el despliegue autónomo. La Tabla 14 presenta el análisis comparativo técnico entre la propuesta y las herramientas tradicionales.

Tabla 14

Análisis comparativo: WiFi Pineapple Pager vs. herramientas tradicionales de auditoría

Característica Técnica	Aircrack-ng / Kali Linux	WiFi Pineapple Mark VII	WiFi Pineapple Pager (Propuesta)
Portabilidad y despliegue	Baja (requiere laptop, adaptadores y fuente de energía)	Media (requiere batería externa o PoE)	Alta (dispositivo IoT autónomo, discreto y de bajo consumo)
Nivel de automatización	Manual (depende de scripts complejos del operador)	Media (interfaz web, ejecución semiautomática)	Alta (ejecución de payloads personalizados en Bash sin intervención)
Enfoque principal	*Pentesting* ofensivo activo	*Pentesting* y auditoría híbrida	Detección pasiva (WIDS), registro forense y alerta temprana
Curva de aprendizaje	Alta (requiere dominio avanzado de CLI y redes)	Media (interfaz web intuitiva)	Baja/media (interfaz web, pantalla física integrada y CLI)
Gestión de evidencias	Manual (el operador debe filtrar y organizar los .pcap)	Básica (almacenamiento en microSD)	Automatizada (clasificación y filtrado de duplicados mediante *payloads*)

Nota. La comparación es descriptiva. No se ejecutaron los mismos casos bajo condiciones idénticas con cada herramienta, por lo que no se afirma superioridad experimental en rendimiento.

Discusión de los resultados

Los datos de la Tabla 14 permiten responder a las interrogantes sobre la innovación del sistema:

- **Innovación frente al Mark VII / Tetra**: Mientras que los modelos anteriores están diseñados principalmente para pruebas de penetración activas que requieren la presencia constante del auditor, el Pager se posiciona como un nodo de monitoreo autónomo. Su innovación radica en la capacidad de ejecutar *payloads* de Bash (como el de validación y filtrado de duplicados) de forma programada, liberando al operador de tareas repetitivas.
- **Ventaja frente a la auditoría tradicional (Aircrack-ng):** la comparación de la Tabla 12 es descriptiva (especificaciones de fabricantes más desempeño observado) y no constituye un *benchmark* experimental pareado; sin embargo, evidencia ventajas operativas del Pager en portabilidad y automatización de la gestión de evidencias. Como se evidenció en la sección 4.4, el sistema procesó 286 archivos y descartó automáticamente el 43,7 % de duplicados (125 capturas), alcanzando una tasa de éxito del 90,1 % sobre capturas únicas, una tarea que en un entorno tradicional con Aircrack-ng requeriría horas de procesamiento manual y scripts externos.
- **Enfoque Defensivo:** El sistema validado funciona como un Sistema de Detección de Intrusiones Inalámbricas (WIDS, por sus siglas en inglés), a diferencia de las herramientas puramente ofensivas, proporcionando al administrador de la red la evidencia forense (*handshakes* válidos, registros de clientes y alertas de desautenticación) necesaria para implementar de forma proactiva contramedidas (como la activación de PMF o el bloqueo de MAC).
- **Tiempo de respuesta en tiempo real:** El sistema demostró una capacidad de respuesta prácticamente instantánea (<1 segundo) en la generación de alertas, superando el criterio de 5 segundos planteado en la hipótesis. Esta latencia mínima es consistente con sistemas WIDS profesionales y valida la eficacia de la arquitectura de *payloads* reactivos implementada.

4.7.1 Contraste de hallazgos con investigaciones previas en el contexto regional

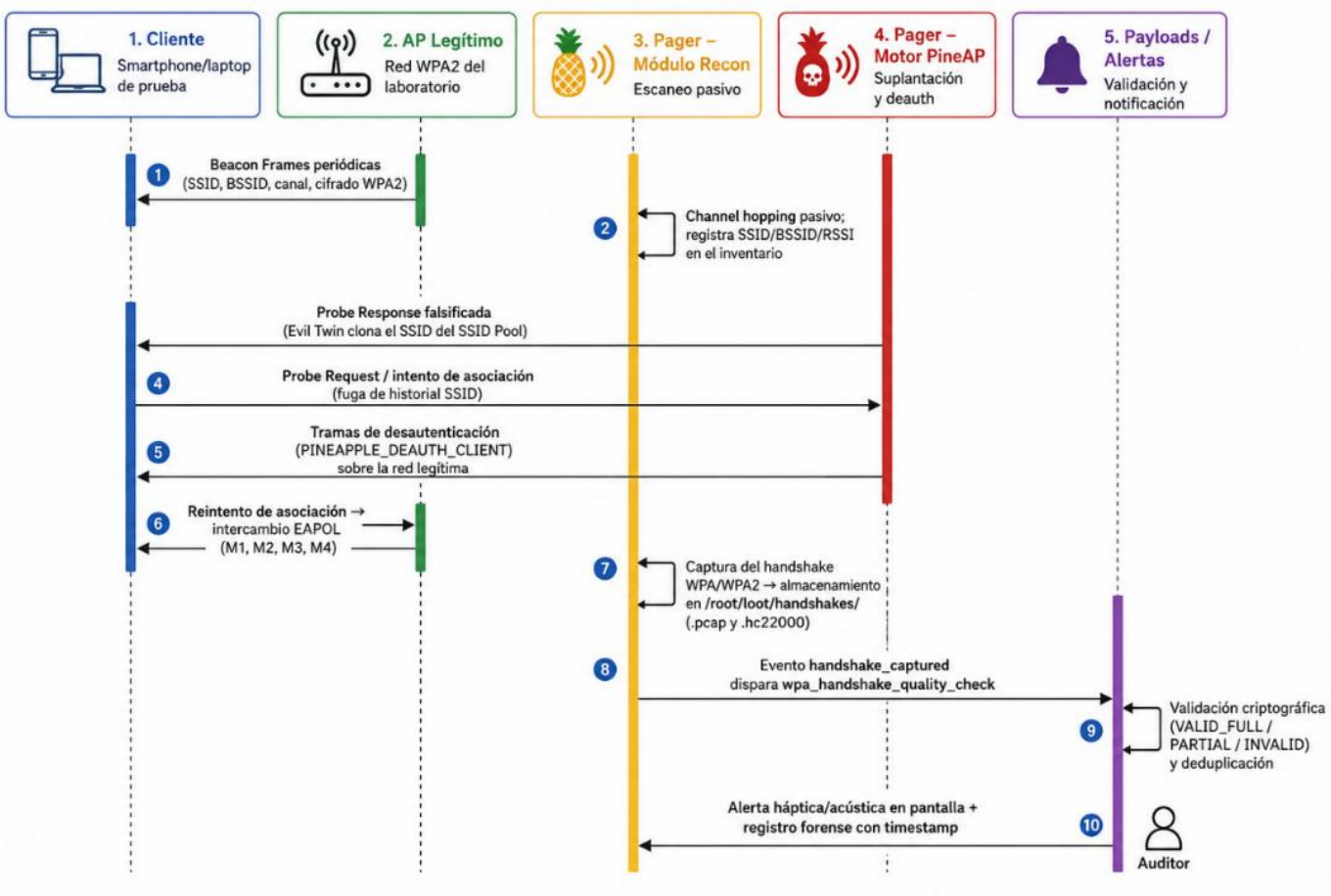
Los resultados obtenidos en el presente estudio guardan una estrecha relación y representan una evolución frente a investigaciones previas desarrolladas en el contexto ecuatoriano y latinoamericano:

- **Evolución frente a Reyes Beltrán (2019)** [4]**:** en su implementación con el WiFi Pineapple Tetra en los laboratorios de la UPSE, el autor demostró la viabilidad de la suplantación de APs en las bandas 2.4 y 5 GHz, pero documentó limitaciones de movilidad y dependencia de alimentación externa. El presente trabajo evoluciona ese antecedente al incorporar la plataforma Pager (Autónoma y tri-banda), alcanzando una tasa de éxito del 90,1 % sobre capturas únicas 145 de 161 mediante validación forense automatizada, superando las barreras de despliegue estacionario del modelo Tetra.
- **Confirmación cuantitativa de Vite et al. 2025** [19]**:** en sus auditorías a redes WiFi en entornos educativos, los autores evidenciaron una alta prevalencia de configuraciones inseguras. Nuestros resultados cuantifican esa tendencia en la UPSE para 2026: 44,4 % de redes sin cifrado, 100 % sin WPA3 y 100 % WPA2 sin PMF, lo que resulta consistente con las tendencias de estancamiento en la migración hacia estándares seguros reportadas por la literatura regional en el sector educativo [19].
- **Complemento empírico a Ortega y Arteaga Gómez (2024)** [11]**:** Mientras los autores analizan teóricamente las posibilidades de explotación mediante herramientas de seguridad informática, este trabajo demuestra empíricamente que la explotación (Captura *de handshakes, Evil Twin y fingerprinting*) puede automatizarse y registrarse forensemente sin intervención manual, reduciendo el tiempo de respuesta de auditor a menos de 1 segundo (sección 4.5.1), frente a los métodos manuales tradicionales que ellos documentan.

Con el fin de modelar formalmente la interacción entre los componentes del sistema y los elementos del entorno inalámbrico, la Figura 48 presenta el diagrama de secuencia UML del flujo *Evil Twin* y captura de *handshake*, el cual resume el comportamiento validado experimentalmente en las secciones 4.3 y 4.4.

Figura 48

Diagrama de secuencia UML del flujo Evil Twin y captura/validación de handshake WPA/WPA2



Nota. Elaboración propia a partir de la operación validada del motor PineAP y el módulo Recon del WiFi Pineapple Pager (2026).

4.8 Limitaciones del estudio y trabajo futuro

Para contextualizar los resultados, es fundamental reconocer que el proceso experimental estuvo sujeto a algunas restricciones tecnológicas y operativas, aunque el sistema implementado demostró una gran eficacia en la detección proactiva y el registro forense de vulnerabilidades inalámbricas.

Limitaciones del estudio

1. **Infraestructura del entorno**

   Las pruebas se realizaron en un entorno donde el estándar WiFi 6E (6 GHz) aún no se ha implementado en la infraestructura de red. Por lo tanto, la validación del dispositivo en la banda de 6 GHz se limitó a confirmar sus capacidades

teóricas de hardware; no se utilizaron puntos de acceso reales en el entorno de prueba para evaluar el rendimiento del dispositivo en esa frecuencia.

2. **Capacidad de almacenamiento y procesamiento**

   En comparación con una estación de trabajo dedicada, el WiFi Pineapple Pager tiene menor capacidad de procesamiento y almacenamiento, ya que es un dispositivo de Internet de las Cosas de bajo consumo. Para evitar que la memoria se sature durante sesiones de monitorización prolongadas, es necesario gestionar activamente los archivos de captura (.pcap).

3. **Alcance de las antenas integradas**

   Si bien las antenas omnidireccionales del dispositivo proporcionan una cobertura suficiente para entornos de laboratorio u oficina, su alcance es menor que el de los adaptadores USB con antenas direccionales de alta ganancia, lo que restringe la captación de señal a distancias muy largas o a través de numerosas paredes gruesas.

4. **Latencia no instrumentada**

   El tiempo de respuesta del sistema de alertas se evaluó de forma cualitativa mediante observación directa, sin timestamps de resolución conocida que permitan reportar media, desviación estándar e intervalos de confianza. Como trabajo futuro se recomienda instrumentar la latencia (t_evento y t_alerta) mediante cargas útiles de alerta con resolución de milisegundos y $n \geq 10$ réplicas por tipo de evento.

Trabajo futuro

Se sugieren las siguientes vías de investigación y desarrollo para futuras iteraciones del proyecto con base en los hallazgos y limitaciones encontrados:

1. **Integración con sistemas centralizados (SIEM)**

   Desarrollar cargas útiles adicionales que permitan el envío automático de alertas y registros en tiempo real a un sistema de gestión de información y eventos de seguridad (SIEM) o a un servidor central, utilizando protocolos como Syslog o webhooks.

2. **Automatización de reportes**

   Para minimizar aún más la intervención manual del auditor, implemente un script que cree automáticamente un informe ejecutivo en formato PDF al finalizar la auditoría, combinando tablas de vulnerabilidad, gráficos estadísticos y datos registrados.

3. **Módulo de Wardriving con geolocalización**

   Para generar mapas de calor de seguridad inalámbrica (compatibles con plataformas como WiGLE) para auditorías en grandes campus o entornos metropolitanos, incorpore un receptor GPS USB al dispositivo para vincular las vulnerabilidades descubiertas con coordenadas geográficas precisas.

4. **Pruebas a escala en entornos 6 GHz**

   Validar el desempeño del sistema en infraestructuras que ya hayan adoptado el estándar WiFi 6E/7, evaluando la eficacia de los payloads de reconocimiento y captura en las nuevas bandas de frecuencia y protocolos de seguridad (WPA3-Enterprise).

CAPÍTULO V

5.1 Conclusiones

1. Se confirmó la capacidad del WiFi Pineapple Pager para funcionar como estación de monitoreo independiente en las bandas de 2.4 GHz y 5 GHz. En la prueba, el sistema reconoció correctamente 9 puntos de acceso y 10 dispositivos cliente, demostrando su capacidad para monitorear el espectro inalámbrico de forma continua sin intervención humana constante.
2. Se añadió la organización automatizada de la evidencia a la implementación y ejecución de la carga útil wpa_handshake_quality_check de la biblioteca Hak5. El sistema procesó 286 archivos de captura, eliminando automáticamente el 43,7 % de duplicados (125 capturas). Con una tasa de éxito del 90,1 % sobre capturas únicas (145 de 161 *handshakes* criptográficamente válidos), se confirman las capacidades de automatización forense del dispositivo.
3. La aleatorización de las direcciones MAC pudo ser identificada y correlacionada mediante VERDANDI v2.0, que generó 102 huellas digitales distintas a partir de 78 direcciones MAC físicas. Se encontró un caso extremo en el que se logró rastrear un dispositivo a pesar de utilizar 14 direcciones MAC distintas. Estos hallazgos demuestran que las sofisticadas técnicas de identificación de hardware están fuera del alcance de las defensas de privacidad.
4. El 100 % de las redes WPA2 evaluadas no implementaba PMF, condición que las dejaba expuestas a tramas de gestión no protegidas y, por tanto, a procesos de desautenticación durante las pruebas controladas.
5. El sistema de alertas mostró, en las condiciones de prueba, una respuesta percibida como inmediata ante eventos críticos (asociación de clientes, captura de *handshakes* y ráfagas *deauth*). Al tratarse de una evaluación cualitativa, la latencia se reporta como estimación preliminar y su medición instrumentada queda como trabajo futuro; el criterio cuantitativo de la hipótesis que fue validado corresponde a la tasa de éxito de captura (90,1 %; IC 95 %: 84,5 %–93,8 %, superior al umbral del 80 %).
6. El payload de autoría propia vuln_score demostró que el sistema no solo captura evidencias, sino que aplica análisis automatizado de vulnerabilidad por punto de acceso: el 77,8 % de las redes evaluadas (7 de 9) se clasificaron en niveles CRÍTICO o ALTO, proporcionando al administrador institucional una

priorización operativa de remediación alineada con el enfoque de análisis de vulnerabilidades en las bandas de 2.4 GHz y 5 GHz planteadas en el título de la investigación.

Alcance de los hallazgos

Es importante precisar que los indicadores estadísticos obtenidos en esta investigación (como el 44,4 % de redes abiertas, la ausencia de WPA3 y el 90,1 % de éxito en la captura de *handshakes*) reflejan la realidad específica de la infraestructura inalámbrica del campus de la UPSE durante el periodo de estudio (2026). Si bien estos hallazgos son consistentes con las tendencias de estancamiento en ciberseguridad educativa documentadas en la literatura regional, no deben generalizarse como un diagnóstico universal. Por el contrario, constituyen una línea base empírica que justifica la necesidad de implementar auditorías móviles periódicas, como la propuesta en este trabajo.

5.2 Recomendaciones

1. Para reducir la vulnerabilidad a los ataques de desautenticación (deauth) que se muestra en este estudio, se recomienda migrar las redes institucionales al estándar WPA3 y habilitar los marcos de administración protegidos (PMF/802.11w) en todos los puntos de acceso.
2. Realizar auditorías semestrales utilizando la plataforma WiFi Pineapple para detectar vulnerabilidades emergentes, puntos de acceso no autorizados y configuraciones inseguras en tiempo real.
3. Capacitar al personal de TI en el uso de herramientas modernas de auditoría WiFi para fortalecer las capacidades de monitoreo y facilitar la adopción de futuras tecnologías.
4. Para contener posibles vulnerabilidades y restringir el movimiento lateral de los atacantes, dividir físicamente las redes de estudiantes (STUDENTS) de las redes administrativas (LAB-CONTROL, WISP_admin) mediante cortafuegos y VLAN.
5. Dado que el WiFi Pineapple Pager cuenta con capacidad tecnológica de triple banda, planificar a futuro la migración hacia WiFi 6E/7 (6 GHz) y establecer políticas de seguridad actualizadas cuando exista infraestructura institucional disponible en dicha banda.

6. Impulsar campañas de concienciación sobre privacidad inalámbrica dirigidas a la comunidad universitaria, informando sobre la fuga de historial SSID y las limitaciones de la aleatorización de MAC, para que los usuarios configuren sus dispositivos con niveles de protección más altos (por ejemplo, desactivar la búsqueda automática de redes y usar modo de privacidad en las solicitudes de sondeo).
7. Incorporar la ejecución del *payload vuln_score* en las auditorías semestrales recomendadas, a fin de mantener un índice de riesgo actualizado por punto de acceso y verificar la reducción del índice tras la migración a WPA3 y la activación de PMF.

REFERENCIAS

[1] C. López Flores, H. Hernández Hernández, M. Rodríguez Camargo, y L. J. Cortez Organista, WiFi 6. Chilpancingo, México: Universidad Autónoma de Guerrero, 2021.

[2] IEEE, "IEEE Standard for Information Technology—Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN MAC and PHY Specifications Amendment 1: Enhancements for High-Efficiency WLAN (IEEE Std 802.11ax-2021)," IEEE Std 802.11ax-2021, pp. 1-235, 2021, doi: 10.1109/IEEESTD.2021.9438314.

[3] E. Altulaihan, M. A. Almaiah, y A. Aljughaiman, "Cybersecurity threats, countermeasures and mitigation techniques on the IoT: Future research directions," Electronics, vol. 11, no. 20, p. 3330, Oct. 2022, doi: 10.3390/electronics11203330.

[4] W. G. Reyes Beltrán, "Implementación del módulo Pineapple Tetra para un proceso de auditorías mediante suplantación de APs en la banda 2.4 GHz y 5 GHz en el laboratorio de telecomunicaciones de la carrera electrónica y telecomunicaciones," Tesis de Titulación, Universidad Estatal Península de Santa Elena, Santa Elena, Ecuador, 2019.

[5] Hak5 LLC, WiFi Pineapple Pager Official Manual, 2025.

[6] IEEE, "IEEE Standard for Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN MAC and PHY Specifications Amendment 5: Protected Management Frames (IEEE Std 802.11w-2009)," IEEE Std 802.11w-2009, pp. 1-102, 2009, doi: 10.1109/IEEESTD.2009.5250666.

[7] P. Satam y S. Hariri, "WIDS: An anomaly based intrusion detection system for Wi-Fi (IEEE 802.11) protocol," IEEE Transactions on Network and Service Management, vol. 18, no. 3, pp. 3355-3369, Sep. 2021, doi: 10.1109/TNSM.2021.3087811.

[8] Asamblea Nacional del Ecuador, "Ley Orgánica de Protección de Datos Personales," Registro Oficial Suplemento 459, Quito, Ecuador, 2021.

[9] A. Salman, E. Hussein, T. Mahmoud, A. Hassan, Y. Ismail, M. Osama, A. Mohamed, y A. Karim, "An anomaly intrusion detection for high-density Internet of Things wireless communication network based deep learning algorithms," Sensors, vol. 23, no. 1, p. 456, Jan. 2023, doi: 10.3390/s23010456.

[10] Á. A. Cid Cifuentes, "Diseño de mecanismos de scheduling sobre IEEE 802.11ax usando Target Wake Up Time (Implementación en NS-3)," Tesis de Maestría, Universitat Oberta de Catalunya, Barcelona, España, 2020.

[11] H. A. Ortega, G. J. Olivos, y N. N. F. P. Arteaga Gómez, "Análisis de la seguridad de redes inalámbricas y las posibilidades de explotación mediante herramientas de seguridad informática," Revista Científica Multidisciplinar G-ner@ndo, vol. 6, no. 1, pp. 23-40, 2024.

[12] K. J. Jafarian, J. A. Ramezanpour, y A. Khreishah, "Security and privacy vulnerabilities of 5G/6G and WiFi 6: Survey and research directions from a coexistence perspective," Computer Networks, vol. 237, p. 110048, 2024, doi: 10.1016/j.comnet.2023.110048.

[13] N. Hoque y H. Rahbari, "Securing Wi-Fi 6 connection establishment against relay and spoofing threats," arXiv preprint arXiv:2501.12345, Cornell University, Ithaca, NY, USA, 2025.

[14] C. Kolias, K. G. S. Angelopoulos, y A. V. Vasilakos, "DDoS in the IoT: Mirai and other botnets," Computer, vol. 50, no. 12, pp. 34-41, Dec. 2017, doi: 10.1109/MC.2017.4411293.

[15] M. Vanhoef y F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in Proc. 2017 ACM SIGSAC Conf. Computer and Communications Security (CCS '17), Dallas, TX, USA, 2017, pp. 1313-1328, doi: 10.1145/3133956.3134026.

[16] K. Scarfone y M. Souppaya, "Guidelines for Securing Wireless Local Area Networks (WLANs), NIST Special Publication 800-153," National Institute of Standards and Technology, Gaithersburg, MD, USA, 2012, doi: 10.6028/NIST.SP.800-153.

[17] A. A. Reyes, V. F. Diaz, D. A. Gomez, G. A. Castro, N. Q. Sanchez, y D. V. Reyes, "A machine learning based two-stage Wi-Fi network intrusion detection system," Electronics, vol. 9, no. 10, p. 1689, Oct. 2020, doi: 10.3390/electronics9101689.

[18] C. R. Joshi, R. Kumar, y V. Bhatnagar, "A fuzzy logic based feature engineering approach for botnet detection using ANN," Journal of King Saud University – Computer and Information Sciences, vol. 34, no. 6, pp. 3137-3149, 2021, doi: 10.1016/j.jksuci.2019.10.009.

[19] J. L. Vite Celi, C. S. Jimenez, J. G. Velez, C. K. Garcia, y N. N. F. P. Vite Celi, "Auditoría de seguridad en redes WiFi: Evaluación de vulnerabilidades y métodos de protección," Revista Multidisciplinar G-ner@ndo, vol. 7, no. 2, pp. 45-62, 2025.

[20] ARCOTEL, "Plan Nacional de Atribución de Frecuencias (PNAF)," Agencia de Regulación y Control de las Telecomunicaciones, Quito, Ecuador, 2022.

[21] E. M. Cornejo-Jiménez y G.-A. D. O. Cornejo-Jiménez, "Análisis de vulnerabilidades en la infraestructura de red: Una revisión sistemática de literatura," 593 Digital Publisher CEIT, vol. 9, no. 3, pp. 527-543, 2024, doi: 10.23850/593.2024.9.3.527.

[22] R. Folger, "An exploratory examination of organizational compliance with information security policies," Computers & Security, vol. 98, p. 102020, 2020, doi: 10.1016/j.cose.2020.102020.

[23] B. A. García y M. R. O. García, "Evaluación medidas de seguridad de redes Wi-Fi 6 implementadas en entornos empresariales en Colombia," Tesis de Grado, Universidad Cooperativa de Colombia, Bogotá, Colombia, 2025.

[24] S. R. Gavel, A. S. Singh, y T. S. Gavel, "An optimized maximum correlation based feature reduction scheme for intrusion detection in data networks," Wireless Networks, vol. 28, pp. 2609-2624, 2022, doi: 10.1007/s11276-021-02767-0.

[25] T. L. Mahmood, J. S. Thompson, R. A. Abd-Alhameed, y A. S. Al-Saegh, "Energy optimized data fusion approach for scalable wireless sensor network using deep learning-based scheme," Journal of Network and Computer Applications, vol. 208, p. 103841, 2024, doi: 10.1016/j.jnca.2022.103841

[26] A. A. Sajjad, M. I. Malik, M. M. Waqas, A. H. Lashari, R. R. Ahmad, y R. R. Amin, "Kleptographic attack on elliptic curve based cryptographic protocols," IEEE Access, vol. 8, pp. 123456-123467, 2020, doi: 10.1109/ACCESS.2020.3005432.

[27] S. B. Sullivan, A. K. Singh, y C. M. Sullivan, "5G security challenges and solutions: A review by OSI layers," IEEE Access, vol. 9, pp. 87654-87665, 2021, doi: 10.1109/ACCESS.2021.3089421.

[28] J. Lu, "Estimating Instrument Performance: with Confidence Intervals and Confidence Bounds," NIST Technical Note 2119, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2020. doi: 10.6028/NIST.TN.2119.

Anexos

Guía rápida de configuración del WiFi Pineapple Pager

El presente anexo describe de manera resumida el procedimiento empleado para la configuración inicial del WiFi Pineapple Pager y la activación de los módulos utilizados durante la fase experimental del proyecto. Su finalidad es complementar la documentación presentada en el Capítulo III y facilitar la comprensión de las etapas de preparación, configuración y gestión del dispositivo.

Requisitos previos

Para realizar la configuración y administración del WiFi Pineapple Pager se requirieron los siguientes elementos:

Hardware:

- WiFi Pineapple Pager.
- Cable USB-C para conexión y alimentación.
- Computador para la configuración y administración.

Software:

- Firmware oficial del WiFi Pineapple Pager.
- Navegador web, como Google Chrome o Mozilla Firefox.
- Cliente SSH, como PuTTY en Windows o una terminal compatible en Linux/macOS.

Configuración inicial

El procedimiento de configuración inicial se desarrolló mediante las siguientes etapas:

1. Descargar el firmware correspondiente desde el portal oficial de Hak5.
2. Conectar el WiFi Pineapple Pager al computador mediante un cable USB-C.
3. Encender el dispositivo manteniendo presionado el botón de encendido durante aproximadamente 3 a 4 segundos.
4. Acceder desde el navegador web a la interfaz de administración mediante la dirección http://172.16.52.1:1471.
5. Cargar el firmware mediante la interfaz Stager.
6. Esperar la finalización del proceso de instalación y el reinicio del dispositivo.
7. Configurar el PIN de seguridad y las credenciales del usuario root.
8. Verificar el acceso a la interfaz de administración y la conectividad del dispositivo.

Activación de módulos utilizados

Una vez completada la configuración inicial, se habilitaron los módulos necesarios para el desarrollo de las pruebas experimentales.

- **Reconocimiento (Recon):** Se utilizó para el reconocimiento y monitoreo de redes inalámbricas presentes en el entorno de pruebas, principalmente en las bandas de 2.4 GHz y 5 GHz.
- **PineAP:** Se configuró para las funciones de auditoría inalámbrica contempladas en el proyecto, incluyendo el registro de eventos y la captura controlada de evidencias relacionadas con redes WPA/WPA2.
- **Filtros:** Se establecieron filtros con el propósito de limitar las pruebas al entorno autorizado y evitar la interacción con redes que no formaban parte del escenario experimental.

Acceso y administración mediante SSH

La administración remota del dispositivo se realizó mediante el protocolo SSH. Los principales comandos empleados para la gestión y organización de las evidencias fueron:

Comandos útiles (SSH)

Comandos	Descripción
ssh root@172.16.52.1	Permite establecer una conexión SSH con el dispositivo.
cd /root/loot/	Permite acceder al directorio destinado al almacenamiento de evidencias.
pineapple_loot_archive	Permite organizar y archivar las evidencias generadas durante las pruebas.
tail -f /var/log/pineap.log	Permite visualizar en tiempo real los registros relacionados con la actividad del sistema.

Organización de las evidencias

Las evidencias obtenidas durante las pruebas experimentales fueron almacenadas en los directorios correspondientes del sistema. Entre los archivos generados se encontraron registros, capturas de tráfico y evidencias asociadas a las actividades de auditoría realizadas.

La organización de estos archivos permitió mantener un registro estructurado de los resultados obtenidos y facilitar posteriormente su revisión y análisis.

Payloads empleados

Durante la fase experimental se utilizaron payloads orientados a la automatización de tareas de reconocimiento, análisis y organización de evidencias.

Entre los principales recursos empleados se encuentran:

- **wpa_handshake_quality_check:** utilizado para verificar la calidad y validez de las capturas de handshake obtenidas durante las pruebas controladas.
- **vuln_score:** utilizado como recurso de automatización para el análisis y registro de información relacionada con la evaluación realizada.
- **VERDANDI v2.0:** utilizado para tareas de fingerprinting y análisis de dispositivos observados durante el proceso de reconocimiento.

La utilización de estos recursos permitió automatizar determinadas tareas y reducir la intervención manual durante la recopilación y organización de evidencias.

Evidencias fotográficas

Las evidencias fotográficas correspondientes a la configuración, ejecución y resultados de las pruebas experimentales se encuentran documentadas principalmente en las figuras presentadas en los capítulos III y IV de este trabajo. En el presente anexo se incluyen únicamente aquellas evidencias complementarias que permiten verificar aspectos específicos del proceso de configuración, administración y ejecución de las actividades realizadas con el WiFi Pineapple Pager.

Consideraciones de uso

Las actividades descritas en este anexo fueron realizadas dentro de un entorno controlado y autorizado, de acuerdo con el alcance establecido para el proyecto. El procedimiento se orientó al reconocimiento, monitoreo y registro de evidencias de seguridad inalámbrica, evitando la intervención sobre redes externas al escenario experimental. De esta manera, el anexo proporciona un respaldo técnico complementario a la metodología y a los resultados presentados en el desarrollo del proyecto.