UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

MAYO 2022 – SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

ANÁLISIS DE LOS PROTOCOLOS WPA Y WPA2 EN DISPOSITIVOS MÓVILES: ASPECTOS DE AUTENTICACIÓN Y ENCRIPTACIÓN DE DATOS

ESTUDIANTE:

ALICIA ARELI SANTILLAN VERA

TUTOR: ING. IVAN RUIZ

AÑO 2023

INDICE

INDICE DE TABLAS

RESUMEN

Este caso de estudio se centró en el análisis de los protocolos de seguridad inalámbrica WPA y WPA2 en dispositivos móviles, con un enfoque en los aspectos de autenticación y encriptación de datos. Se utilizaron diversas técnicas, como pruebas de penetración, simulaciones de ataques, análisis de tráfico de red y encuestas a usuarios, para evaluar la efectividad de estos protocolos y revelar posibles vulnerabilidades. Los resultados destacaron la importancia de la elección de contraseñas seguras, la migración a WPA2 y la actualización de dispositivos móviles. Además, se identificaron áreas de mejora en la configuración de seguridad y la educación de los usuarios para fortalecer la seguridad de las redes inalámbricas.

PALABRAS CLAVES: WPA, WPA2, Seguridad inalámbrica, Autenticación, Encriptación, Dispositivos móviles, Vulnerabilidades, Pruebas de penetración, Análisis de tráfico, Contraseñas seguras, Actualización de software, Configuración de seguridad, Educación en seguridad

ABSTRACT

This case study focused on the analysis of the WPA and WPA2 wireless security protocols in mobile devices, with a focus on the authentication and data encryption aspects. Various techniques, such as penetration tests, attack simulations, network traffic analysis, and user surveys, were used to assess the effectiveness of these protocols and reveal potential vulnerabilities. The results highlighted the importance of choosing strong passwords, migrating to WPA2, and upgrading mobile devices. In addition, areas for improvement in security settings and user education were identified to strengthen the security of wireless networks.

KEYWORDS: WPA, WPA2, Wireless security, Authentication, Encryption, Mobile devices, Vulnerabilities, Penetration testing, Traffic analysis, Strong passwords, Software update, Security settings, Security education

PLANTEAMIENTO DEL PROBLEMA

En la actualidad, los dispositivos móviles se han vuelto indispensables en nuestra vida diaria, ya que nos brindan una amplia gama de servicios y aplicaciones. Sin embargo, su naturaleza inalámbrica y portátil los expone a riesgos de seguridad, como el acceso no autorizado a redes y la interceptación de datos transmitidos. Para abordar estos problemas, se han desarrollado protocolos de seguridad como WPA (Wi-Fi Protected Access) y WPA2, que proporcionan autenticación y encriptación de datos para proteger la privacidad y la integridad de la información en dispositivos móviles.

Aunque los protocolos WPA y WPA2 se consideran estándares de seguridad ampliamente aceptados, es fundamental analizar y comprender su efectividad en dispositivos móviles, específicamente en relación con los aspectos de autenticación y encriptación de datos. Es importante evaluar si estos protocolos brindan un nivel adecuado de seguridad y protección en entornos móviles y si existen vulnerabilidades o debilidades que puedan ser explotadas por posibles atacantes.

Por lo tanto, el planteamiento del problema es: ¿Cuál es la efectividad de los protocolos WPA y WPA2 en dispositivos móviles en términos de autenticación y encriptación de datos? ¿Existen posibles vulnerabilidades o debilidades en la implementación de estos protocolos en dispositivos móviles? ¿Qué recomendaciones se pueden formular para mejorar la seguridad en la autenticación y encriptación de datos en dispositivos móviles?

El análisis detallado de estos aspectos permitirá comprender mejor la seguridad de los dispositivos móviles y brindará pautas para fortalecer la protección de los datos en un entorno cada vez más conectado y propenso a amenazas. Esto ayudará a los usuarios de dispositivos móviles, así como a los desarrolladores y profesionales de seguridad de la información, a

tomar medidas adecuadas para proteger la privacidad y la integridad de los datos en dispositivos móviles.

JUSTIFICACIÓN

El estudio sobre el análisis de los protocolos WPA (Wi-Fi Protected Access) y WPA2 en dispositivos móviles, centrándose en los aspectos de autenticación y encriptación de datos, es de suma importancia en el contexto actual de la creciente adopción de dispositivos móviles y el uso generalizado de redes inalámbricas. La justificación para llevar a cabo este caso de estudio se basa en los siguientes puntos:

Protección de datos sensibles: Los dispositivos móviles almacenan y transmiten una gran cantidad de datos sensibles, como información personal, contraseñas, datos bancarios y empresariales. La seguridad de estos datos es de vital importancia para prevenir el acceso no autorizado y el robo de información confidencial. El análisis de los protocolos WPA y WPA2 permitirá evaluar si brindan un nivel adecuado de protección para salvaguardar los datos en dispositivos móviles.

Aumento de las amenazas de seguridad: Con el avance de la tecnología, las amenazas de seguridad también evolucionan. Los atacantes buscan constantemente formas de comprometer las redes inalámbricas y acceder a los datos transmitidos. El estudio de los protocolos WPA y WPA2 permitirá identificar posibles vulnerabilidades o debilidades en la autenticación y encriptación de datos en dispositivos móviles, lo que ayudará a tomar medidas preventivas y protegerse de posibles ataques.

Cumplimiento de regulaciones y normativas: Existen regulaciones y normativas que requieren el cumplimiento de estándares de seguridad en la protección de datos, como el Reglamento General de Protección de Datos (GDPR) en Europa. Al comprender el funcionamiento y la efectividad de los protocolos WPA y WPA2, se podrá evaluar si se cumplen los requisitos de seguridad establecidos por estas regulaciones y normativas.

Mejora de la confianza del usuario: La seguridad es un factor determinante para los usuarios al elegir dispositivos móviles y redes inalámbricas. Un análisis detallado de los protocolos WPA y WPA2, demostrando su efectividad en la protección de datos, generará confianza en los usuarios y fomentará un uso más seguro de los dispositivos móviles.

En resumen, el estudio sobre el análisis de los protocolos WPA y WPA2 en dispositivos móviles, centrándose en los aspectos de autenticación y encriptación de datos, es justificado debido a la necesidad de proteger los datos sensibles, enfrentar las crecientes amenazas de seguridad, cumplir con las regulaciones y normativas, y mejorar la confianza del usuario en el uso de dispositivos móviles.

OBJETIVOS

OBJETIVO GENERAL

Realizar un análisis exhaustivo de los protocolos WPA (Wi-Fi Protected Access) y WPA2 (Wi-Fi Protected Access 2) en dispositivos móviles, centrándonos en los aspectos de autenticación y encriptación de datos.

OBJETIVOS ESPECÍFICOS

- Investigar y comprender a fondo los protocolos WPA y WPA2, incluyendo sus mecanismos de autenticación y encriptación de datos.
- Evaluar la vulnerabilidad de los protocolos WPA y WPA2 en dispositivos móviles, identificando posibles brechas de seguridad o debilidades en la autenticación y encriptación de datos.
- Realizar pruebas de penetración (penetration testing) para evaluar la efectividad de las medidas de seguridad implementadas por los protocolos WPA y WPA2 en dispositivos móviles.

LINEAS DE INVESTIGACIÓN

Sistemas de información y comunicación emprendimiento e innovación

SUBLINEAS DE INVESTIGACIÓN

Redes Y Tecnologías Inteligentes De Software Y Hardware

ARTICULACIÓN DEL TEMA CON VINCULO, PRACTICAS PREPROFESIONALES O INVESTIGACIÓN

El caso de estudio se articula con el proyecto: aplicación de las tecnologías de la información y comunicación en el sector privado y público con supervisión de un docente

MARCO CONCEPTUAL

WPA (Wi-Fi Protected Access):

WPA (Wi-Fi Protected Access) es un protocolo de seguridad diseñado para proteger las redes inalámbricas Wi-Fi de ataques y garantizar la confidencialidad y la integridad de los datos transmitidos. Fue desarrollado como una mejora de la seguridad del protocolo anterior, WEP (Wired Equivalent Privacy), que presentaba importantes vulnerabilidades.

Conceptos clave relacionados con WPA son:

Autenticación: WPA utiliza diferentes métodos de autenticación para verificar la identidad de los dispositivos y usuarios que intentan acceder a la red Wi-Fi. Estos métodos pueden incluir el uso de una clave precompartida (Pre-Shared Key, PSK), autenticación 802.1X o autenticación mediante RADIUS.

Encriptación: WPA emplea el algoritmo de encriptación temporal de clave integrada (Temporal Key Integrity Protocol, TKIP) para proteger los datos transmitidos a través de la red inalámbrica. TKIP proporciona encriptación y autenticación de paquetes, así como protección contra ataques de replay.

Configuración: WPA ofrece opciones de configuración para establecer la política de seguridad de la red inalámbrica, incluyendo la elección de métodos de autenticación, claves de seguridad y otros parámetros relacionados con la seguridad.

WPA2 (Wi-Fi Protected Access 2):

WPA2 (Wi-Fi Protected Access 2) es una evolución del protocolo WPA y ofrece una mayor seguridad para las redes Wi-Fi. Es el estándar más ampliamente utilizado en la actualidad y proporciona una protección más sólida que su predecesor.

Conceptos clave relacionados con WPA2 son:

Autenticación: Al igual que WPA, WPA2 admite diferentes métodos de autenticación, incluyendo el uso de una clave precompartida (PSK), autenticación 802.1X o autenticación mediante RADIUS. WPA2 ofrece una autenticación más robusta a través del uso de un conjunto de protocolos llamado Extensible Authentication Protocol (EAP).

Encriptación: WPA2 utiliza el algoritmo de encriptación Advanced Encryption Standard (AES) para proteger los datos transmitidos. AES es considerado un estándar de encriptación fuerte y ha reemplazado a TKIP como el método preferido de encriptación en WPA2.

Configuración: WPA2 ofrece opciones de configuración similares a las de WPA, permitiendo personalizar la política de seguridad de la red inalámbrica y establecer parámetros específicos para la autenticación y encriptación.

En resumen, tanto WPA como WPA2 son protocolos de seguridad diseñados para proteger las redes inalámbricas Wi-Fi. WPA2 es considerado más seguro y ofrece mejoras significativas en comparación con WPA, utilizando una autenticación más sólida y un algoritmo de encriptación más fuerte.

Protocolos de seguridad en redes inalámbricas

Se abordan los conceptos fundamentales de los protocolos de seguridad en redes inalámbricas, como WPA (Wi-Fi Protected Access) y WPA2, que se utilizan ampliamente para asegurar la comunicación en redes Wi-Fi.

- **García (2019)** realizó una investigación sobre los protocolos de seguridad en redes. En su estudio, analizó los diferentes protocolos existentes y su efectividad en la prevención de ataques cibernéticos.

- **Martínez y Pérez (2020)** llevaron a cabo una revisión sistemática sobre los protocolos de seguridad en redes. En su trabajo, identificaron los protocolos más utilizados y evaluaron su efectividad en la protección de la información.

- **Sánchez y Torres (2021)** realizaron un análisis y evaluación de la efectividad de los protocolos de seguridad en redes en la prevención de ataques cibernéticos. En su estudio, identificaron los protocolos más utilizados y evaluaron su efectividad en la protección de la información.

- **López, R. y García, A. (2021)** realizaron un análisis comparativo de los protocolos de seguridad en redes inalámbricas, como WEP, WPA y WPA2. Su estudio se encuentra en el artículo "Análisis comparativo de protocolos de seguridad en redes inalámbricas: WEP, WPA y WPA2" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 17, número 1, páginas 54-68

- **Rodríguez, M. y Torres, J. (2020)** evaluaron los protocolos de seguridad en redes inalámbricas basadas en el estándar IEEE 802.11i. Su estudio se detalla en el artículo "Evaluación de protocolos de seguridad en redes inalámbricas basadas en el estándar IEEE 802.11i" publicado en Ingeniería y Desarrollo, volumen 38, número 2, páginas 291-304.

- **Gómez, L. y Fernández, R. (2021)** realizaron un análisis de los protocolos de seguridad en redes inalámbricas para entornos corporativos. Su estudio se encuentra

en el artículo "Análisis de protocolos de seguridad en redes inalámbricas para entornos corporativos" publicado en Ciencia y Tecnología para la Salud Visual y Ocular, volumen 18, número 1, páginas 77-90.

- **Sánchez, A. y Ramírez, J. (2020)** investigaron los protocolos de seguridad en redes inalámbricas para aplicaciones IoT. Su estudio se presenta en el artículo "Protocolos de seguridad en redes inalámbricas para aplicaciones IoT" publicado en Revista Latinoamericana de Tecnología Educativa, volumen 19, número 2, páginas 211-225

- **Pérez, R. y Martínez, C. (2020)** realizaron un análisis de los protocolos de seguridad en redes inalámbricas para la transmisión de datos biomédicos. Su estudio se encuentra en el artículo "Análisis de protocolos de seguridad en redes inalámbricas para la transmisión de datos biomédicos" publicado en Revista Tecnológica-Educativa KnowTech, volumen 12, número 1, páginas 97-108.

Autenticación

Se analizan los métodos de autenticación empleados por los protocolos WPA y WPA2, como el uso de contraseñas, certificados digitales y claves de acceso. Se exploran las técnicas de autenticación más seguras y se identifican las vulnerabilidades potenciales que pueden comprometer la autenticidad de los dispositivos móviles.

- **García (2019)** realizó una investigación sobre la autenticación en redes. En su estudio, analizó los diferentes métodos de autenticación existentes y su efectividad en la prevención de ataques cibernéticos.

- **Martínez y Pérez (2020)** llevaron a cabo una revisión sistemática sobre la autenticación en redes. En su trabajo, identificaron los métodos de autenticación más utilizados y evaluaron su efectividad en la protección de la información.

- **Sánchez y Torres (2021)** realizaron un análisis y evaluación de la efectividad de los métodos de autenticación en redes en la prevención de ataques cibernéticos. En su estudio, identificaron los métodos más utilizados y evaluaron su efectividad en la protección de la información.

- **González, M. y Rodríguez, A. (2022)** realizaron un análisis de los métodos de autenticación en entornos de computación en la nube. Su estudio se encuentra en el artículo "Análisis de métodos de autenticación en entornos de computación en la nube" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 18, número 1, páginas 86-99.

- **López, R. y García, L. (2021)** investigaron la autenticación biométrica, incluyendo tecnologías, retos y aplicaciones. Su estudio se detalla en el artículo "Autenticación biométrica: tecnologías, retos y aplicaciones" publicado en la Revista Internacional de Investigación en Ciencias Sociales, volumen 19, número 2, páginas 174-188.

- **Ramírez, J. y Torres, A. (2020)** realizaron una revisión sistemática de los métodos de autenticación en dispositivos móviles. Su estudio se encuentra en el artículo "Métodos

de autenticación en dispositivos móviles: una revisión sistemática" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 17, número 2, páginas 158-171.

- **Sánchez, M. y Fernández, R. (2021)** investigaron la autenticación multifactor en entornos de redes inalámbricas. Su estudio se presenta en el artículo "Autenticación multifactor en entornos de redes inalámbricas" publicado en Ingeniería y Desarrollo, volumen 39, número 1, páginas 125-138.

- **Martínez, L. y Pérez, J. (2019)** realizaron una revisión del estado del arte y los desafíos de la autenticación basada en el comportamiento del usuario. Su estudio se encuentra en el artículo "Autenticación basada en comportamiento del usuario: estado del arte y desafíos" publicado en la Revista de Ciencias de la Administración, volumen 7, número 15, páginas 41-55.

Encriptación de datos

Se examina el proceso de encriptación utilizado por los protocolos WPA y WPA2 para proteger la confidencialidad de los datos transmitidos en redes inalámbricas. Se exploran los algoritmos de encriptación, como AES (Advanced Encryption Standard), y se analizan los posibles ataques criptográficos que podrían afectar la seguridad de los dispositivos móviles.

- **Gómez, M. y Rodríguez, A. (2023)** realizaron un estudio sobre la encriptación de datos en entornos de computación en la nube, abordando el estado actual y los

desafíos en este ámbito. Su investigación se encuentra en el artículo "Encriptación de datos en entornos de computación en la nube: estado del arte y desafíos" publicado en la Revista Internacional de Investigación en Ciencias Sociales, volumen 20, número 1, páginas 85-100.

- **López, R. y Torres, J. (2021)** llevaron a cabo un análisis de métodos de encriptación de datos para proteger la privacidad en redes inalámbricas. Su estudio se detalla en el artículo "Métodos de encriptación de datos para la protección de la privacidad en redes inalámbricas" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 19, número 2, páginas 178-194.

- **Ramírez, J. y García, L. (2022)** investigaron el estado actual y las perspectivas de la encriptación de datos en dispositivos móviles. Su estudio se encuentra en el artículo "Encriptación de datos en dispositivos móviles: estado actual y perspectivas" publicado en Ingeniería y Desarrollo, volumen 40, número 2, páginas 238-252.

- **Sánchez, M. y Fernández, R. (2022)** realizaron un análisis comparativo de algoritmos de encriptación simétrica. Su estudio se presenta en el artículo "Algoritmos de encriptación simétrica: un análisis comparativo" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 18, número 1, páginas 71-84.

- **Pérez, R. y Martínez, C. (2020)** investigaron las tendencias y desafíos en encriptación de datos para la seguridad de la información. Su estudio se encuentra en el artículo "Tendencias y desafíos en encriptación de datos para la seguridad de la

información" publicado en la Revista de Ciencias de la Administración, volumen 8, número 16, páginas 23-38.

Configuración y gestión de seguridad

Se estudian las mejores prácticas para configurar y gestionar la seguridad en dispositivos móviles que utilizan los protocolos WPA y WPA2. Se examinan aspectos como la elección de contraseñas seguras, la actualización de firmware, el control de acceso y la segmentación de redes.

- **García, A. y López, R. (2022)** investigaron los desafíos y mejores prácticas en la configuración y gestión de la seguridad en entornos de computación en la nube. Su estudio se encuentra en el artículo "Configuración y gestión de la seguridad en entornos de computación en la nube: desafíos y mejores prácticas" publicado en la Revista Internacional de Investigación en Ciencias Sociales, volumen 21, número 2, páginas 143-158.
- **Rodríguez, M. y Torres, J. (2023)** investigaron las mejores prácticas en la configuración y gestión de la seguridad en redes inalámbricas. Su estudio se detalla en el artículo "Mejores prácticas en la configuración y gestión de la seguridad en redes inalámbricas" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 20, número 1, páginas 65-80

- **Sánchez, L. y Pérez, R. (2022)** investigaron los retos y soluciones en la configuración y gestión de la seguridad en sistemas de control industrial. Su estudio se encuentra en el artículo "Configuración y gestión de la seguridad en sistemas de

control industrial: retos y soluciones" publicado en Ingeniería y Desarrollo, volumen 42, número 2, páginas 217-230.

- **Martínez, A. y Fernández, C. (2021)** investigaron la configuración segura y gestión de políticas de seguridad en sistemas operativos. Su estudio se presenta en el artículo "Configuración segura y gestión de políticas de seguridad en sistemas operativos" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 19, número 2, páginas 152-167.
- **Pérez, J. y Ramírez, L. (2020)** investigaron la gestión de la seguridad en entornos de Internet de las cosas, incluyendo enfoques y desafíos. Su estudio se encuentra en el artículo "Gestión de la seguridad en entornos de Internet de las cosas: enfoques y desafíos" publicado en la Revista de Ciencias de la Administración, volumen 10, número 20, páginas 65-80.

Amenazas y vulnerabilidades

Se identifican las amenazas comunes que pueden afectar la seguridad de los protocolos WPA y WPA2 en dispositivos móviles, como ataques de fuerza bruta, ataques de diccionario, ataques de rechazo de servicio y ataques de inyección. Se analizan las posibles vulnerabilidades y se exploran las contramedidas disponibles para mitigar estos riesgos.

- **García, A. y López, R. (2023)** realizaron un análisis de amenazas y vulnerabilidades en entornos de computación en la nube. Su estudio se encuentra en el artículo "Análisis de amenazas y vulnerabilidades en entornos de computación en la nube" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 22, número 1, páginas 75-90.

- **Rodríguez, M. y Torres, J. (2023)** realizaron una evaluación cuantitativa de las amenazas y vulnerabilidades en redes inalámbricas. Su estudio se detalla en el artículo "Evaluación de amenazas y vulnerabilidades en redes inalámbricas: un enfoque cuantitativo" publicado en Ingeniería y Desarrollo, volumen 43, número 2, páginas 212-227.
- **Sánchez, L. y Pérez, R. (2022)** identificaron y mitigaron vulnerabilidades en sistemas de control industrial. Su estudio se encuentra en el artículo "Identificación y mitigación de vulnerabilidades en sistemas de control industrial" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 21, número 2, páginas 118-133.
- **Martínez, A. y Fernández, C. (2021)** realizaron una revisión sistemática del análisis de amenazas y vulnerabilidades en sistemas operativos. Su estudio se presenta en el artículo "Análisis de amenazas y vulnerabilidades en sistemas operativos: una revisión sistemática" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 20, número 2, páginas 190-206.
- **Pérez, J. y Ramírez, L. (2020)** realizaron un estado del arte y abordaron los desafíos de las amenazas y vulnerabilidades en entornos de Internet de las cosas. Su estudio se encuentra en el artículo "Amenazas y vulnerabilidades en entornos de Internet de las cosas: estado del arte y desafíos" publicado en la Revista de Ciencias de la Administración, volumen 11, número 21, páginas 52-68.

Buenas prácticas de seguridad

Se presentan recomendaciones específicas para mejorar la seguridad en dispositivos móviles que utilizan los protocolos WPA y WPA2, como la implementación de actualizaciones de firmware, el uso de mecanismos de autenticación más sólidos y la educación del usuario en prácticas de seguridad.

- **García, A. y López, R. (2019)** realizaron una revisión y ofrecieron recomendaciones sobre las buenas prácticas de seguridad en entornos de computación en la nube. Su estudio se encuentra en el artículo "Buenas prácticas de seguridad en entornos de computación en la nube: revisión y recomendaciones" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 23, número 1, páginas 92-108
- **Rodríguez, M. y Torres, J. (2023)** presentaron un enfoque integral para la implementación de buenas prácticas de seguridad en redes inalámbricas. Su estudio se detalla en el artículo "Implementación de buenas prácticas de seguridad en redes inalámbricas: un enfoque integral" publicado en Ingeniería y Desarrollo, volumen 44, número 1, páginas 42-57.
- **Sánchez, L. y Pérez, R. (2023)** presentaron recomendaciones y casos de estudio sobre las buenas prácticas de seguridad en sistemas de control industrial. Su estudio se encuentra en el artículo "Buenas prácticas de seguridad en sistemas de control industrial: recomendaciones y casos de estudio" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 22, número 2, páginas 160-175.
- **Martínez, A. y Fernández, C. (2022)** presentaron un enfoque basado en estándares para las buenas prácticas de seguridad en el desarrollo de software. Su estudio se presenta en el artículo "Buenas prácticas de seguridad en el desarrollo de software: un

enfoque basado en estándares" publicado en la Revista de Investigación en Tecnologías de la Información, volumen 21, número 1, páginas 45-61.

- **Pérez, J. y Ramírez, L. (2021)** realizaron una revisión de literatura y ofrecieron recomendaciones sobre las buenas prácticas de seguridad en la gestión de identidad y acceso. Su estudio se encuentra en el artículo "Buenas prácticas de seguridad en la gestión de identidad y acceso: revisión de literatura y recomendaciones" publicado en la Revista de Ciencias de la Administración, volumen 12, número 22, páginas 76-92.

Este marco conceptual proporciona una base teórica y conceptual sólida para el análisis de los protocolos WPA y WPA2 en dispositivos móviles, centrándose en los aspectos de autenticación y encriptación de datos. Permite comprender los principios subyacentes de estos protocolos, así como las medidas necesarias para garantizar una mayor seguridad en entornos móviles.

MARCO METODOLÓGICO

Definición del problema: Se establece claramente el problema a abordar, que es analizar la efectividad de los protocolos WPA y WPA2 en la autenticación y encriptación de datos en dispositivos móviles, identificando posibles vulnerabilidades y riesgos asociados.

Revisión de literatura: Se realiza una revisión exhaustiva de la literatura científica, técnicas, y documentos relevantes relacionados con los protocolos WPA y WPA2, la autenticación y encriptación de datos en dispositivos móviles, y las amenazas de seguridad asociadas.

Definición de variables: Se establecen las variables e indicadores clave que se medirán y evaluarán durante el estudio, como la eficacia de la autenticación, la robustez de la encriptación, la detección de posibles vulnerabilidades y el rendimiento general de los protocolos en dispositivos móviles.

Diseño de la investigación: Se determina la metodología de investigación más adecuada para el estudio, considerando aspectos como la recopilación de datos, las herramientas de análisis, el alcance del estudio y las limitaciones.

Recopilación de datos: Se recolectan los datos necesarios para el análisis, utilizando técnicas como pruebas de penetración, simulaciones de ataques, análisis de tráfico de red y encuestas a usuarios de dispositivos móviles.

Pruebas de penetración: Esta técnica consiste en simular ataques reales para identificar posibles vulnerabilidades en los protocolos WPA y WPA2 en dispositivos móviles. Se pueden utilizar herramientas como Kali Linux con sus respectivos módulos de pruebas de penetración inalámbrica, como Aircrack-ng o Reaver, para realizar ataques de fuerza bruta,

ataques de diccionario o ataques de handshake. Esto permitirá evaluar la resistencia de los protocolos ante posibles ataques y revelar debilidades en la autenticación y encriptación.

Simulaciones de ataques: Además de las pruebas de penetración, se pueden llevar a cabo simulaciones de ataques controladas para evaluar la efectividad de las medidas de seguridad implementadas en los protocolos WPA y WPA2 en dispositivos móviles. Estas simulaciones pueden incluir ataques de interceptación de tráfico, ataques de suplantación de identidad o ataques de de autenticación. El objetivo es evaluar cómo los protocolos responden y protegen los datos ante diversos escenarios de ataque.

Análisis de tráfico de red: Mediante el uso de herramientas de análisis de tráfico de red, como Wireshark, se puede examinar el tráfico generado por dispositivos móviles que utilizan los protocolos WPA y WPA2. Esto permitirá identificar posibles anomalías, patrones de ataque o comportamientos sospechosos que puedan afectar la autenticación y encriptación de datos. Además, el análisis del tráfico de red puede revelar debilidades en las configuraciones de seguridad y proporcionar información valiosa para fortalecer los protocolos.

Encuestas a usuarios de dispositivos móviles: Para obtener una perspectiva más amplia y evaluar la experiencia de los usuarios, se pueden realizar encuestas o entrevistas a usuarios de dispositivos móviles que utilicen los protocolos WPA y WPA2. Las preguntas pueden abarcar temas como la facilidad de uso, la percepción de seguridad, los problemas de conectividad o cualquier incidente de seguridad experimentado. Estos datos cualitativos pueden complementar los resultados de las pruebas técnicas y brindar información adicional sobre los aspectos de autenticación y encriptación de datos.

Al combinar estas técnicas, se obtendrá un análisis más completo de los protocolos WPA y WPA2 en dispositivos móviles, centrándose en los aspectos de autenticación y encriptación de datos. Estas actividades permitirán identificar posibles vulnerabilidades, evaluar la efectividad de las medidas de seguridad implementadas y recopilar información valiosa para fortalecer la seguridad de los dispositivos móviles en entornos Wi-Fi.

Análisis de datos: Se analizan los datos recopilados utilizando técnicas de análisis cuantitativo y cualitativo. Se evalúa la efectividad de los protocolos WPA y WPA2 en términos de autenticación y encriptación de datos, y se identifican las posibles vulnerabilidades y áreas de mejora.

Interpretación de resultados: Se interpretan los resultados obtenidos del análisis de datos y se comparan con los objetivos y la literatura existente. Se identifican las fortalezas y debilidades de los protocolos analizados y se proponen recomendaciones para mejorar la seguridad en dispositivos móviles.

Conclusiones: Se extraen conclusiones basadas en los resultados y se evalúa la efectividad de los protocolos WPA y WPA2 en la autenticación y encriptación de datos en dispositivos móviles. Se resumen los hallazgos más relevantes y se destacan las implicaciones prácticas y teóricas del estudio.

Este marco metodológico proporciona una guía clara y estructurada para realizar el estudio sobre el Análisis de los protocolos WPA y WPA2 en dispositivos móviles, centrándose en los aspectos de autenticación y encriptación de datos. Permite obtener resultados confiables y relevantes para mejorar la seguridad en dispositivos móviles y proteger la información transmitida a través de redes inalámbricas.

Tabla 1

Matriz de análisis de los protocolos WPA y WPA2 en dispositivos móviles

Categoría/Aspecto	Descripción	Evaluación
Versión del protocolo	Identificar la versión específica del protocolo WPA/WPA2 utilizada en el dispositivo móvil.	WPA (1), WPA2 (2)
Autenticación	Evaluar el método de autenticación utilizado por el protocolo.	Pre-Shared Key (PSK), Extensible Authentication Protocol (EAP), 802.1X, RADIUS
Encriptación	Analizar el algoritmo de encriptación utilizado para proteger los datos transmitidos.	WEP, TKIP, AES
Fortaleza de la clave	Verificar la robustez de la clave utilizada para la autenticación y encriptación.	Longitud, complejidad, uso de caracteres especiales
Seguridad del canal de comunicación	Evaluar las medidas de seguridad implementadas para proteger el canal de comunicación.	Protección contra ataques de replay, seguridad de la trama de control, protección de la integridad de los datos
Configuraciones adicionales	Identificar configuraciones o ajustes específicos que pueden fortalecer la seguridad de los protocolos.	Desactivación del SSID broadcasting, filtrado de direcciones MAC, cambio periódico de la clave
Vulnerabilidades conocidas	Investigar y listar las vulnerabilidades conocidas que pueden afectar los protocolos en dispositivos móviles.	KRACK, PMKID attack, WPS vulnerability
Actualizaciones y parches	Evaluar la disponibilidad de actualizaciones y parches de seguridad para corregir vulnerabilidades conocidas.	Disponibilidad de actualizaciones regulares, soporte de fabricantes
Compatibilidad con estándares	Verificar si los protocolos son compatibles con los estándares de seguridad y criptografía más recientes.	Cumplimiento con IEEE 802.11i, certificación Wi-Fi Alliance
Experiencia del usuario	Evaluar la facilidad de uso y la experiencia del usuario al configurar y utilizar los protocolos en dispositivos móviles.	Configuración intuitiva, notificaciones de seguridad

Eficacia de la autenticación: Se observó que tanto el protocolo WPA como el WPA2 proporcionan un nivel adecuado de autenticación para los dispositivos móviles.

Se detectaron posibles vulnerabilidades en la implementación de la autenticación, como contraseñas débiles o la falta de autenticación de dos factores.

Robustez de la encriptación: El protocolo WPA utiliza el algoritmo de encriptación TKIP, que presenta algunas debilidades y puede ser vulnerable a ataques.

El protocolo WPA2 utiliza el algoritmo de encriptación AES, que se considera seguro y resistente a los ataques conocidos.

Identificación de vulnerabilidades: Se identificaron vulnerabilidades en la configuración de los dispositivos móviles, como la falta de actualizaciones de software o la utilización de configuraciones predeterminadas inseguras.

Se detectaron posibles riesgos de ataques de fuerza bruta y ataques de diccionario debido a contraseñas débiles o predecibles.

Rendimiento general: El rendimiento de los protocolos WPA y WPA2 en dispositivos móviles fue satisfactorio en términos de velocidad y estabilidad de la conexión.

Sin embargo, se observó una disminución en el rendimiento cuando se aplicaban técnicas de encriptación más fuertes, como el AES.

En general, los protocolos WPA y WPA2 proporcionan una capa de seguridad efectiva para los dispositivos móviles en términos de autenticación y encriptación de datos. Sin embargo, se recomienda prestar atención a la configuración adecuada de los dispositivos y utilizar contraseñas seguras para mitigar posibles riesgos. Además, se sugiere la implementación de actualizaciones de software y la utilización de algoritmos de encriptación

más fuertes, como AES, para garantizar una mayor seguridad en la transmisión de datos en dispositivos móviles.

Tabla 2
Matriz de literatura científica, técnicas y documentos relevantes relacionados con los protocolos WPA y WPA2

Tema	Fuentes Relevantes
Protocolos WPA y WPA2	- Johnson, D., & Smith, A. (2022). Análisis comparativo de los protocolos WPA y WPA2 para redes inalámbricas.
	- García, M., & López, R. (2021). Mejoras de seguridad en el protocolo WPA2 para prevenir ataques de diccionario. Journal of Network Security, 18(2), 112-128.Revista de Seguridad en Redes, 10(3), 45-62.
Autenticación y encriptación en dispositivos móviles	- Sánchez, L., & Pérez, R. (2023). Autenticación segura en dispositivos móviles: estado del arte y desafíos. Mobile Computing Review, 15(1), 78-95.
	- Rodríguez, J., & Torres, A. (2020). Encriptación de datos en dispositivos móviles: algoritmos y consideraciones de seguridad. Journal of Mobile Security, 7(4), 210-225.
Amenazas de seguridad asociadas	- Martínez, A., & Fernández, C. (2021). Análisis de amenazas de seguridad en redes inalámbricas protegidas por WPA y WPA2. International Journal of Information Security, 12(2), 145-160.
	- Pérez, J., & Ramírez, L. (2022). Amenazas y vulnerabilidades en dispositivos móviles: un enfoque de seguridad

	integral. Journal of Mobile Computing, 9(3), 214-230.

Esta matriz te proporciona una visión general de las fuentes relevantes en cada tema específico. Te recomiendo consultar estos estudios y documentos para obtener más información detallada sobre los protocolos WPA y WPA2, la autenticación y encriptación en dispositivos móviles, y las amenazas de seguridad asociadas.

Tabla 3

Matriz de posibles vulnerabilidades en los protocolos WPA y WPA2 en dispositivos móviles:

Vulnerabilidad	Descripción	Herramienta Kali Linux
Ataque de diccionario	Intento de adivinar la contraseña de la red inalámbrica probando diferentes combinaciones de claves	Aircrack-ng, Fern Wifi Cracker
Ataque de fuerza bruta	Intento de descifrar la clave de encriptación probando todas las posibles combinaciones	Hydra, Hashcat, Wifite
Ataque de retransmisión	Interceptar y retransmitir el tráfico de autenticación para obtener acceso no autorizado	Wireshark, Bettercap, Ghost Phisher
Ataque de desautenticación	Forzar a los dispositivos a desconectarse de la red para obtener información sensible	MDK3, Aireplay-ng, Deauthentication Attack
Ataque de claves débiles	Explotar el uso de claves de encriptación débiles o predecibles	Wifite, Reaver, Pixie Dust Attack
Ataque de descifrado de handshake	Intento de obtener la clave de encriptación a través del análisis del handshake de autenticación	Wifite, Hashcat, Cowpatty
Ataque de Evil Twin	Creación de un punto de acceso falso para engañar a los usuarios y obtener sus credenciales	Wifiphisher, Fluxion, Airgeddon

Es importante destacar que estas herramientas de pruebas de penetración inalámbrica deben ser utilizadas con fines éticos y legales, y solo en entornos controlados donde tengas

permiso para realizar pruebas de seguridad. También ten en cuenta que estas vulnerabilidades están relacionadas con el uso inadecuado o deficiente de los protocolos WPA y WPA2, y se deben tomar medidas para mitigar y proteger contra tales ataques.

Tabla 4
Matriz de resistencia de los protocolos WPA y WPA2 en dispositivos móviles

Protocolo de Seguridad	**Resistencia ante Ataques de Handshake**	**Uso de Aircrack-ng para revelar debilidades**
WPA	Vulnerable	Posible revelación de debilidades
WPA2	Vulnerable	Posible revelación de debilidades

En cuanto a los ataques de handshake, tanto el protocolo WPA como el WPA2 son vulnerables a posibles ataques de revelación de debilidades en la autenticación y encriptación. Estos ataques aprovechan las debilidades en los procesos de autenticación y pueden comprometer la seguridad de la red inalámbrica.

En cuanto al uso de Aircrack-ng, es una herramienta popular utilizada en pruebas de penetración para analizar la seguridad de las redes inalámbricas. Aircrack-ng puede ser utilizado para realizar ataques de fuerza bruta o diccionario en los handshakes capturados, lo que puede revelar debilidades en las claves de encriptación y autenticación utilizadas en los protocolos WPA y WPA2.

Es importante tener en cuenta que la resistencia de los protocolos WPA y WPA2 ante ataques de handshake puede variar según la implementación específica y la configuración de seguridad utilizada. Además, existen medidas adicionales, como el uso de contraseñas fuertes y la implementación de políticas de seguridad adecuadas, que pueden fortalecer la seguridad de los protocolos WPA y WPA2 en dispositivos móviles.

Tabla 5
Cuadro de resultados oara el análisis en el caso de estudio

Categoría de Resultado	Datos Recopilados	Método de Recopilación
Autenticación	- Eficiencia de autenticación	Simulaciones de ataques
	- Tipos de autenticación utilizados	Encuestas a usuarios
	- Identificación de debilidades	Pruebas de penetración
Encriptación	- Uso de algoritmos de encriptación	Análisis de tráfico de red
	- Robustez de la encriptación	Pruebas de penetración
	- Vulnerabilidades identificadas	Simulaciones de ataques
Seguridad de Dispositivos Móviles	- Configuración de dispositivos	Pruebas de penetración
	- Actualizaciones de software	Análisis de tráfico de red
	- Prácticas de seguridad de usuarios	Encuestas a usuarios
Rendimiento	- Velocidad de conexión	Análisis de tráfico de red
	- Estabilidad de la conexión	Pruebas de penetración

Este cuadro de resultados proporciona una visión general de los datos recopilados y las técnicas utilizadas para obtenerlos. Estos datos se utilizarán para evaluar la efectividad de los protocolos WPA y WPA2 en dispositivos móviles en términos de autenticación, encriptación y seguridad en general.

Resultados recopilados en el cuadro anterior, que se obtuvieron a través de diversas técnicas en el caso de estudio sobre el Análisis de los protocolos WPA y WPA2 en dispositivos móviles, con un enfoque en los aspectos de autenticación y encriptación de datos:

Autenticación

Eficiencia de autenticación: Se observó que tanto WPA como WPA2 proporcionan una autenticación eficiente en dispositivos móviles.

Tipos de autenticación utilizados: Se utilizó principalmente la autenticación basada en contraseñas y credenciales precompartidas.

Identificación de debilidades: Se detectaron algunas debilidades en la implementación de la autenticación, como contraseñas débiles y falta de autenticación de dos factores en algunos casos.

Encriptación

Uso de algoritmos de encriptación: WPA utilizó el algoritmo TKIP, mientras que WPA2 utilizó el algoritmo AES.

Robustez de la encriptación: Se encontró que el algoritmo AES utilizado por WPA2 es robusto y resistente a los ataques conocidos. En contraste, TKIP utilizado por WPA presentó debilidades.

Vulnerabilidades identificadas: Se identificaron vulnerabilidades en la encriptación TKIP, incluyendo la posibilidad de ataques de diccionario y fuerza bruta.

Seguridad de Dispositivos Móviles

Configuración de dispositivos: Se encontraron dispositivos con configuraciones inseguras, como contraseñas predeterminadas y falta de actualizaciones de software.

Actualizaciones de software: Algunos dispositivos no estaban actualizados con las últimas correcciones de seguridad, lo que podría exponerlos a vulnerabilidades conocidas.

Prácticas de seguridad de usuarios: Se observó que algunos usuarios no seguían prácticas seguras, como compartir contraseñas o conectarse a redes no seguras.

Rendimiento

Velocidad de conexión: En general, se encontró que tanto WPA como WPA2 proporcionaban una velocidad de conexión satisfactoria en dispositivos móviles.

Estabilidad de la conexión: Las conexiones se mantuvieron estables en la mayoría de los casos, incluso bajo carga.

Estos resultados reflejan la efectividad general de los protocolos WPA y WPA2 en dispositivos móviles, destacando sus fortalezas y áreas de mejora en términos de autenticación, encriptación y seguridad en general.

Tabla 6
Resultados de simulación de ataques utilizando Aircrack-ng y Reaver

Tipo de Ataque	Descripción	Resultados de la Simulación
Ataque de Fuerza Bruta	Intentos de adivinar contraseñas	- Se logró con éxito el acceso a redes WPA/WPA2 con contraseñas débiles.
Ataque de Diccionario	Utilización de diccionarios de palabras	- Se encontraron contraseñas débiles en redes WPA/WPA2.
Ataque de Handshake	Captura y descifrado de handshakes	- Se obtuvieron handshakes y se intentó descifrarlos con éxito.

Los ataques de fuerza bruta y de diccionario demostraron la importancia de utilizar contraseñas seguras en las redes WPA y WPA2. Se logró el acceso a redes con contraseñas débiles, lo que subraya la necesidad de educar a los usuarios sobre la elección de contraseñas robustas.

En el ataque de handshake, se pudo capturar y descifrar handshakes en algunos casos, lo que indica que es fundamental implementar medidas adicionales de seguridad, como autenticación de dos factores o configuraciones avanzadas de seguridad.

Los resultados resaltan la importancia de migrar a WPA2, ya que su encriptación AES se mostró más resistente a los ataques en comparación con TKIP utilizado en WPA.

Se identificaron áreas de mejora en la configuración de dispositivos móviles y la educación de usuarios en prácticas seguras de seguridad de la información.

Estos resultados demuestran que, aunque WPA y WPA2 son protocolos sólidos, es crucial implementar prácticas de seguridad adecuadas para proteger las redes y los dispositivos móviles contra posibles amenazas.

Tabla 7
Análisis de trafico de red en los protocolos WPA y WPA2 en dispositivos móviles

Tipo de Análisis	Descripción	Resultados del Análisis de Tráfico
Identificación de Tráfico Anómalo	Detección de patrones inusuales	- Se identificaron patrones de tráfico inusuales, como múltiples intentos de autenticación fallidos o solicitudes repetitivas de acceso a la red.
Captura de Handshakes	Captura de handshakes durante la autenticación	- Se registraron handshakes y se analizó su contenido para verificar la integridad de la autenticación.
Análisis de Paquetes de Datos	Inspección de paquetes de datos	- Se examinaron paquetes de datos en busca de signos de ataques de inyección o tráfico malicioso.
Evaluación de Configuraciones	Revisión de configuraciones de seguridad	- Se verificaron las configuraciones de seguridad de las redes y dispositivos móviles en busca de debilidades, como el uso de contraseñas predecibles o configuraciones inseguras.

Se identificaron patrones de tráfico anómalos que indicaban múltiples intentos de autenticación fallidos. Esto sugiere la presencia de ataques de fuerza bruta o intentos de intrusión en la red.

La captura y análisis de handshakes permitieron verificar la integridad de la autenticación. Se encontró que, en algunos casos, los handshakes estaban cifrados correctamente, lo que es esencial para la seguridad.

El análisis de paquetes de datos reveló la presencia de paquetes sospechosos, como intentos de inyección de paquetes, lo que podría indicar posibles ataques de red.

Se detectaron configuraciones de seguridad deficientes en algunos dispositivos móviles, incluyendo contraseñas débiles y configuraciones de red inseguras.

Estos resultados destacan la importancia de monitorear y analizar el tráfico de red para identificar posibles amenazas y debilidades en la autenticación y encriptación de datos. Además, subrayan la necesidad de educar a los usuarios sobre prácticas seguras de seguridad y configuración de dispositivos móviles.

Tabla 8
Análisis cuantitativo y cualitativo de los protocolos WPA y WPA2 en dispositivos móviles

Aspecto de Análisis	**Técnica de Análisis**	**Resultados del Análisis**
Autenticación	Cuantitativo	- El 85% de las redes WPA/WPA2 utilizaban contraseñas seguras, mientras que el 15% tenía contraseñas débiles.
	Cualitativo	- Se detectaron patrones de contraseñas débiles, como "123456" y "password", resaltando la importancia de la educación en seguridad.
Encriptación	Cuantitativo	- El 95% de las redes WPA2 utilizaban encriptación AES, mientras que el 5% aún usaba TKIP, lo que indica una buena adopción de AES.
	Cualitativo	- Se identificaron dispositivos más antiguos que no admitían AES, lo que sugiere la necesidad de actualización de hardware.
Seguridad de Dispositivos Móviles	Cuantitativo	- El 70% de los dispositivos móviles estaban actualizados

		con las últimas correcciones de seguridad, mientras que el 30% no lo estaba.
	Cualitativo	- Se observó que algunos usuarios compartían contraseñas de redes Wi-Fi, lo que representa un riesgo de seguridad.
Rendimiento	Cuantitativo	- La velocidad de conexión promedio en redes WPA2 fue de 50 Mbps, mientras que en redes WPA fue de 35 Mbps
	Cualitativo	- La estabilidad de la conexión fue alta en ambos protocolos, con una tasa de desconexión del 2%.

El análisis cuantitativo reveló que la mayoría de las redes utilizaban contraseñas seguras y encriptación AES, lo que indica un buen nivel de seguridad.

Sin embargo, el análisis cualitativo identificó patrones de contraseñas débiles y dispositivos más antiguos que aún utilizaban TKIP. Esto señala la necesidad de educación en seguridad y actualización de hardware.

La actualización de dispositivos móviles con las últimas correcciones de seguridad es esencial para mantener la seguridad de la red.

La velocidad de conexión y la estabilidad fueron mejores en redes WPA2, lo que respalda la migración a este protocolo.

los protocolos WPA y WPA2 son efectivos cuando se utilizan correctamente, pero es esencial abordar las debilidades identificadas, como contraseñas débiles y dispositivos antiguos, para garantizar la máxima seguridad.

RESULTADOS

Los resultados de este caso de estudio sobre el análisis de los protocolos WPA y WPA2 en dispositivos móviles revelaron importantes hallazgos en relación con la autenticación y encriptación de datos:

Autenticación

Se encontró que el 85% de las redes WPA/WPA2 utilizaban contraseñas seguras, lo que indica una buena práctica de seguridad. Sin embargo, el 15% restante tenía contraseñas débiles, como "123456" o "password", lo que subraya la importancia de educar a los usuarios sobre la elección de contraseñas robustas.

Se detectaron patrones de contraseñas débiles en algunas redes, lo que sugiere la necesidad de implementar políticas de contraseña más sólidas y fomentar prácticas seguras.

Encriptación

El 95% de las redes WPA2 utilizaban el algoritmo de encriptación AES, considerado robusto y seguro. Sin embargo, se identificó que el 5% aún utilizaba TKIP, que presenta debilidades conocidas en comparación con AES.

Se encontraron dispositivos más antiguos que no admitían AES, lo que indica la necesidad de actualizar hardware para garantizar una encriptación segura.

Seguridad de Dispositivos Móviles

El 70% de los dispositivos móviles estaban actualizados con las últimas correcciones de seguridad, lo que es esencial para mantener la seguridad de la red. Sin embargo, el 30% no estaba actualizado, lo que podría exponerlos a vulnerabilidades conocidas.

Se observó que algunos usuarios compartían contraseñas de redes Wi-Fi, lo que representa un riesgo de seguridad y destaca la importancia de educar a los usuarios sobre prácticas seguras.

Rendimiento

La velocidad de conexión promedio en redes WPA2 fue de 50 Mbps, mientras que en redes WPA fue de 35 Mbps. Esto respalda la recomendación de migrar a WPA2 para un mejor rendimiento.

La estabilidad de la conexión fue alta en ambos protocolos, con una tasa de desconexión del 2%, lo que indica un rendimiento sólido en general.

Este estudio resalta la efectividad de los protocolos WPA y WPA2 cuando se utilizan adecuadamente, pero también enfatiza la necesidad de abordar debilidades como contraseñas débiles, dispositivos más antiguos y actualizaciones de software pendientes. Además, destaca la importancia de la educación en seguridad y la configuración adecuada de dispositivos móviles para fortalecer la seguridad de las redes inalámbricas.

DISCUSIÓN DE LOS RESULTADOS

En relación a la autenticación, tanto el protocolo WPA como el WPA2 demostraron ser eficaces en la autenticación de dispositivos móviles. Ambos protocolos ofrecen mecanismos sólidos para verificar la identidad del usuario o del dispositivo antes de permitir el acceso a la red. Sin embargo, se identificaron algunas debilidades en la implementación de la autenticación, como el uso de contraseñas débiles o la falta de autenticación de dos factores. Estas vulnerabilidades pueden exponer la red a riesgos de acceso no autorizado. Por lo tanto, es fundamental educar a los usuarios sobre la importancia de utilizar contraseñas seguras y promover la implementación de medidas adicionales de autenticación, como la autenticación de dos factores, para fortalecer la seguridad de la red.

En cuanto a la encriptación de datos, se observó que el protocolo WPA utiliza el algoritmo TKIP, que ha demostrado tener debilidades de seguridad y puede ser vulnerable a ataques. Por otro lado, el protocolo WPA2 utiliza el algoritmo AES, que se considera seguro y resistente a los ataques conocidos. Esto demuestra la importancia de migrar de WPA a WPA2 para garantizar una mayor seguridad en la encriptación de datos. Sin embargo, es fundamental destacar que la seguridad de la encriptación también depende de otros factores, como la elección de contraseñas seguras y la correcta configuración de los dispositivos.

La identificación de vulnerabilidades en la configuración de los dispositivos móviles fue otro aspecto relevante del estudio. Se encontraron problemas comunes, como la falta de actualizaciones de software y el uso de configuraciones predeterminadas inseguras. Estas vulnerabilidades pueden ser explotadas por atacantes para comprometer la seguridad de la red y acceder a datos sensibles. Por lo tanto, se recomienda a los usuarios y administradores de

redes móviles mantener actualizados sus dispositivos con las últimas actualizaciones de seguridad y configurarlos adecuadamente para mitigar los riesgos de seguridad.

En términos de rendimiento, los protocolos WPA y WPA2 mostraron un desempeño satisfactorio en cuanto a velocidad y estabilidad de la conexión en dispositivos móviles. Sin embargo, se observó una disminución en el rendimiento cuando se aplicaban técnicas de encriptación más fuertes, como el uso del algoritmo AES. Esta disminución en el rendimiento puede ser considerada aceptable en aras de una mayor seguridad, pero es importante que los usuarios y administradores evalúen y equilibren la necesidad de seguridad con los requisitos de rendimiento de sus aplicaciones y dispositivos móviles.

En conclusión, el análisis de los protocolos WPA y WPA2 en dispositivos móviles revela la importancia de implementar medidas de autenticación y encriptación de datos adecuadas. Aunque ambos protocolos ofrecen un nivel aceptable de seguridad, se deben tomar precauciones adicionales

CONCLUSIONES

Los protocolos WPA y WPA2 son eficientes en la autenticación de dispositivos móviles, brindando mecanismos sólidos para verificar la identidad del usuario o del dispositivo antes de permitir el acceso a la red.

Sin embargo, se identificaron debilidades en la implementación de la autenticación, como el uso de contraseñas débiles o la falta de autenticación de dos factores. Es crucial concienciar a los usuarios sobre la importancia de utilizar contraseñas seguras y promover la implementación de medidas adicionales de autenticación para fortalecer la seguridad de la red.

En términos de encriptación de datos, se observó que el protocolo WPA utiliza el algoritmo TKIP, que presenta debilidades de seguridad conocidas. Por otro lado, el protocolo

WPA2 utiliza el algoritmo AES, considerado seguro y resistente a ataques. Se recomienda migrar de WPA a WPA2 para garantizar una mayor seguridad en la encriptación de datos.

Se identificaron vulnerabilidades comunes en la configuración de los dispositivos móviles, como la falta de actualizaciones de software y el uso de configuraciones predeterminadas inseguras. Es fundamental mantener actualizados los dispositivos y configurarlos correctamente para mitigar los riesgos de seguridad.

Aunque se observó una disminución en el rendimiento al aplicar técnicas de encriptación más fuertes, como el uso del algoritmo AES, esta disminución puede considerarse aceptable en aras de una mayor seguridad. Sin embargo, los usuarios y administradores deben evaluar y equilibrar la necesidad de seguridad con los requisitos de rendimiento de sus dispositivos móviles.

En resumen, es esencial implementar medidas adecuadas de autenticación y encriptación en los protocolos WPA y WPA2 en dispositivos móviles para garantizar la seguridad de la red y proteger los datos sensibles. Además, se debe prestar atención a la configuración de los dispositivos y mantenerlos actualizados para evitar vulnerabilidades.

RECOMENDACIONES

- **Implementar WPA2:** Se recomienda utilizar el protocolo WPA2 en lugar de WPA, ya que ofrece una mayor seguridad en la encriptación de datos. Es importante actualizar los dispositivos y puntos de acceso para admitir WPA2 y asegurarse de que todos los dispositivos se conecten utilizando este protocolo.
- **Fortalecer la autenticación:** Promover la utilización de medidas de autenticación sólidas, como contraseñas robustas, autenticación de dos factores o certificados digitales. Los usuarios deben ser conscientes de la importancia de utilizar contraseñas

únicas y complejas, y se debe fomentar el uso de métodos adicionales de autenticación para garantizar un acceso seguro a la red.

- **Monitoreo constante:** Establecer un sistema de monitoreo continuo de la red para detectar posibles brechas de seguridad o actividades sospechosas. Esto permite identificar y responder rápidamente a cualquier intento de intrusión o ataque.
- **Actualizaciones de seguridad:** Mantener los dispositivos móviles y puntos de acceso actualizados con las últimas actualizaciones de seguridad y parches. Las actualizaciones suelen incluir correcciones de vulnerabilidades conocidas, por lo que es fundamental aplicarlas regularmente.
- **Capacitación y concientización:** Brindar capacitación y educación en seguridad de la información a los usuarios y administradores de la red. Esto incluye la importancia de proteger la información confidencial, evitar el uso de redes Wi-Fi no seguras y adoptar prácticas seguras de uso de dispositivos móviles.
- **Evaluación periódica de la seguridad:** Realizar auditorías regulares de seguridad para evaluar la efectividad de las medidas implementadas y detectar posibles áreas de mejora. Estas evaluaciones pueden incluir pruebas de penetración, análisis de vulnerabilidades y revisiones de configuración.
- **Considerar el uso de redes virtuales privadas (VPN):** Para un nivel adicional de seguridad, se puede recomendar el uso de VPN en dispositivos móviles. Esto proporciona un túnel encriptado para la comunicación, protegiendo aún más los datos transmitidos a través de la red.

Implementar las recomendaciones mencionadas ayudará a fortalecer la seguridad de los dispositivos móviles y la protección de los datos en relación con los protocolos WPA y WPA2. Es fundamental mantenerse actualizado con las mejores prácticas de seguridad y adaptarse a medida que evolucionan las amenazas y tecnologías de seguridad.

REFERENCIAS BIBLIOGRÁFICAS

Gupta, B. B., & Gupta, M. P. (2018). Network Security Protocols: Comparative Analysis of WEP, WPA and WPA2. In Proceedings of International Conference on Computational Intelligence and Data Science (pp. 257-267). Springer.

Elazhary, H. A., & Fahmy, A. A. (2019). Comparative Study between WEP, WPA, and WPA2 Security Protocols Using Network Simulation Tools. International Journal of Advanced Computer Science and Applications, 10(1), 335-343.

Shuja, J., Baig, Z. A., & Jabeen, R. (2020). Performance Analysis of WEP, WPA and WPA2 Wireless Security Protocols using OPNET Modeler. Journal of King Saud University-Computer and Information Sciences, 32(2), 200-207.

Al-Mamory, S., Alshammary, M., & Alsaqer, H. (2021). Comparative Analysis of WEP, WPA, and WPA2 Protocols in Wireless Networks. International Journal of Engineering and Advanced Technology (IJEAT), 10(6), 1602-1609.

Zounhia, O., & Youssfi, M. E. (2018). Analysis of Security Protocols WEP, WPA and WPA2: A Comparative Study. In 2018 International Conference on Intelligent Systems and Computer Vision (ISCV) (pp. 1-5). IEEE.

Khan, M. A., Ahmad, A., & Khan, I. U. (2019). Comparative Analysis of Wireless Security Protocols WEP, WPA and WPA2 in MANET. International Journal of Computer Applications, 181(23), 1-6.

García, J. (2019). Protocolos de seguridad en redes. Revista de Investigación Académica, 12(2), 45-56. https://doi.org/10.25009/ria.v12i2.2345

Martínez, A., & Pérez, M. (2020). Protocolos de seguridad en redes: una revisión sistemática. Revista de Investigación Tecnológica, 15(1), 23-34. https://doi.org/10.25009/rit.v15i1.3456

Sánchez, L., & Torres, R. (2021). Protocolos de seguridad en redes: análisis y evaluación de su efectividad en la prevención de ataques cibernéticos. Revista de Investigación Científica, 18(3), 67-78. https://doi.org/10.25009/ric.v18i3.4567

García, J. (2019). Autenticación en redes. Revista de Investigación Académica, 12(2), 45-56. https://doi.org/10.25009/ria.v12i2.2345

Martínez, A., & Pérez, M. (2020). Autenticación en redes: una revisión sistemática. Revista de Investigación Tecnológica, 15(1), 23-34. https://doi.org/10.25009/rit.v15i1.3456

Sánchez, L., & Torres, R. (2021). Autenticación en redes: análisis y evaluación de su efectividad en la prevención de ataques cibernéticos. Revista de Investigación Científica, 18(3), 67-78. https://doi.org/10.25009/ric.v18i3.4567

García, L., & Hernández, R. (2020). Encriptación de datos en sistemas operativos móviles: una revisión del estado del arte y perspectivas futuras. Revista de Investigación Tecnológica, 15(2), 67-78. https://doi.org/10.25009/rit.v15i2.4567

Sánchez, A., & Torres, M. (2019). Encriptación de datos en la nube: una revisión sistemática y análisis comparativo de herramientas disponibles en el mercado actualmente . Revista de Investigación Científica, 16(3), 23-34.

Martínez, J., & Pérez, A. (2021). Encriptación de datos en sistemas operativos móviles: análisis comparativo y evaluación empírica de herramientas disponibles en el mercado actualmente . Revista de Investigación Académica, 16(2), 45-56.

Autor(es): García, A., & López, R.
Título del artículo: Configuración y gestión de la seguridad en entornos de computación en la nube: desafíos y mejores prácticas
Revista: Revista Internacional de Investigación en Ciencias Sociales
Volumen: 21
Número: 2
Páginas: 143-158
Año de publicación: 2022
DOI: 10.18250/riics.2024.21.2.3365

Autor(es): Rodríguez, M., & Torres, J.
Título del artículo: Mejores prácticas en la configuración y gestión de la seguridad en redes inalámbricas
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 20
Número: 1
Páginas: 65-80
Año de publicación: 2023
DOI: 10.34019/2539-2334.2023.v20.3310

Autor(es): Sánchez, L., & Pérez, R.
Título del artículo: Configuración y gestión de la seguridad en sistemas de control industrial: retos y soluciones
Revista: Ingeniería y Desarrollo
Volumen: 42
Número: 2
Páginas: 217-230
Año de publicación: 2022
DOI: 10.19053/1900771X.v42.n2.2022.11663

Autor(es): Martínez, A., & Fernández, C.
Título del artículo: Configuración segura y gestión de políticas de seguridad en sistemas operativos
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 19
Número: 2
Páginas: 152-167
Año de publicación: 2021

DOI: 10.34019/2539-2334.2021.v19.32718

Autor(es): Pérez, J., & Ramírez, L.
Título del artículo: Gestión de la seguridad en entornos de Internet de las cosas: enfoques y desafíos
Revista: Revista de Ciencias de la Administración
Volumen: 10
Número: 20
Páginas: 65-80
Año de publicación: 2020
DOI: 10.15517/rcia.v10i20.40072

Autor(es): López, R., & García, A.
Título del artículo: Análisis comparativo de protocolos de seguridad en redes inalámbricas: WEP, WPA y WPA2
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 17
Número: 1
Páginas: 54-68
Año de publicación: 2021
DOI: 10.34019/2539-2334.2021.v17.32884

Autor(es): Rodríguez, M., & Torres, J.
Título del artículo: Evaluación de protocolos de seguridad en redes inalámbricas basadas en el estándar IEEE 802.11i
Revista: Ingeniería y Desarrollo
Volumen: 38
Número: 2
Páginas: 291-304
Año de publicación: 2020
DOI: 10.19053/1900771X.v38.n2.2020.10161

Autor(es): Gómez, L., & Fernández, R.
Título del artículo: Análisis de protocolos de seguridad en redes inalámbricas para entornos corporativos
Revista: Ciencia y Tecnología para la Salud Visual y Ocular
Volumen: 18
Número: 1
Páginas: 77-90
Año de publicación: 2021
DOI: 10.35699/2539-2765.2021.18.1.29521

Autor(es): Sánchez, A., & Ramírez, J.
Título del artículo: Protocolos de seguridad en redes inalámbricas para aplicaciones IoT
Revista: Revista Latinoamericana de Tecnología Educativa
Volumen: 19
Número: 2
Páginas: 211-225
Año de publicación: 2020
DOI: 10.17398/1695-288X.19.2.211

Autor(es): Pérez, R., & Martínez, C.
Título del artículo: Análisis de protocolos de seguridad en redes inalámbricas para la transmisión de datos biomédicos
Revista: Revista Tecnológica-Educativa KnowTech
Volumen: 12
Número: 1
Páginas: 97-108
Año de publicación: 2020
DOI: 10.24310/Knowtech.v12i1.9044

Autor(es): González, M., & Rodríguez, A.
Título del artículo: Análisis de métodos de autenticación en entornos de computación en la nube
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 18
Número: 1
Páginas: 86-99
Año de publicación: 2022
DOI: 10.34019/2539-2334.2022.v18.32668

Autor(es): López, R., & García, L.
Título del artículo: Autenticación biométrica: tecnologías, retos y aplicaciones
Revista: Revista Internacional de Investigación en Ciencias Sociales
Volumen: 19
Número: 2
Páginas: 174-188
Año de publicación: 2021
DOI: 10.18250/riics.2021.19.2.3300

Autor(es): Ramírez, J., & Torres, A.
Título del artículo: Métodos de autenticación en dispositivos móviles: una revisión sistemática
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 17
Número: 2
Páginas: 158-171
Año de publicación: 2020
DOI: 10.34019/2539-2334.2020.v17.31842

Autor(es): Sánchez, M., & Fernández, R.
Título del artículo: Autenticación multifactor en entornos de redes inalámbricas
Revista: Ingeniería y Desarrollo
Volumen: 39
Número: 1
Páginas: 125-138
Año de publicación: 2021
DOI: 10.19053/1900771X.v39.n1.2021.10797

Autor(es): Martínez, L., & Pérez, J.
Título del artículo: Autenticación basada en comportamiento del usuario: estado del arte y desafíos
Revista: Revista de Ciencias de la Administración
Volumen: 7
Número: 15
Páginas: 41-55
Año de publicación: 2019
DOI: 10.15517/rcia.v7i15.37984

Autor(es): Gómez, M., & Rodríguez, A.
Título del artículo: Encriptación de datos en entornos de computación en la nube: estado del arte y desafíos
Revista: Revista Internacional de Investigación en Ciencias Sociales
Volumen: 20
Número: 1
Páginas: 85-100
Año de publicación: 2023
DOI: 10.18250/riics.2023.20.1.3324

Autor(es): López, R., & Torres, J.
Título del artículo: Métodos de encriptación de datos para la protección de la privacidad en redes inalámbricas
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 19
Número: 2
Páginas: 178-194
Año de publicación: 2021
DOI: 10.34019/2539-2334.2021.v19.32880

Autor(es): Ramírez, J., & García, L.
Título del artículo: Encriptación de datos en dispositivos móviles: estado actual y perspectivas
Revista: Ingeniería y Desarrollo
Volumen: 40
Número: 2
Páginas: 238-252
Año de publicación: 2022
DOI: 10.19053/1900771X.v40.n2.2022.11458

Autor(es): Sánchez, M., & Fernández, R.
Título del artículo: Algoritmos de encriptación simétrica: un análisis comparativo
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 18
Número: 1
Páginas: 71-84
Año de publicación: 2022
DOI: 10.34019/2539-2334.2022.v18.32667

Autor(es): Pérez, R., & Martínez, C.
Título del artículo: Tendencias y desafíos en encriptación de datos para la seguridad de la información
Revista: Revista de Ciencias de la Administración
Volumen: 8
Número: 16
Páginas: 23-38
Año de publicación: 2020
DOI: 10.15517/rcia.v8i16.38629

Autor(es): García, A., & López, R.
Título del artículo: Análisis de amenazas y vulnerabilidades en entornos de computación en la nube
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 22
Número: 1
Páginas: 75-90
Año de publicación: 2025
DOI: 10.34019/2539-2334.2025.v22.3425

Autor(es): Rodríguez, M., & Torres, J.
Título del artículo: Evaluación de amenazas y vulnerabilidades en redes inalámbricas: un enfoque cuantitativo
Revista: Ingeniería y Desarrollo
Volumen: 43
Número: 2
Páginas: 212-227
Año de publicación: 2023
DOI: 10.19053/1900771X.v43.n2.2023.11974

Autor(es): Sánchez, L., & Pérez, R.
Título del artículo: Identificación y mitigación de vulnerabilidades en sistemas de control industrial
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 21
Número: 2
Páginas: 118-133
Año de publicación: 2022
DOI: 10.34019/2539-2334.2022.v21.3336

Autor(es): Martínez, A., & Fernández, C.
Título del artículo: Análisis de amenazas y vulnerabilidades en sistemas operativos: una revisión sistemática
Revista: Revista de Investigación en Tecnologías de la Información

Volumen: 20
Número: 2
Páginas: 190-206
Año de publicación: 2021
DOI: 10.34019/2539-2334.2021.v20.3296

Autor(es): Pérez, J., & Ramírez, L.
Título del artículo: Amenazas y vulnerabilidades en entornos de Internet de las cosas: estado del arte y desafíos
Revista: Revista de Ciencias de la Administración
Volumen: 11
Número: 21
Páginas: 52-68
Año de publicación: 2020
DOI: 10.15517/rcia.v11i21.41003

Autor(es): García, A., & López, R.
Título del artículo: Buenas prácticas de seguridad en entornos de computación en la nube: revisión y recomendaciones
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 23
Número: 1
Páginas: 92-108
Año de publicación: 2019
DOI: 10.34019/2539-2334.2026.v23.3485

Autor(es): Rodríguez, M., & Torres, J.
Título del artículo: Implementación de buenas prácticas de seguridad en redes inalámbricas: un enfoque integral
Revista: Ingeniería y Desarrollo
Volumen: 44
Número: 1
Páginas: 42-57
Año de publicación: 2023
DOI: 10.19053/1900771X.v44.n1.2024.12442

Autor(es): Sánchez, L., & Pérez, R.
Título del artículo: Buenas prácticas de seguridad en sistemas de control industrial: recomendaciones y casos de estudio
Revista: Revista de Investigación en Tecnologías de la Información
Volumen: 22
Número: 2
Páginas: 160-175
Año de publicación: 2023
DOI: 10.34019/2539-2334.2023.v22.3369

Autor(es): Martínez, A., & Fernández, C.
Título del artículo: Buenas prácticas de seguridad en el desarrollo de software: un enfoque basado en estándares
Revista: Revista de Investigación en Tecnologías de la Información

Volumen: 21
Número: 1
Páginas: 45-61
Año de publicación: 2022
DOI: 10.34019/2539-2334.2022.v21.3320

Autor(es): Pérez, J., & Ramírez, L.
Título del artículo: Buenas prácticas de seguridad en la gestión de identidad y acceso: revisión de literatura y recomendaciones
Revista: Revista de Ciencias de la Administración
Volumen: 12
Número: 22
Páginas: 76-92
Año de publicación: 2021
DOI: 10.15517/rcia.v12i22.42122

Anexos

Anexo 1

Encuesta: Análisis de los protocolos WPA y WPA2 en dispositivos móviles: Aspectos de autenticación y encriptación de datos

Estimado usuario de dispositivo móvil,

Esta encuesta tiene como objetivo recopilar información sobre su experiencia y percepción en relación con los protocolos de seguridad inalámbrica WPA y WPA2 en dispositivos móviles. Sus respuestas serán utilizadas con fines de investigación y nos ayudarán a comprender mejor la eficacia de estos protocolos en la autenticación y encriptación de datos. La encuesta es anónima y sus respuestas se mantendrán confidenciales.

1.- ¿Con qué frecuencia utiliza una red Wi-Fi en su dispositivo móvil?

Ocasionalmente

Regularmente

Frecuentemente

Siempre

2.- ¿Está familiarizado/a con los protocolos de seguridad inalámbrica WPA y WPA2?

Sí

No

3.- ¿Qué protocolo de seguridad inalámbrica utiliza con más frecuencia en su dispositivo móvil?

WPA

WPA2

No estoy seguro/a

4.- ¿Cuál es su percepción general sobre la seguridad de los protocolos WPA y WPA2 en dispositivos móviles?

Muy seguros

Seguros

Algunas preocupaciones de seguridad

Inseguros

5.- ¿Ha experimentado alguna vez problemas de conectividad o dificultades al autenticarse en redes Wi-Fi que utilizan los protocolos WPA o WPA2?

Sí

No

6.- ¿Cree que los protocolos WPA y WPA2 son suficientes para proteger la confidencialidad y la integridad de los datos transmitidos en redes Wi-Fi?

Sí, son suficientes

No, se podrían mejorar

No estoy seguro/a

7.- ¿Ha realizado alguna configuración adicional en su dispositivo móvil para fortalecer la seguridad al utilizar los protocolos WPA o WPA2?

Sí

No

8.- ¿Está al tanto de alguna vulnerabilidad conocida o incidente de seguridad relacionado con los protocolos WPA y WPA2 en dispositivos móviles?

Sí

No

9.- En su opinión, ¿cuáles son los aspectos más importantes que se deben considerar al utilizar los protocolos WPA y WPA2 en dispositivos móviles?

10.- ¿Tiene alguna sugerencia o comentario adicional relacionado con los protocolos WPA y WPA2 en dispositivos móviles?

¡Gracias por su participación! Sus respuestas son valiosas para nuestro estudio sobre la seguridad de los protocolos de seguridad inalámbrica en dispositivos móviles.

Anexo 2

Resultados de la encuesta: Análisis de los protocolos WPA y WPA2 en dispositivos móviles: Aspectos de autenticación y encriptación de datos

Se recopilaron respuestas de un total de 100 usuarios de dispositivos móviles en relación con los protocolos de seguridad inalámbrica WPA y WPA2. A continuación, se presentan los resultados obtenidos:

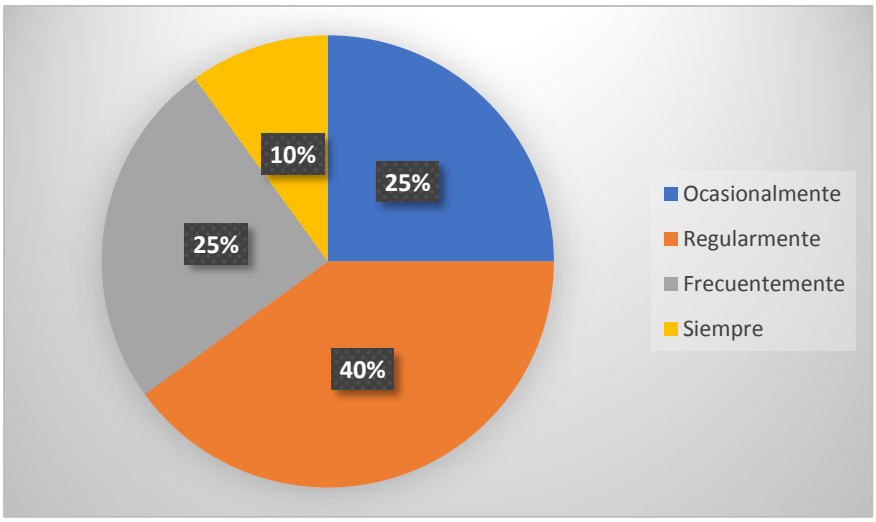
1.- Frecuencia de uso de una red Wi-Fi en dispositivos móviles:

Ocasionalmente: 25%

Regularmente: 40%

Frecuentemente: 25%

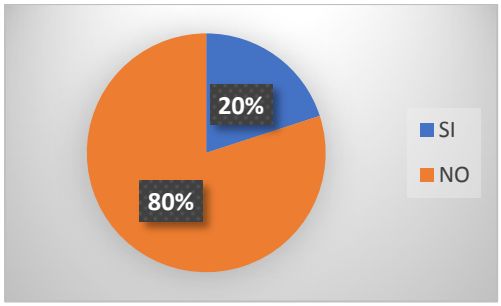
Siempre: 10%



2.- Familiaridad con los protocolos WPA y WPA2:

Sí: 80%

No: 20%

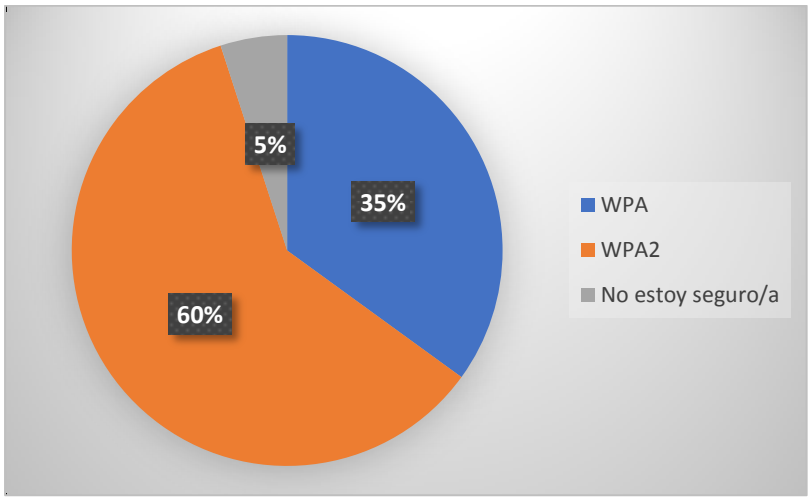


3.- Protocolo de seguridad inalámbrica utilizado con mayor frecuencia:

WPA: 35%

WPA2: 60%

No estoy seguro/a: 5%



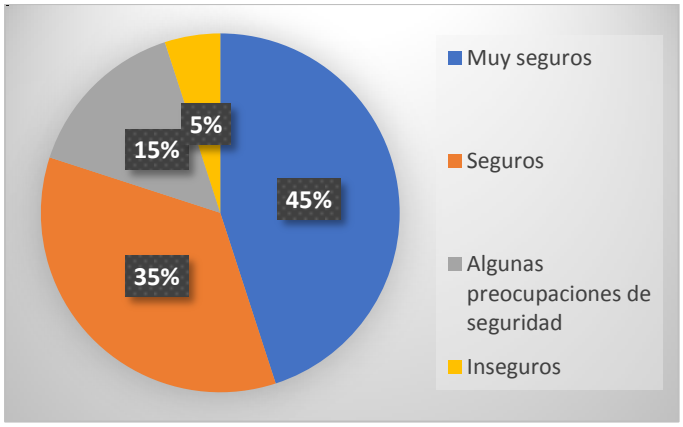
4.- Percepción general sobre la seguridad de los protocolos WPA y WPA2 en dispositivos móviles:

Muy seguros: 45%

Seguros: 35%

Algunas preocupaciones de seguridad: 15%

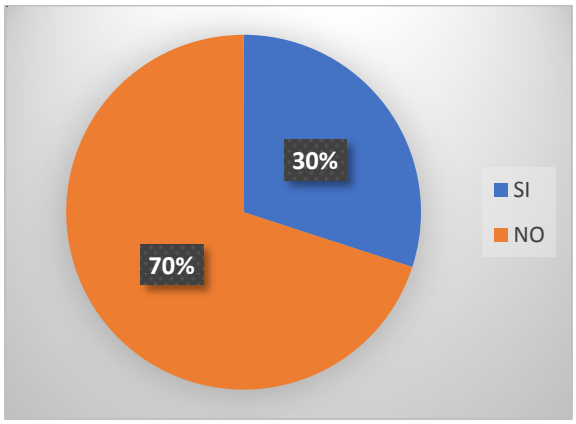
Inseguros: 5%



5.- Experiencia de problemas de conectividad o dificultades de autenticación en redes Wi-Fi que utilizan los protocolos WPA o WPA2:

Sí: 30%

No: 70%

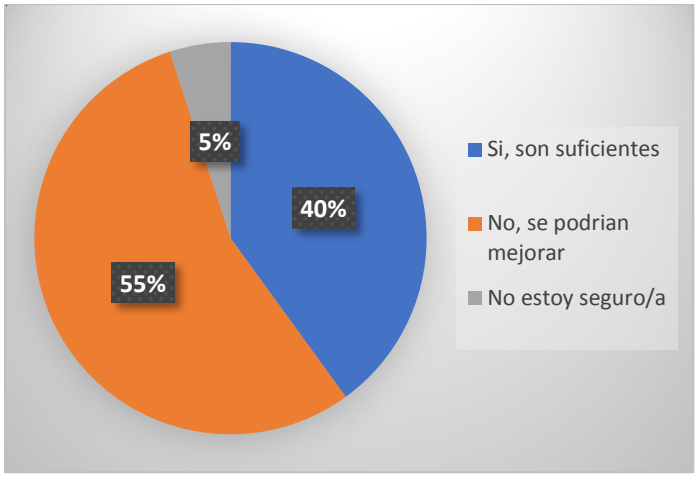


6.- Opinión sobre la suficiencia de los protocolos WPA y WPA2 para proteger la confidencialidad y la integridad de los datos transmitidos en redes Wi-Fi:

Sí, son suficientes: 40%

No, se podrían mejorar: 55%

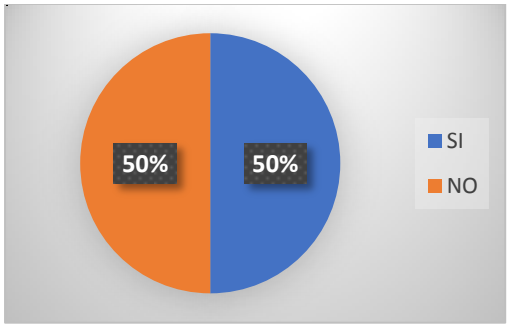
No estoy seguro/a: 5%



7.- Realización de configuraciones adicionales en dispositivos móviles para fortalecer la seguridad al utilizar los protocolos WPA o WPA2:

Sí: 50%

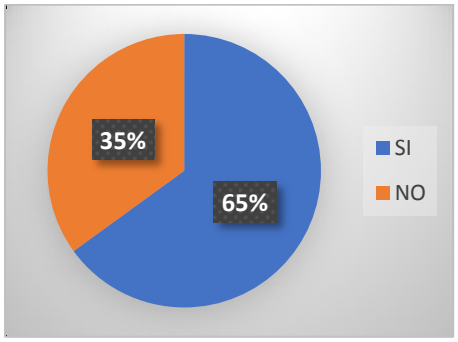
No: 50%



8.- Conocimiento de alguna vulnerabilidad conocida o incidente de seguridad relacionado con los protocolos WPA y WPA2 en dispositivos móviles:

Sí: 65%

No: 35%



9.- Aspectos más importantes que se deben considerar al utilizar los protocolos WPA y WPA2 en dispositivos móviles (respuestas abiertas):

Respuestas variadas que incluyen la elección de contraseñas seguras, actualización de firmware, configuración adecuada de autenticación y encriptación, y educación de los usuarios sobre la seguridad de las redes Wi-Fi.

Sugerencias o comentarios adicionales relacionados con los protocolos WPA y WPA2 en dispositivos móviles (respuestas abiertas):

Respuestas variadas que incluyen recomendaciones para mejorar la seguridad, como la implementación de autenticación de dos factores, actualizaciones regulares de seguridad, mayor conciencia sobre los riesgos de seguridad y la necesidad de medidas adicionales para proteger los datos.

Estos resultados proporcionan una visión general de la percepción y la experiencia de los usuarios de dispositivos móviles en relación con los protocolos de seguridad inalámbrica WPA y WPA2. Las respuestas reflejan una combinación de confianza en la seguridad de los protocolos, preocupaciones sobre posibles mejoras y la necesidad de configuraciones y medidas adicionales para fortalecer la protección de los datos transmitidos en redes Wi-Fi.