UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA ACADÉMICO PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

ANÁLISIS DE PROTOCOLOS DE PROTECCIÓN DE REDES INALÁMBRICAS WI-FI PARA LA DETECCIÓN DE VULNERABILIDADES FRENTE A POSIBLES ATAQUES QUE ATENTEN CONTRA LA SEGURIDAD DE LA INFORMACIÓN

PARA OPTAR EL TÍTULO PROFESIONAL

DE INGENIERO DE SISTEMAS

Autores:

Br. CARMEN LUCINDA TAFUR BARDALES

Br. JOSÉ LUIS CHÁVEZ MONTERO

Asesor:
Ing. CORONADO NAVARRO ALEX FRANKLIN

Línea de Investigación:

Tecnologías de la Información

Lima – Perú

2018

ANÁLISIS DE PROTOCOLOS DE PROTECCIÓN DE REDES INALÁMBRICAS WI-FI PARA LA DETECCIÓN DE VULNERABILIDADES FRENTE A POSIBLES ATAQUES QUE ATENTEN CONTRA LA SEGURIDAD DE LA INFORMACIÓN

Aprobación de la Tesis

Mg. Villegas Cubas Juan Elías

Presidente del jurado de tesis

Ing. Mejía Cabrera Heber Iván

Secretario del jurado de tesis

Mg. Bravo Ruiz Jaime Arturo

Vocal del jurado de tesis

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

DEDICATORIA

A mi Madre por todo el esfuerzo y sacrificio, por el compromiso y el apoyo incondicional, a mis hijos quienes hacen día a día que todo esfuerzo valga la pena.

A mis padres quienes son mi estímulo para seguir adelante, a mis hermanos por dar inicio a este peldaño de mi carrera.

AGRADECIMIENTO

A Dios por ser nuestra guía y fortaleza y por estar a mi lado a cada momento, a mi esposa por ayudarme con mis hijos mientras realizaba investigaciones.

A mi hermano por acompañarme en mis noches de desvelo y a mis amigos por su apoyo e impulsarme a terminar este proyecto.

Tabla de contenido

INTRODUCCIÓN 1
I. CAPITULO I: PROBLEMAS DE INVESTIGACIÓN 2
1.1. Situación problemática 2
1.2. Formulación del problema 3
1.3. Delimitación de la Investigación 3
1.4. Justificación e importancia 4
1.5. Limitaciones de la investigación 5
1.6. Objetivos 6
II. CAPITULO II: MARCO TEÓRICO 7
2.1. Antecedentes de Estudios 7
2.2. Estado del Arte 9
2.3. Bases teórico científicas 12
2.3.1. Redes Inalámbricas Wi-Fi 12
2.3.1.1. Concepto 12
2.3.1.2. Arquitectura de una Red Inalámbrica Wi-Fi 12
2.3.1.2.1. BSS (Basic Service Set) 12
2.3.1.2.2. ESS (Extended Service Set) 14
2.3.2. Protocolos de Protección y Seguridad 14
2.3.2.1. Concepto 14
2.3.2.2. Tipos de Protocolo 15
2.3.2.2.1. WEP 15
2.3.2.2.2. WPA 15
2.3.2.2.3. WPA2 16
2.4. Definición de términos básicos 17
III. CAPITULO III: MARCO METODOLÓGICO 25
3.1. Tipo y diseño de investigación 25
3.1.1. Tipo de Investigación 25
3.1.2. Diseño de Investigación 25
3.2. Población y muestra 25
3.3. Hipótesis 27
3.4. Variables 28
3.5. Operacionalización 28
3.6. Métodos, técnicas e instrumentos de recolección de datos 29

3.6.1. Métodos 29
3.6.2. Técnicas 30
3.6.3. Instrumentos de recolección de datos 30
3.7. Procedimiento para la recolección de datos 31
3.7.1. Uso de las Herramientas de Auditoría 31
3.7.1.1. Ataque de Fuerza Bruta (Contraseña) 31
3.7.1.2. Ataque de Denegación de Servicios (DoS) 37
3.7.2. Escenario de Pruebas 41
3.7.2.1. Escenario #1: Pruebas a nivel doméstico 41
3.7.2.2. Escenario #2: Pruebas a nivel corporativo 42
3.7.3. Pruebas realizadas en campo 43
3.8. Criterios Éticos 46
3.9. Criterios de rigor científico 46
IV. CAPITULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS 48
4.1. Análisis Estadístico e Interpretación de datos 48
4.1.1. Variable Independiente 48
4.1.2. Variable Dependiente 61
4.2. Discusión de Resultados 72
V. CAPITULO V: PROPUESTA DE INVESTIGACIÓN 74
5.1. Propuesta para Pequeñas Oficinas y Hogares (SOHO) 75
5.1.1. Usuario (Consideraciones) 76
5.1.2. Access Point (Consideraciones) 76
5.1.3. Protocolos de Seguridad (Consideraciones) 77
5.2. Propuesta EMPRESARIAL (Corporativa) 77
5.2.1. Políticas Generales Empresariales 78
5.2.2. Arquitectura de Red 80
5.2.3. Controlador de APs 83
5.2.4. Sistema de Prevención de Intrusos en Red Inalámbrica (WIPS) 83
5.2.5. Herramientas de Gestión 84
VI. CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES 85
CONCLUSIONES 85
RECOMENDACIONES 86
REFERENCIAS 87

Índice de Tablas

Tabla 1 Resumen de características de los estándares de seguridad Wi-Fi 16
Tabla 2 Población de protocolos de protección 26
Tabla 3 Población de vulnerabilidades en protocolos de protección 27
Tabla 4 Muestreo de vulnerabilidades de protocolos de protección 27
Tabla 5 Operacionalización Variable Independiente 28
Tabla 6 Operacionalización Variable Dependiente 28
Tabla 7 Pruebas de campo realizadas 43
Tabla 8 Pruebas de campo realizadas por tipo de ataque / protocolo 44
Tabla 9 Cuantificador de indicadores 48
Tabla 10 Escala Cualitativa de cuantificación de indicadores: Variable Independiente... 48
Tabla 11. Cifrado de Protocolos – Nivel Doméstico 49
Tabla 12. Cifrado de Protocolos – Nivel Corporativo 50
Tabla 13 Mecanismos de Entrega de Datos - Nivel Doméstico 52
Tabla 14 Mecanismos de Entrega de Datos - Nivel Corporativo 53
Tabla 15. Autorización – Nivel Doméstico 54
Tabla 16. Autorización – Nivel Corporativo 55
Tabla 17 Subtotales del Análisis de la Variable Independiente – Ambos Escenarios 58
Tabla 18 Sumatoria de Análisis de la Variable Independiente – Ambos Escenarios 58
Tabla 19 Porcentaje Total de Cada Protocolo Analizado 59
Tabla 20 Porcentaje por Protocolo de Variable Independiente 59
Tabla 21 Escala Cualitativa de cuantificación de indicadores: Variable Dependiente 61
Tabla 22 Confidencialidad - Nivel Doméstico 61
Tabla 23 Confidencialidad - Nivel Corporativo 62
Tabla 24 Integridad - Nivel Doméstico 64
Tabla 25 Integridad - Nivel Corporativo 65
Tabla 26 Autentificación - Nivel Doméstico 67
Tabla 27 Autentificación - Nivel Corporativo 68
Tabla 28 Subtotales del Análisis de la Variable Dependiente – Ambos Escenarios 70
Tabla 29 Sumatoria de Análisis de la Variable Dependiente – Ambos Escenarios 70
Tabla 30 Porcentaje Total de Cada Protocolo Analizado 71
Tabla 31 Porcentaje por Protocolo de Variable Dependiente 71

Índice de Figuras

Figura 1. Red Inalámbrica Ad-hoc 13
Figura 2. Red Inalámbrica Wi-Fi en Modo Infraestructura 13
Figura 3. Configuración ESS con Varios Puntos de Acceso 14
Figura 4. Herramientas de Auditoría usadas en el trabajo de campo 31
Figura 5. Ataque de Fuerza Bruta (paso 1) 31
Figura 6. Ataque de Fuerza Bruta (paso 2) 32
Figura 7. Ataque de Fuerza Bruta (paso 3) 32
Figura 8. Ataque de Fuerza Bruta (paso 4) 33
Figura 9. Ataque de Fuerza Bruta (paso 5) 34
Figura 10. Ataque de Fuerza Bruta (paso 6) 34
Figura 11. Ataque de Fuerza Bruta (paso 7) 35
Figura 12. Ataque de Fuerza Bruta (paso 8) 35
Figura 13. Ataque de Fuerza Bruta (paso 9) 36
Figura 14. Ataque de Fuerza Bruta (paso 10) 36
Figura 15. Ataque de Fuerza Bruta (paso 11) 37
Figura 16. Ataque DoS (paso 1) 37
Figura 17. Ataque DoS (paso 2) 38
Figura 18. Ataque DoS (paso 3) 38
Figura 19. Ataque DoS (paso 4a y 4b) 38
Figura 20. Ataque DoS (paso 5) 39
Figura 21. Ataque DoS (paso 6) 39
Figura 22. Ataque DoS (paso 7) 40
Figura 23. Ataque DoS (paso 8) 40
Figura 24. Ataque DoS (paso 9) 41
Figura 25. Escenario #1: Pruebas a nivel doméstico 42
Figura 26. Escenario #2: Pruebas a nivel corporativo 43
Figura 27. Pruebas de Campo Realizadas 44
Figura 28. Ataques Realizados por Tipo de Escenario 45
Figura 29. Ataque de Fuerza Bruta 45
Figura 30. Ataque de Denegación de Servicios 46
Figura 31. Cifrado de los Protocolos – Nivel Doméstico 49
Figura 32. Cifrado de los Protocolos – Nivel Corporativo 50
Figura 33. Mecanismos de Entrega de Datos – Nivel Doméstico 52
Figura 34. Mecanismos de Entrega de Datos – Nivel Corporativo 53

Figura 35. Autorización – Nivel Doméstico 55
Figura 36. Autorización – Nivel Corporativo 56
Figura 37. Porcentaje por Protocolo de Variable Independiente 60
Figura 38. Confidencialidad – Nivel Doméstico 62
Figura 39. Confidencialidad – Nivel Corporativo 63
Figura 40. Integridad – Nivel Doméstico 65
Figura 41. Integridad – Nivel Corporativo 66
Figura 42. Autentificación – Nivel Doméstico 67
Figura 43. Autentificación – Nivel Corporativo 68
Figura 44. Porcentaje por Protocolo de Variable Dependiente 72
Figura 45. Elementos de solución WPA2 ENT / EAP-TTLS 78
Figura 46. Arquitectura de Red Empresarial 81

RESUMEN

Las supuestas ventajas que ofrecen las tecnologías inalámbricas de red, han hecho que estas se difundan de una manera rápida y desmedida, los usuarios promedio no han observado los peligros a los que se encuentran expuestos al no contar con una conexión física. Este hecho ha promovido que extraños deseen intervenir dichas redes, obteniendo claves de acceso, realizando suplantaciones y negando servicios.

Este estudio busca aportar soluciones relacionados al problema de la inseguridad en el uso las redes inalámbricas Wi-Fi, frente a los ataques de extraños malintencionados. A fin de lograr el objetivo, se realizó un estudio del desempeño de los estándares de seguridad inalámbrica Wi-Fi mayormente usados, luego el análisis comparativo de sus vulnerabilidades en los estándares WEP, WPA y WPA2 PSK, WPA y WPA2 Empresarial en redes IEEE 802.11b, con el IEEE 802.1X-EAP-TTLS. Posteriormente se realizó una evaluación de las contramedidas de cara a los ataques relacionados a las vulnerabilidades halladas.

Al final del estudio se plantea una propuesta de diseño y configuración de una red inalámbrica segura, con los parámetros de protección que reportaron los resultados más óptimos en el acceso seguro a redes Wi-Fi.

Palabras Clave: Red Inalámbrica, Protocolo, Seguridad, Ataque, Vulnerabilidad

ABSTRACT

The supposed advantages offered by wireless network technologies, have made these spread quickly and unmeasured, average users have not observed the dangers that are exposed to not have a physical connection. This fact has encouraged strangers to wish to intervene in these networks, obtaining access codes, making impersonations and denying services.

This study seeks to provide solutions related to the problem of insecurity in the use of Wi-Fi wireless networks, against the attacks of malicious strangers. In order to achieve the objective, a study of the performance of the wireless security standards most widely used has carried out, then the comparative analysis of their vulnerabilities in the WEP, WPA and WPA2 PSK, WPA and WPA2 Enterprise standards in IEEE 802.11b networks, with the IEEE 802.1X-EAP-TTLS. Subsequently an evaluation of the countermeasures was made in order to face the attacks related to the vulnerabilities found.

At the end of the study a proposal of design and configuration of a secure wireless network is proposed, with the protection parameters that reported the most optimal results in the secure access to Wi-Fi networks.

Key Words: Wireless Network, Protocol, Security, Attack, Vulnerability

INTRODUCCIÓN

Las redes inalámbricas y de manera particular las de acceso local Wi-Fi, proveen características especiales de uso que se manifiestan en la forma de conectarse, la portabilidad, el golpe visual en cuanto a las instalaciones y los bajos costos de implementación en infraestructura. Sin embargo, estas no son tan seguras como las redes cableadas, las cuales se recomiendan para cualquier organización. Monsalve, J., Aponte, F., Chaparro, F., (2015), Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia. *DYNA, 82 (189), 226-232,* doi: https://doi.org/10.15446/dyna.v82n189.43259, así lo menciona.

Existen distintos métodos que permiten garantizar la seguridad de las redes inalámbricas Wi-Fi. Las alternativas de mayor uso son la implementación de mecanismos de seguridad de datos, estos mecanismos se diseñaron específicamente para los protocolos de redes Wi-Fi como el WEP y el WPA. Ellos brindan seguridad en las distintas fases de autenticación, integridad y confidencialidad, implementados directamente por los mismos dispositivos inalámbricos. Giménez, J. (2014). *Seguridad en equipos informáticos***.** Madrid, España: IC Editorial.

Esta investigación fue realizada con el fin de demostrar de forma teórico – práctica las vulnerabilidades más resaltantes de los cifrados en los protocolos WEP, WPA y WPA2, de esta manera contribuir con los usuarios domésticos y administradores de redes inalámbricas Wi-Fi a que protejan sus redes con mayor eficacia.

I. CAPITULO I: PROBLEMAS DE INVESTIGACIÓN

1.1. Situación problemática

Los nuevos estilos de vida acelerados y dependientes de conexión tecnológica han llevado a cambiar las formas de comunicación con un uso excesivo de dispositivos móviles y un aumento en la necesidad de conexión a redes inalámbricas Wi-Fi. El uso de estas redes tiene como principal característica la flexibilidad de uso, proveniente de la no conectividad física y el ahorro en los costos a comparación de las redes cableadas, sin embargo, estas redes están expuestas a interferencias y errores debido al tipo de bandas de frecuencia libre utilizadas, Monsalve, J., Aponte, F., Chaparro, F., (2015), Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia. *DYNA, 82 (189), 226-232,* doi: https://doi.org/10.15446/dyna.v82n189.43259, así lo menciona.

Desafortunadamente a causa del auge que han tenido las redes inalámbricas Wi-Fi, sus mecanismos de seguridad se han visto superados por usuarios no autorizados, como son los Hackers de sombrero negro y/o Crackers y otros quienes descubren la vulnerabilidad de estos sistemas.

Por otro lado, Giménez, J. (2014). *Seguridad en equipos informáticos***.** Madrid, España: IC Editorial, menciona que es una realidad que los atacantes a los sistemas inalámbricos van creciendo en número y cada vez están mejor organizados y con mayores habilidades, es por ello que se han venido desarrollando diversas estrategias para intentar minimizar las intrusiones. Sin embargo, el problema de las medidas de seguridad en las redes va en aumento.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

1.2. Formulación del problema

Habiendo analizado la situación problemática actual se formuló el siguiente problema de manera interrogativa: ¿Cómo Detectar Vulnerabilidades Frente a Posibles Ataques que Atenten contra la Seguridad de la Información a través del Análisis de Protocolos de Protección de Redes Inalámbricas Wi-Fi?

1.3. Delimitación de la Investigación

Una red inalámbrica es la interconexión de distintos dispositivos con la capacidad de compartir información entre ellos, sin hacer uso de un medio físico de transmisión. Estos dispositivos pueden ser de formas y tecnologías, entre las cuales se encuentran, las ondas de radio, las microondas, los rayos láser, infrarrojo, Bluetooth y la tecnología Wi-Fi (Wireless Fidelity) que traducido literalmente al español es Fidelidad Sin Cables.

Esta investigación se circunscribe y limita básicamente a esta última tecnología en redes inalámbricas Wi-Fi, la misma que consiste en la transmisión por medio de ondas de radio con muy buena calidad de emisión para distancias cortas (teóricamente hasta 100 m).

Dentro del marco de esta tecnología de red inalámbrica, se tratarán muy rápidamente los temas de componentes, configuraciones básicas, estándares y otros, para centrarse de manera especial en los Protocolos de Protección: WEP, WPA y WPA2, que constituyen los tópicos objeto de este estudio.

1.4. Justificación e importancia

Debido al incremento en la diversidad de ataques a los cuales vienen siendo víctimas los usuarios de redes inalámbricas Wi-Fi y a la manifiesta vulnerabilidad de las mismas, es que la presente propuesta de investigación tiene como propósito, indagar acerca de las vulnerabilidades que se presentan en los protocolos de seguridad de redes inalámbricas Wi-Fi, a fin de advertir sobre los mencionados ataques e intrusiones de terceros cuya finalidad es atentar contra la seguridad de la información.

Justificación Académica:

La presente investigación devendrá en la obtención de nuevos conocimientos en el aseguramiento de la información y administración de redes inalámbricas Wi-Fi, las mismas que podrán servir de base para desarrollar estudios posteriores.

Relevancia Social:

Esta investigación tendrá una importante relevancia social, toda vez que los usuarios de redes inalámbricas Wi-Fi domésticas se verán beneficiados con nueva tecnología, más segura y libre de intrusiones malintencionadas. Entre los usuarios corporativos beneficiados se encuentra el personal de seguridad de la información y los administradores de redes.

Justificación Tecnológica:

El aporte tecnológico consistirá en la definición de nuevos parámetros de configuración de redes inalámbricas Wi-Fi, más seguras frente a los ataques e intrusiones.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Implicancias Prácticas:

La investigación aportará soluciones prácticas en las eventuales configuraciones de redes inalámbricas Wi-Fi, coadyuvando directamente en la solución del problema de la inseguridad de la información, minimizando y evitando los ataques malintencionados.

En respuesta a la problemática encontrada en este contexto se presenta como propuesta de investigación, el Análisis de Protocolos de Protección y Mecanismos de Seguridad en Redes Inalámbricas Wi-Fi y su Vulnerabilidad frente a Ataques Externos.

1.5. Limitaciones de la investigación

La principal limitación que se presentó durante la elaboración de este proyecto de investigación ha sido la escasa o prácticamente nula bibliografía local acerca del tema en cuestión, no se encontraron trabajos similares previos en el banco de libros de la Universidad Señor de Sipán ni en otras del país, esto hubiera brindado una visión del tema acorde a la realidad peruana. Afortunadamente esto fue suplido con información del exterior.

Otra limitación a considerar es el presupuesto, ya que este proyecto es autofinanciado y podría ser insuficiente al aparecer gastos imprevistos que no se hayan contemplado.

El acceso a técnicas y materiales para abordar ciertos tópicos muy especializados de la investigación podrían constituirse en otra limitación, dada la escasa bibliografía local a consultar y la poca experiencia en el tema.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

1.6. Objetivos

Objetivo general:

Analizar los protocolos de protección de redes inalámbricas Wi-Fi, a fin de minimizar las vulnerabilidades frente a posibles ataques que atenten contra la seguridad de la información

Objetivos específicos

OE1. Analizar las tecnologías de seguridad en redes inalámbricas Wi-Fi.

OE2. Realizar un análisis comparativo de la vulnerabilidad de los diferentes protocolos de seguridad inalámbrica Wi-Fi.

OE3. Comprobar cuan vulnerables pueden ser los protocolos de seguridad.

OE4. Plantear el diseño de una configuración de red inalámbrica Wi-Fi segura.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

II. CAPITULO II: MARCO TEÓRICO

2.1. Antecedentes de Estudios

Se encontró una investigación desarrollada por Begoña L. (2012). *Seguridad en Comunicaciones Sin Hilo: Riesgos y Amenazas Wi-Fi* (tesis de pregrado). Universitat Oberta de Catalunya, España; en la cual utiliza la Metodología Analítica e Inductiva, haciendo uso de diversos softwares de intrusión (los cuales se pueden adquirir libremente en el mercado) demostrando la vulnerabilidad real de las redes inalámbricas Wi-Fi. Los resultados de estas prácticas de ataques e intrusiones fueron exitosos y se concluye que los protocolos de protección de redes inalámbricas Wi-Fi son efectivamente vulnerables. Sus recomendaciones fueron la implementación urgente de mejoras en las políticas de seguridad de la información.

La investigación de Begoña se relaciona con esta investigación en que ambas buscan demostrar las vulnerabilidades en las redes inalámbricas Wi-Fi a través de diversos mecanismos informáticos. El aporte ofrecido fue demostrar que efectivamente las redes inalámbricas Wi-Fi son vulnerables y se requieren de mejores políticas de seguridad de la información.

De igual manera Suarez, M. (2012). *Mecanismos De Seguridad En Redes Inalámbricas.* México; analiza los diferentes protocolos de protección en redes inalámbricas Wi-Fi, concluyendo que existen vulnerabilidades en cada una de ellas. Finalmente recomienda realizar un filtrado de acceso a la red mediante direcciones MAC, aunque reconoce que esta técnica no es 100% segura, ya que en la actualidad existen técnicas de clonación de direcciones MAC.

Esta investigación guarda relación con el planteamiento presentado en el sentido que Suarez realiza un análisis de los diferentes protocolos de protección,

en busca de posibles debilidades. El aporte encontrado en esta investigación radica en el hallazgo de un mecanismo de seguridad a través del control de acceso al medio (MAC)

Ruz, J., Riveros, B., Varas, A., (2012) Redes WPA/WPA2. Chile; realiza una introducción a los protocolos de seguridad más seguros en la actualidad, y haciendo uso de la metodología analítica y valiéndose de herramientas de Auditoría Wireless, permite observar las ventajas de los protocolos de seguridad estudiados, así también sus vulnerabilidades. Concluyendo que el tema de la seguridad en redes es un campo donde queda mucho camino por recorrer y que no existe la seguridad absoluta.

Los objetivos de la presente investigación se relacionan directamente con el análisis de los protocolos realizado por Javier Ruz Maleunda et al, los cuales fueron los más seguros en su tiempo. Su aporte consistió en la declaración de que el tema de la seguridad en redes es un campo muy amplio de investigación.

Por otra parte en el artículo del DYNA: Monsalve, J., Aponte, F., Chaparro, F., (2015), Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia. *DYNA, 82 (189), 226-232,* doi: https://doi.org/10.15446/dyna.v82n189.43259, de manera inductiva, aplica diversas técnicas como Warchalking y Wardriving, a fin de demostrar la vulnerabilidad de las redes Wireless. Identificó que más del 30% de las redes inalámbricas encontradas en su estudio presentan autenticación WEP lo cual indica que son vulnerables a ser atacadas.

El uso de la técnica de Wardriving *como herramientas de análisis en la investigación de Julián Mosalve-Pulido tiene relación con el presente estudio, ya*

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

que de igual modo se hará uso de técnicas poco ortodoxas para comprobar vulnerabilidades en las redes inalámbricas Wi-Fi, ya que hoy en día se pueden realizar auditorías Wi-Fi hasta con smartphones y tablets, y existen adaptadores Wi-Fi USB especialmente aptos para este tipo de propósitos. El aporte de Monsalve-Pulido radica en dar a conocer la proliferación de WEP y lo vulnerable que este resulta ser, además de evidenciar malas prácticas en las configuraciones realizadas por los administradores de red y/o los proveedores de servicios de internet.

2.2. Estado del Arte

Las redes inalámbricas Wi-Fi deben su aparición a la necesidad de brindar acceso a red a dispositivos de cómputo primordialmente portátiles, bien es cierto que una de sus mayores ventajas es definitivamente el bajo costo de implementación, ya que se elimina el cableado Ethernet y demás conexiones físicas, sin embargo, emerge una gran desventaja: El Sistema de Seguridad, el cual debe ser mucho más robusto a fin de evitar intrusiones y ataques mal intencionados.

Desafortunadamente a causa del auge que han tenido las redes inalámbricas Wi-Fi, sus mecanismos de seguridad se han visto superados por usuarios no autorizados, como son los Hackers de sombrero negro y/o Crackers y otros quienes descubren la vulnerabilidad de estos sistemas.

Vano, M., Piessens F., (2017), Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Recuperado de: https://papers.mathyvanhoef.com/ccs2017.pdf, del Grupo de Investigación de la Imec-DistriNet, Katholieke Universiteit Leuven,

revelaron una debilidad grave en el protocolo WPA2 que permite a los atacantes dentro del alcance del dispositivo vulnerable o punto de acceso, interceptar contraseñas, correos electrónicos y otros datos presuntamente encriptados, y en algunos casos, inyectar ransomware u otro contenido malicioso en un sitio web que un cliente esté visitando. Esto se ejecuta cuando el cliente quiere unirse a una red Wi-Fi protegida y confirma que tiene las credenciales correctas para conectarse. En este ataque, el atacante consigue que la víctima vuelva a utilizar una clave que ya está en uso. Esto se consigue mediante la manipulación y el reemplazo de los mensajes cifrados del "handshake".

Gutiérrez, M. (2012). Mecanismos De Seguridad En Redes Inalámbricas. México, en su artículo para la Universidad Veracruzana, menciona que organizaciones como la IEEE (Institute of Electrical and Electronics Engineers) y la Wi-Fi Alliance, comenzaron a buscar alternativas de solución a los problemas de inseguridad en las redes inalámbricas Wi-Fi, dando como resultado los protocolos de protección: WEP (Wired Equivalent Privacy) en el 1999, WPA (Wi-Fi Protected Access) en el 2003 y WPA2 (Wi-Fi Protected Access II) en el 2006.

La PHYS ORG. (2014). WPA2 wireless security cracked. Inderscience Publishers. Recuperado de: http://phys.org/news/2014-03-wpa2-wireless.html, indica, como se mencionó anteriormente, que existen varias maneras de proteger una red inalámbrica Wi-Fi y que unas son consideradas más seguras que otras. Algunas como WEP (Wired Equivalent Privacy) fueron "quebradas" años atrás y ya no son más recomendadas como una medida de mantener alejados a los intrusos de las redes privadas.

Una mejora sustancial de WPA con respecto a WEP, según: Iniesta M., (2010). *Seguridad WI-FI. Agresiones posibles* (tesis de pregrado) Universidad Politécnica de Valencia. España, fue la implementación de un Servidor AAA (Authentication Authorization Accounting), como son los servidores RADIUS (Remote Authentication Dial-In User Service) el cual se encarga de autentificar la entrada de un nuevo cliente a la red. La idea principal es que este servidor RADIUS contenga la información de todos los usuarios y de existir algún cambio, sea preciso realizar los cambios en el, olvidándose del Access Point para las tareas administrativas. Esta solución requiere de una mayor infraestructura y se aplica comúnmente en ambientes empresariales.

Un estudio publicado en la International Journal of Information and Computer Security, revela que uno de los más fuertes sistemas de seguridad, Wi-Fi Protected Access 2 (WPA2) puede también ser fácilmente quebrada en redes locales inalámbricas Wi-Fi (WLANs).

El artículo científico publicado en InderScience Publisher, por Tsitroulis, A., Lampoudis D., Tsekleves. E., (2014). Exposing WPA2 security protocol vulnerabilities**.** *Int. J. Information and Computer Security*, 82 (6) 93-107. DOI: 10.1504/IJICS.2014.059797, informan que los autores, han investigado las vulnerabilidades en WPA2 y presentan sus debilidades. Informan que este sistema de seguridad podría ser violado con relativa facilidad por ataques malintencionados en una red. Sugieren que, en una cuestión de urgencia, que los expertos en seguridad y programadores trabajen juntos para eliminar las vulnerabilidades en WPA2 con el fin de reforzar su seguridad o para desarrollar protocolos alternativos a fin de mantener nuestras redes inalámbricas Wi-Fi a salvo de hackers.

2.3. Bases teórico científicas

2.3.1. Redes Inalámbricas Wi-Fi

2.3.1.1. Concepto

Moreno, J., Santos, M. (2014). Sistemas Informáticos y Redes Locales. España, también conocidas como WLAN (Wireless LAN), redes de área local que permiten la conexión de un equipo a una red sin la necesidad de una infraestructura, estas redes utilizan ondas electromagnéticas para la transmisión de datos. La proliferación de dispositivos móviles con grandes capacidades de conectividad hoy en día ha aumentado la demanda de este tipo de redes.

2.3.1.2. Arquitectura de una Red Inalámbrica Wi-Fi

Moreno, J., Santos, M. (2014). Sistemas Informáticos y Redes Locales. España, contempla dos posibles configuraciones mediante las cuales se puede interconectar dispositivos en una red inalámbrica Wi-Fi, BSS y ESS, explicando su funcionamiento en los siguientes apartados.

2.3.1.2.1. BSS (Basic Service Set)

Esta configuración es utilizada para crear redes inalámbricas Wi-Fi con un área de cobertura simple y número limitado de equipos, soporta dos modos de operación Ad-hoc e Infraestructura, el primer modo de operación es conocido como IBSS (Independent Basic Service Set), este modo establece la conexión inalámbrica compuesta por dos equipos o más sin grandes exigencias de cobertura. Por otro lado, Infraestructura, modo mejorado al anterior, basa su funcionamiento en el uso de un dispositivo denominado

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Punto de Acceso o AP (Access Point). Este dispositivo permite la conexión de una red cableada con una red inalámbrica Wi-Fi permitiendo la mayor cantidad de dispositivos conectados con una mayor cobertura que el modo ad-hoc.

Figura 1. Red Inalámbrica Ad-hoc.

Fuente: Adaptado de https://bit.ly/2EMoIMK

Figura 2. Red Inalámbrica Wi-Fi en Modo Infraestructura

Fuente: Adaptado de https://bit.ly/2IQusrd

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2.3.1.2.2. ESS (Extended Service Set)

Configuración utilizada cuando se requiere mayor alcance en la red inalámbrica Wi-Fi, hace uso de Puntos de Acceso permitiendo la conexión de red cableada con una red inalámbrica Wi-Fi, la principal función de esta configuración es ampliar la cobertura de una red inalámbrica Wi-Fi haciendo uso de varios Puntos de Acceso.

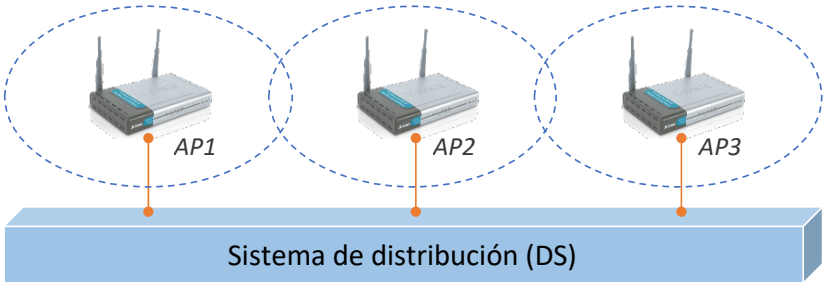

Figura 3. Configuración ESS con Varios Puntos de Acceso

Fuente: Adaptado de https://bit.ly/2IQusrd

2.3.2. Protocolos de Protección y Seguridad

2.3.2.1. Concepto

Moreno, J., Santos, M. (2014). Sistemas Informáticos y Redes Locales. España, indica que "Es evidente que uno de los factores que más importancia tienen cuando se decide utilizar o implementar una red inalámbrica Wi-Fi es la seguridad. Esto es así porque, a diferencia de lo que ocurre en las redes cableadas, los datos transferidos a través de redes inalámbricas Wi-Fi utilizan un medio de comunicación que no está restringido, como es el aire. El mecanismo estándar de seguridad en Wi-Fi incluye tanto la autenticación de la conexión como el cifrado de los datos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Actualmente, los dispositivos Wi-Fi se pueden configurar con varios mecanismos o protocolos de seguridad".

2.3.2.2. Tipos de Protocolo

2.3.2.2.1. WEP

"El mecanismo de seguridad inicialmente especificados en el estándar 802.11 es WEP (Wired Equivalent Privacy, Privacidad equivalente al cable). Este mecanismo está considerado actualmente como poco robusto y relativamente fácil de romper, por lo que actualmente no se aconseja su uso". "Para utilizar WEP es necesario configurar, tanto en el punto de acceso como en los dispositivos de la red, una clave de autenticación común para todos ellos. Esta clave admite dos formatos: El formato corto, que pueden ser de 10 caracteres hexadecimales o 5 caracteres alfanuméricos. El valor obtenido será de 40 bits en ambos casos. Y el formato largo, que pueden ser de 26 caracteres hexadecimales o 13 caracteres alfanuméricos. El valor obtenido será de 104 bits". "La clave o contraseña de validación se utiliza junto con un vector de inicialización de 24 bits para generar la clave de encriptación, que será de 64 o 128 bits".

2.3.2.2.2. WPA

"La WPA (Wi-Fi Protected Access, Acceso protegido Wi-Fi) utiliza un nuevo protocolo de seguridad llamado TKIP (Temporal Key Intergrity Protocol), que es el mismo que se utiliza en el estándar IEEE 802.11i. Este sistema también utiliza claves simétricas con el algoritmo RC4, pero para añadir protección adicional, TKIP genera claves temporales que son cambiadas de forma

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

dinámica. Corrige fallos de seguridad y añade algunas mejoras más respecto a WEP, por ejemplo, usa un vector de iniciación de 48 bits en lugar de los 24 utilizados en WEP.

En WPA se contemplan los siguientes algoritmos de autenticación:

WPA-Enterprise: donde la autenticación se realiza por medio de un servidor de autenticación (tipo RADIUS), normalmente esta solución se implementa en escenarios corporativos.

WPA-PSK (WPA Pre-Shared Key): Se realiza por medio de una clave pre compartida, este tipo de solución tiene menos restricciones y es usada en ambientes caseros. La contraseña comúnmente solicitada es de tipo alfanumérica de entre 8 a 63 caracteres teniendo un valor de 256 bits.

2.3.2.2.3. WPA2

"En 2004 se publica el estándar IEEE 802.11i al que también se le conoce como WPA2. Uno de los principales cambios es la utilización de AES (Advanced Encryption Standard, Estándar de encriptación avanzado) en lugar de usar RC4, aunque el uso de este estándar implica un cambio del hardware utilizado. Incluye además el uso de IEEE 802.1x con todas las características de WPA".

Tabla 1
Resumen de características de los estándares de seguridad Wi-Fi

Estándar	Protocolo de seguridad	Encriptación	Autenticación
IEEE 802.11	WEP	RC4	No hay
WPA (Wi-Fi Alliance)	TKIP	RC4	IEEE 802.1x (EAP)
WPA2 (IEEE 802.11i)	TKIP	AES	IEEE 802.1x (EAP)

Datos obtenidos de diversas fuentes (elaboración propia)

2.4. Definición de términos básicos

ACL (Access Control List): Una Lista de Control de Acceso es un concepto de seguridad informática usado para fomentar la separación de privilegios. Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. (Álvarez, 2009)

AES (Advanced Encryption Standard). También conocido como Rijndael (pronunciado "Rain Doll" en inglés), es un esquema de cifrado por bloques adoptado como un estándar de cifrado por el gobierno de los Estados Unidos. Es uno de los algoritmos más seguros y más utilizados hoy en día disponible para uso público. (González, 2018)

Algoritmo Simétrico. También llamada criptografía de clave secreta o criptografía de una clave, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. (De Luz, 2010)

AP (Access Point): Es un dispositivo de red que interconecta equipos de comunicación inalámbricos, para formar una red inalámbrica que interconecta dispositivos móviles o tarjetas de red inalámbricas. (Castillos, 2016)

Ataque de Contraseña – Diccionario. Consiste en intentar averiguar una contraseña probando todas las palabras de un diccionario. Este tipo de ataque suele ser más eficiente que un ataque de fuerza bruta. (Vivancos, 2013)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Ataque de Contraseña - Fuerza Bruta. Forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permita el acceso. (Oncina, 2013)

Ataque de Fragmentación. Técnica que le permite a un atacante generar e inyectar paquetes cifrados en una red WEP sin la necesidad de conocer la clave, solamente es necesario capturar un paquete cifrado en la red y posteriormente aplicar este ataque. (Vila, 2017)

Ataque DoS (Denial of Service). Ataque de Denegación Servicios, consiste en inundar de tráfico un sistema o una red hasta que no sea capaz de dar servicio a usuarios legítimos. (Vila, 2017)

Ataque por Inducción – Chop Chop. Este ataque intercepta un paquete de datos cifrados con la clave WEP y decrementándolo iterativamente byte a byte (con fuerza bruta), se obtiene el contenido del paquete. (López, 2013)

BSS (Basic Service Set). Configuración utilizada para crear redes inalámbricas Wi-Fi con un área de cobertura simple y número limitado de equipos. Soporta los modos Ad-Hoc e Infraestructura. (Gonzáles, 2014)

CCMP o CCM. Son las siglas de Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, también conocido como AES CCMP, y es el mecanismo de cifrado actual que sustituye a TKIP y el estándar definido para su uso con WPA2. (Oltra, 2010)

Cracker y Hacker. Los hackers y crackers son individuos de la sociedad moderna que poseen conocimientos avanzados en el área tecnológica e informática, pero la

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

diferencia básica entre ellos es que los hackers solamente construyen cosas para el bien y los crackers destruyen. (Bastidas, 2013)

CRC (Verificación por Redundancia Cíclica). Es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos. (Cuadrado y Artega, 2016)

DMZ (Zona Desmilitarizada): Es una zona insegura que se ubica entre la red interna de una organización y una red externa, generalmente en Internet. (Camacho, 2014)

EAP (Extensible Authentication Protocol). Es un framework de autenticación frecuentemente usado en redes inalámbricas y conexiones point-to-point. (Oltra, 2010).

EAPoL (Extensible Authentication Protocol over LAN). Is a network port authentication protocol used in IEEE 802.1X (Port Based Network Access Control) developed to give a generic network sign-on to access network resources (Ulloa y Fonseca, 2012)

EAP-TLS (Transport Layer Security). En un método de autenticación IETF (Internet Engineering Task Force) estandarizado, basado en el mismo protocolo usado para seguridad de tráfico Web vía protocolo SSL (Secure Sockets Layer). (Ulloa y Fonseca, 2012)

EAP-TTLS. El sistema de autenticación se basa en una identificación de un usuario y contraseña que se transmiten cifrados mediante TLS, para evitar su transmisión en texto limpio. Es decir se crea un túnel mediante TLS para transmitir el nombre

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

de usuario y la contraseña. A diferencia de EAP-TLS sólo requiere un certificado de servidor. (Ulloa y Fonseca, 2012)

ESS (Extended Service Set). Hace uso de Puntos de Acceso permitiendo la conexión de red cableada con una red inalámbrica Wi-Fi, la principal función de esta configuración es ampliar la cobertura de una red inalámbrica Wi-Fi haciendo uso de varios Puntos de Acceso. (Gómez, 2010)

IBSS (Independent BSS). También conocido como modo ad-hoc, se ha diseñado para facilitar las conexiones punto a punto. (Gómez, 2010)

ICV (Integrity Check Value). Es el resultado del proceso de integridad. Esto normalmente implica el algoritmo HMAC (Hash Message Authentication Code) y las funciones MD5 (Message Digest 5) o SHA-1. (Muñoz y Romero, 2010)

IEEE 802.11. Estándar que define el uso de los dos niveles inferiores de la arquitectura o modelo OSI (capa física y capa de enlace de datos), especificando sus normas de funcionamiento en una red de área local inalámbrica (WLAN). (Retamal, 2015)

IV (Initialization Vector). Vector de inicialización es un bloque de bits que es requerido para permitir un cifrado en flujo o un cifrado por bloques, en uno de los modos de cifrado, con un resultado independiente de otros cifrados producidos por la misma clave. (Sanz, 2016)

MAC. En las redes de computadoras, la dirección MAC (siglas en inglés de media access control; en español "control de acceso al medio") es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

dispositivo de red. Se conoce también como dirección física, y es única para cada dispositivo. (Gonzáles, 2014)

MIC o Algoritmo Michael. WPA implementa un código de integridad del mensaje (MIC - Message Integrity Code), también conocido como "Michael". (Ulloa y Fonseca, 2012)

Modo Ad-Hoc (peer-to-peer). Una red ad hoc es una conexión temporal entre equipos y dispositivos usada para un fin específico como, por ejemplo, compartir documentos durante una reunión o participar en juegos informáticos de varios jugadores. (Porras, 2017)

Modo Infraestructura. Es una red tipo cliente-servidor, donde los clientes suelen ser los ordenadores personales que se conectan al servidor, llamado punto de acceso en este caso. (Porras, 2017)

Protocolo AAA. Corresponde a un tipo de protocolos que realizan tres funciones: autenticación, autorización y registro (en inglés, Authentication, Authorization and Accounting). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados. (Muñoz, 2015)

RC4. Es el sistema de cifrado de flujo Stream cipher y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). (Navas, 2016)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

RFC (Request for Comments). Son una serie de publicaciones del grupo de trabajo de ingeniería de internet (IETF)que describen diversos aspectos del funcionamiento de Internet y otras redes de computadoras, como protocolos, procedimientos, etc. y comentarios e ideas sobre estos. (Rodríguez, 2015)

Servidor DHCP (Dynamic Host Configuration Protocol). Conjunto de reglas y normas que permite que los clientes de una red IP obtengan de manera automática sus parámetros de configuración. Por tanto, el servidor DHCP es el que se encarga de asignar datos de configuración IP a los equipos que se conectan a la red. (Ramírez, 2017)

Servidor RADIUS (Remote Authentication Dial-In User Server). Protocolo que permite gestionar la "autenticación, autorización y registro (cuentas)" de usuarios remotos sobre un determinado recurso. (Ulloa y Fonseca, 2012)

SOHO (Small Office, Home Office): es una red de área local pensada para ser utilizada en oficinas pequeñas. Una de las particularidades de este tipo de redes es que tienen un número reducido de ordenadores conectados a ella. (Quiroga, 2018)

SSH (Secure Shell). Es un protocolo que facilita las comunicaciones seguras entre dos sistemas usando una arquitectura cliente/servidor y que permite a los usuarios conectarse a un host remotamente. A diferencia de otros protocolos de comunicación remota tales como FTP o Telnet, SSH encripta la sesión de conexión, haciendo imposible que alguien pueda obtener contraseñas no encriptadas. (Bernal, 2015)

SSID (Service Set Identifier). Es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un

máximo de 32 caracteres, que la mayoría de las veces son alfanuméricos (aunque el estándar no lo específica, así que puede consistir en cualquier carácter). Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID. (Pari, 2010)

SSL (Secure Sockets Layer) y TLS (Transport Layer Security). Son los protocolos de seguridad de uso común que establecen un canal seguro entre dos ordenadores conectados a través de Internet o de una red interna. (Hernández, 2015)

Suplicante: Cliente que pide acceder a la red. (Ricciardi, 2012)

TKIP (Temporal Key Integrity Protocol). Es también llamado hashing de clave WEP WPA, incluye mecanismos del estándar emergente 802.11i para mejorar el cifrado de datos inalámbricos. (Oltra, 2010)

TTLS (Tunneled TLS). TTLS utiliza el canal TLS para el intercambio de "pares atributo-valor" (AVPs), tanto como RADIUS. (Vaca, 2014)

WEP. Acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. (Oltra, 2010)

Wi-Fi. Organización que certifica la interoperabilidad de dispositivos 802.11 como un estándar compatible y global de redes WLAN. (Espinosa, 2013)

WIPS (Wireless Intrusion Prevention System). Sistema de Prevención de Intrusiones Inalámbricas, es un hardware de red que supervisa el espectro

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

radioeléctrico para detectar la presencia de puntos de acceso no autorizados (detección de intrusión) y para tomar contramedidas (prevención de intrusos) automáticamente. (Santos, 2017)

WLAN: Red de Área Local Inalámbrica. (Espinosa, 2013)

WPA. Wi-Fi Protected Access, llamado también WPA (en español «Acceso Wi-Fi protegido») es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo, Wired Equivalent Privacy (WEP). (Muñoz y Romero, 2010)

XOR. En criptografía, el cifrado XOR es, como su nombre indica, un algoritmo de cifrado basado en el operador binario XOR. (García, 2011)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

III. CAPITULO III: MARCO METODOLÓGICO

3.1. Tipo y diseño de investigación

3.1.1. Tipo de Investigación

Por la propia naturaleza del presente caso, el tipo de investigación a realizarse es el comparativo, así también el tecnológico, ya que se hará uso del conocimiento existente para realizar un estudio comparativo de los mecanismos de protección, a fin de encontrar la tecnología más segura en cuanto a protocolos de seguridad en redes Wi-Fi se refiere.

3.1.2. Diseño de Investigación

El diseño de la presente investigación es cuasi experimental, dado que no habrá asignación aleatoria de los sujetos o grupo de sujetos de estudio. Los parámetros y protocolos de seguridad no contemplan ser elegidos al azar, más bien serán definidos con anterioridad para las pruebas de campo.

3.2. Población y muestra

La población es el conjunto de todos los elementos a los cuales está referida la investigación, es decir es el conjunto de todas las unidades de muestreo. El estudio propuesto busca indagar acerca de las debilidades existentes en los protocolos de seguridad en redes inalámbricas Wi-Fi, por ello se definen los siguientes aspectos:

Protocolos de seguridad

Los protocolos de seguridad en redes inalámbricas Wi-Fi que conforman la población a estudiar son las WEP, WPA y WPA2, las mismas que han sido extraídas de los estándares IEEE 802.11 y la Wi-Fi Alliance. Los parámetros seleccionados para el análisis comparativo de los protocolos de seguridad en el presente estudio están relacionados con la Autenticación y el Cifrado.

Tabla 2
Población de protocolos de protección

		WEP	WPA	WPA2
Autenticación	Autenticación	WEP	802.1X + EAP	802.1X + EAP
	Pre-autenticación	No	No	802.1X (EAPOL)
Cifrado	Negación del cifrado	No	Si	Si
	Cifrado	RC4 40-bit o 104-bit	TKIP: RC4 128-bit	CCMP: AES 128-bit
	Vector de inicialización	24 bits	48 bits	48 bits
	Integridad de cabecera	No	MIC	CCM
	Integridad de datos	CRC-32	MIC	CCM
	Protección de respuesta	No	Fuerza secuencia de IV	Fuerza secuencia de IV
	Gestión de clave	No	Basada en EAP	Basada en EAP
	Distribución de clave	Manual	802.1X (EAP)	802.1X (EAP)
	Clave asignada a:	Red	Paquete, session y usuario	Paquete, session y usuario
	Clave por paquete	Concatenación de IV	Mezclado TKIP	No necesario
Otros	Seguridad ad-hoc	No	No	Si (IBSS)

Datos extraídos de la NIST (elaboración propia)

Vulnerabilidades

IEEE 802.11 contempla los siguientes servicios de seguridad en el ámbito de las redes inalámbricas Wi-Fi: Autenticación, Confidencialidad e Integridad.

Tabla 3
Población de vulnerabilidades en protocolos de protección

Servicio	Vulnerabilidad
Autenticación	Shared Key Adivinar, PSK Cracking, Robo de aplicación Login, Inicio de sesión de dominio Cracking, VPN Login Cracking 802.1X, robo de identidad, Adivinar contraseña LEAP 802.1x, Cracking802.1X, fragmentación e inyección
Confidencialidad	Espionaje, Clave WEP, Evil Twin AP, AP Phishing, Man in the Middle, Ataque de contraseñas (fuerza bruta/ diccionario) Inducción chopchop, ataque estadístico.
Integridad	Fragmentación 802,11 marco de inyección, 802,11 datos Replay, 802.1X EAP Replay

Datos extraídos de diversas fuentes (elaboración propia)

Si alguno de estos servicios fuera quebrantado, significaría una vulnerabilidad en el sistema, vulnerabilidad que se busca encontrar en el presente estudio.

Tabla 4
Muestreo de vulnerabilidades de protocolos de protección

Servicio	Ataques
Autenticación	Ataque de fragmentación e inyección, y ataque de contraseñas (fuerza bruta/ diccionario)
Confidencialidad	Ataque de contraseñas (fuerza bruta/ diccionario) Inducción chopchop, ataque estadístico.
Integridad	Ataque de fragmentación e inyección

Datos obtenidos de diversas fuentes (elaboración propia)

3.3. Hipótesis

“El análisis de los protocolos de protección de redes inalámbricas Wi-Fi, permitirá seleccionar una tecnología adecuada para el acceso seguro a redes inalámbricas Wi-Fi evitando posibles ataques que atenten contra la seguridad de la información”.

3.4. Variables

Independiente:

Análisis de protocolos de protección de redes inalámbricas Wi-Fi.

Dependiente:

Detección de Vulnerabilidades Frente a Posibles Ataques que Atenten Contra la Seguridad de la Información

3.5. Operacionalización

Tabla 5
Operacionalización Variable Independiente

Variable Independiente	Dimensiones	Indicadores	Técnicas e Instrumentos de recolección de datos
Análisis de protocolos de protección de redes inalámbricas Wi-Fi	✓ Protocolos de protección inalámbrico existentes	✓ Cuantificación del número de Protocolos de protección	✓ Observación ✓ Recopilación de información
	✓ Cifrado	✓ Grado de complejidad en la generación de cifrado pseudoaleatorio. ✓ Nivel de Susceptibilidad en tamaño del algoritmo de cifrado. ✓ Grado de Resistencia a Ataques de Fuerza Bruta.	✓ Observación ✓ Recopilación de información ✓ Análisis
	✓ Mecanismos de entrega de datos	✓ Porcentaje de Paquetes de datos entregados. ✓ Cuantificación de paquetes íntegramente transferidos. ✓ Ratios de transmisión en ambiente de pruebas.	✓ Observación ✓ Recopilación de información ✓ Análisis
	✓ Autorización	✓ Cuantificación de APs No Autorizados mediante metodologías de convergencia y vectores. ✓ Porcentaje de APs accedidos Sin Autorización	✓ Observación ✓ Pruebas ✓ Recopilación de información ✓ Análisis

Datos obtenidos de diversas fuentes (Elaboración propia)

Tabla 6
Operacionalización Variable Dependiente

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Variable Dependiente	Dimensiones	Indicadores	Técnicas e Instrumentos de recolección de datos
Detección de Vulnerabilidades Frente a Posibles Ataques que Atenten Contra la Seguridad de la Información	✓ Confidencialidad	✓ Ratio de Tiempo que se demoran los vectores de inicialización para generar claves diferentes para cada trama. ✓ Porcentaje de ataques en conexiones inalámbricas protegidas que violan la confidencialidad de una trama durante su transmisión.	✓ Observación ✓ Análisis ✓ Pruebas
	✓ Integridad	✓ Cuantificación de mecanismos sin Integridad de cabecera. ✓ Numero de técnicas de detección de errores que no son eficientes para garantizar la integridad de envíos.	✓ Observación ✓ Análisis ✓ Pruebas
	✓ Autenticación	✓ Número total de accesos mediante una Autenticación basadas en máquina. ✓ Porcentaje de vulnerabilidades de alto impacto mitigadas	✓ Observación ✓ Análisis ✓ Pruebas

Datos obtenidos de diversas fuentes (elaboración propia)

3.6. Métodos, técnicas e instrumentos de recolección de datos

3.6.1. Métodos

En el presente estudio se utilizarán los siguientes métodos de investigación:

Científico:

El cual a través de una serie de pasos sistemáticos servirá de utilidad para recopilar información necesaria, a fin de encontrar la tecnología adecuada a ser aplicada en el escenario de pruebas para nuestros análisis.

Deductivo:

Ya que al estudiar los diferentes tipos de protocolos de seguridad en redes inalámbricas Wi-Fi desde su nivel más amplio hacia los detalles, se buscará encontrar la tecnología que posea las características más seguras y con menos vulnerabilidades.

3.6.2. Técnicas

Las técnicas a emplearse en el presente estudio son:

Observación

Análisis

Pruebas

3.6.3. Instrumentos de recolección de datos

Dado el propósito del presente estudio, se considera que los instrumentos adecuados para para le recolección de datos son las guías de observación, estándares y documentos técnicos de la RFC (Request for Comments) y publicaciones de la NIST (National Institute of Standards and Technology), de esta manera es posible definir los parámetros para desarrollar el análisis de los protocolos de protección y autenticación, los mismos que arrojarán resultados, mostrando las vulnerabilidades de dichos protocolos en redes inalámbricas Wi-Fi.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

3.7. Procedimiento para la recolección de datos

Para la recolección de datos en ambos escenarios se hace uso de las siguientes herramientas de auditoria Wi-Fi:

Figura 4. Herramientas de Auditoría usadas en el trabajo de campo

Fuente: logowifislax.png, kali-logo-gray-trans.png, Beini-logo.jpg, logo.png © Todos los derechos reservados por: Wifislax, Kali Linux, Beini, Xiaopan Os. Obtenidas de: https://www.kali.org/, http://www.wifislax.com/, http://beini.es/, https://xiaopan.co/

3.7.1. Uso de las Herramientas de Auditoría

3.7.1.1. Ataque de Fuerza Bruta (Contraseña)

1. La herramienta utilizada para el Ataque de Contraseña es Wifislax – Linset.

Figura 5. Ataque de Fuerza Bruta (paso 1)

Fuente: Herraminenta Wifislax - Linset

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

2. Seleccionar la tarjeta de red a utilizar en el equipo atacante.

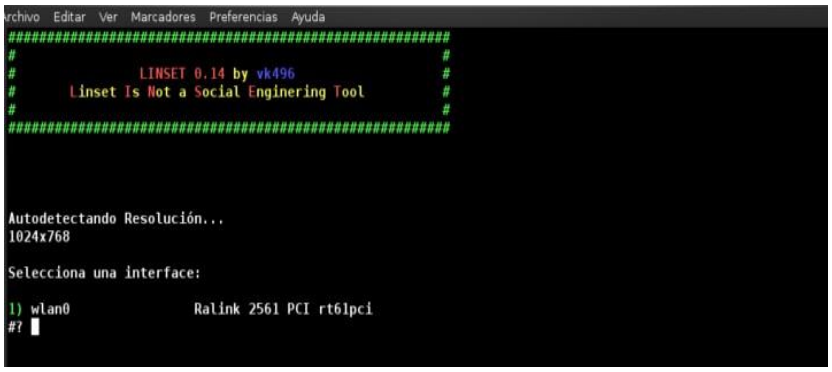

Figura 6. Ataque de Fuerza Bruta (paso 2)

Fuente: Herraminenta Wifislax - Linset

3. Seleccionar todos los canales para el escaneo de objetos correspondiente.

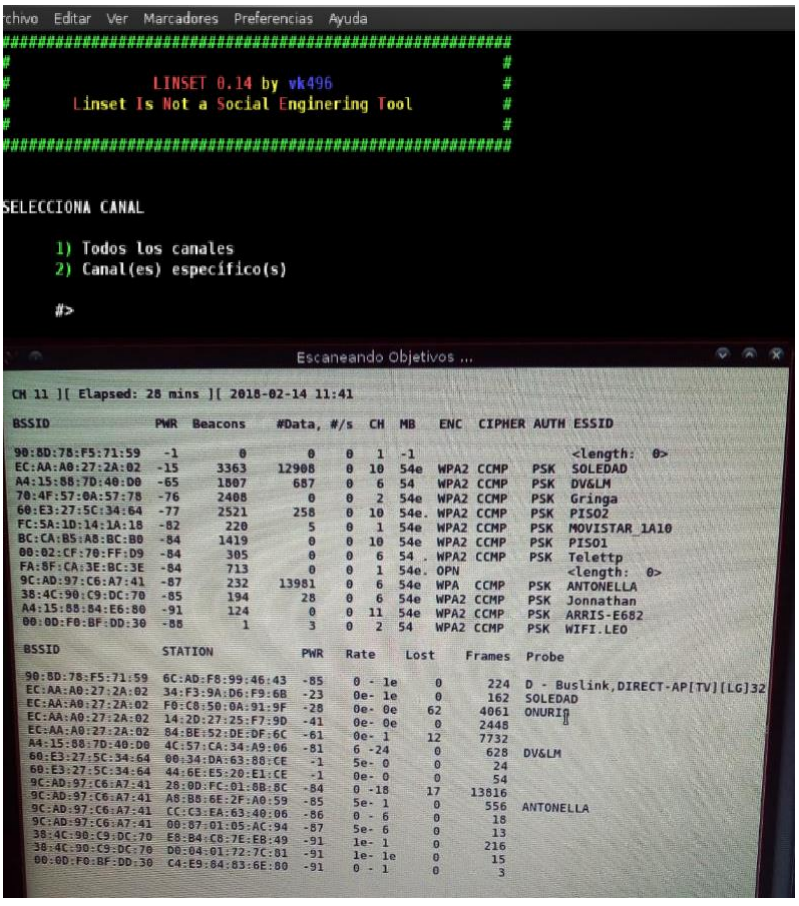

Figura 7. Ataque de Fuerza Bruta (paso 3)

Fuente: Herraminenta Wifislax - Linset

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4. Del listado de objetos escaneados se selecciona el que tenga mayor porcentaje de intensidad teniendo en cuenta que debe tener al menos un cliente conectado. En este ejemplo se ha seleccionado el AP con nombre APOLLLINE con intensidad de conexión 56% ubicado en el número 23 en el canal 6.

Figura 8. Ataque de Fuerza Bruta (paso 4)
Fuente: Herraminenta Wifislax - Linset

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5. Elegir el tipo de ataque a realizar, seleccionando por defecto el ataque recomendado Hostpad.

Figura 9. Ataque de Fuerza Bruta (paso 5)
Fuente: Herraminenta Wifislax - Linset

6. Obtener el handshake, se utiliza modo aircrack-ng (Posibilidades de Fallo).

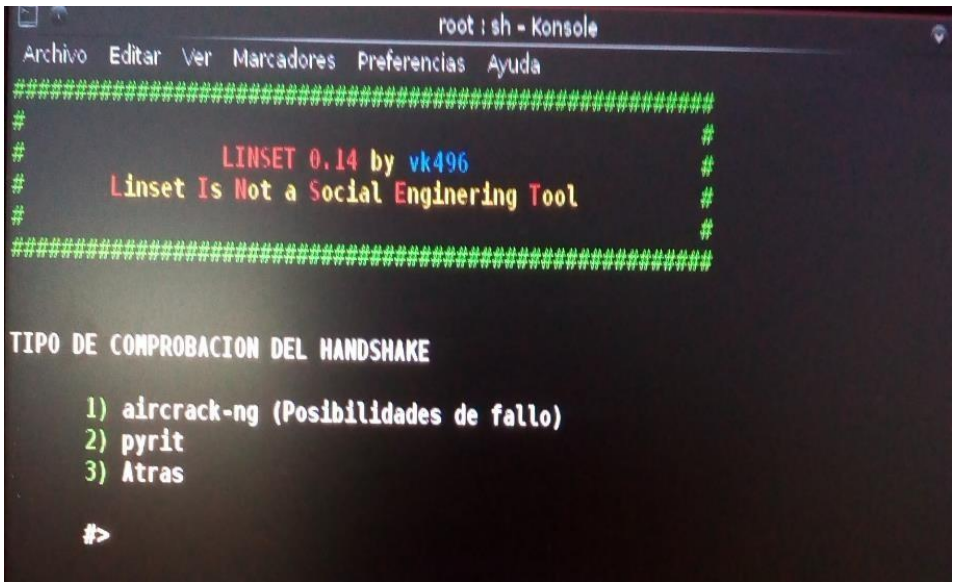

Figura 10. Ataque de Fuerza Bruta (paso 6)
Fuente: Herraminenta Wifislax - Linset

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

7. Seleccionar el tipo de desautenticación, en las pruebas realizadas se ha utilizado Realizar desautenticación masiva al AP objetivo.

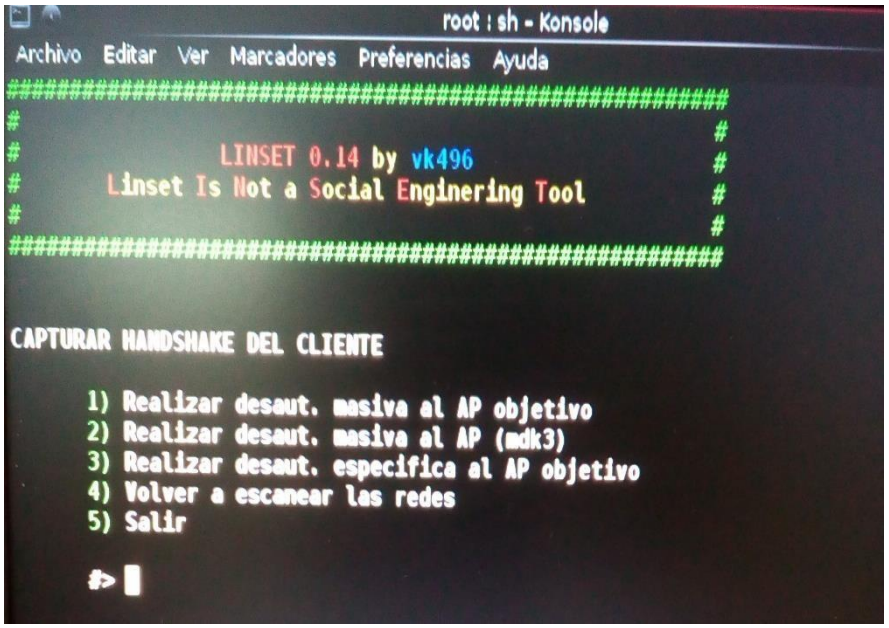

Figura 11. Ataque de Fuerza Bruta (paso 7)
Fuente: Herraminenta Wifislax - Linset

8. Verificar en la parte superior derecha si se ha capturado el handshake.

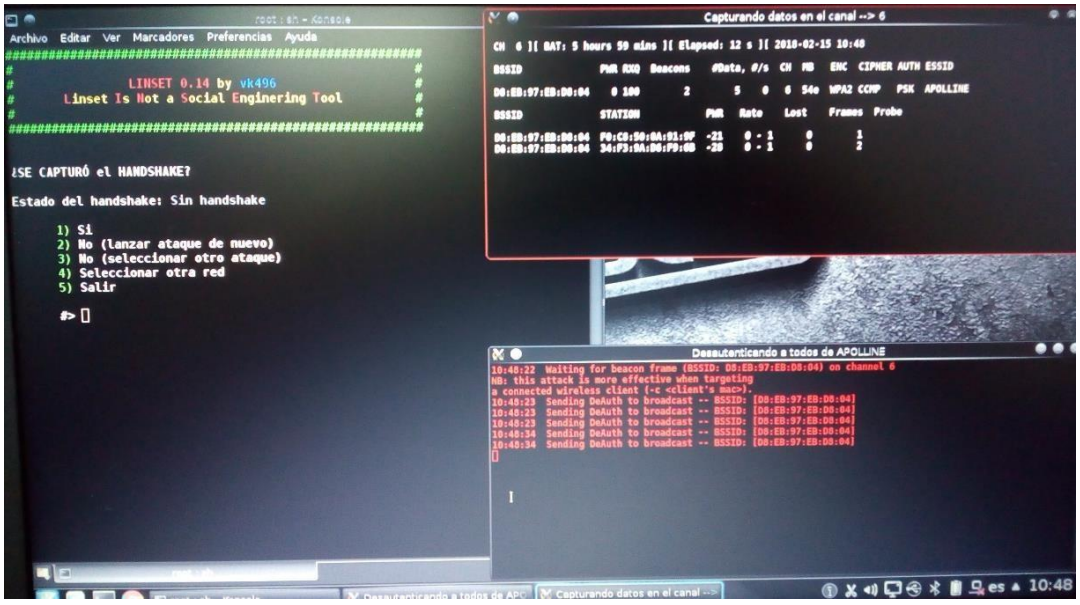

Figura 12. Ataque de Fuerza Bruta (paso 8)
Fuente: Herraminenta Wifislax - Linset

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

9. Lograda la vulneración, se crea una doble conexión de red inalámbrica, en la cual solicita el ingreso nuevamente de la clave, esta a su vez es capturada, Linset realiza una comparación con el AP real para ver si coinciden.

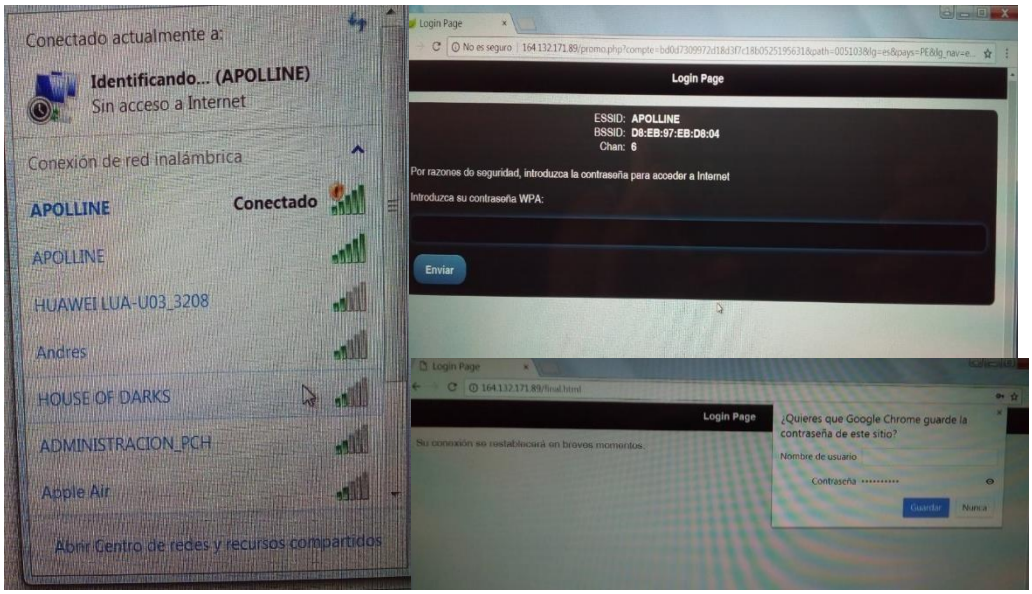

Figura 13. Ataque de Fuerza Bruta (paso 9)
Fuente: Ventana de Windows 7 Professional

10. Linset captura la clave ingresada por la víctima, en la siguiente pantalla se puede observar la clave del AP vulnerado.

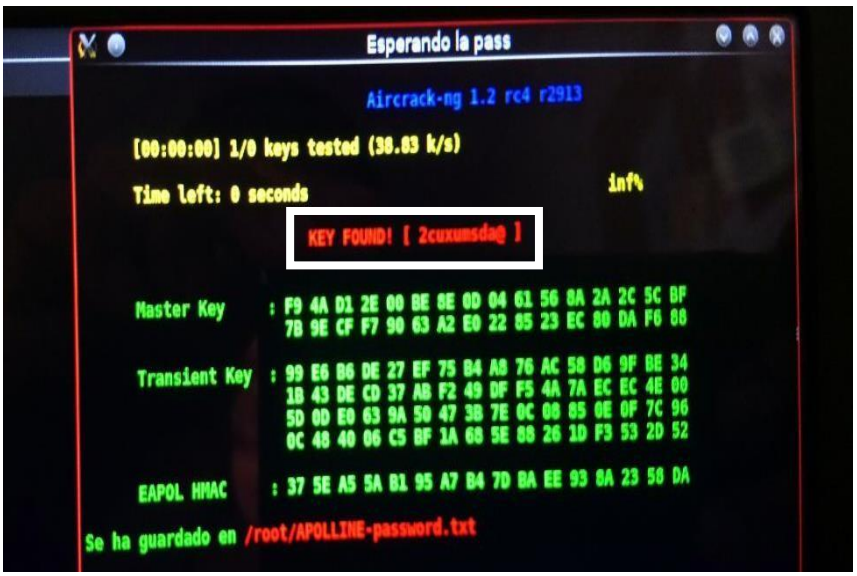

Figura 14. Ataque de Fuerza Bruta (paso 10)
Fuente: Fuente: Herraminenta Wifislax - Linset

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

11. Vulnerado el AP se puede ver el tráfico de la red de acuerdo a los movimientos que realizan los equipos conectados.

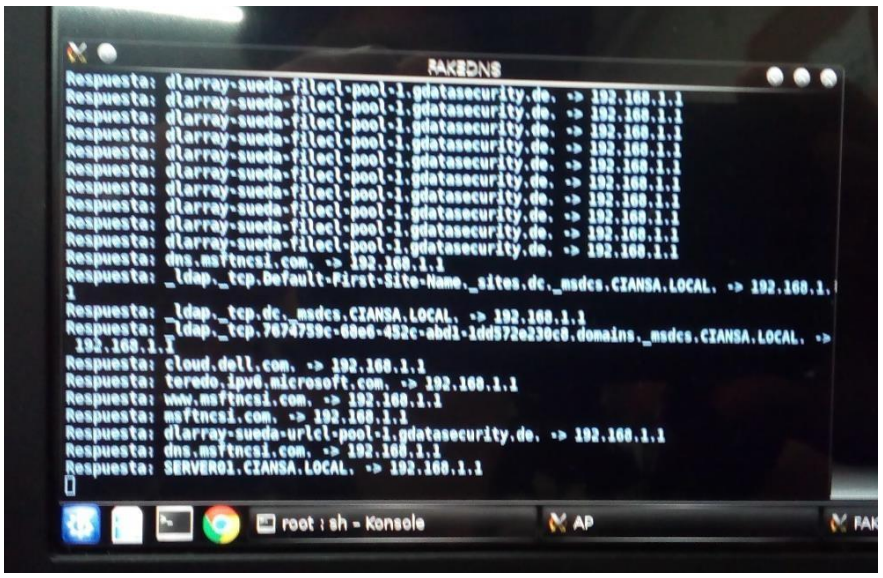

Figura 15. Ataque de Fuerza Bruta (paso 11)
Fuente: Fuente: Herraminenta Wifislax - Linset

3.7.1.2. Ataque de Denegación de Servicios (DoS)

La herramienta elegida para este tipo de ataque es Kali Linux

1. Conocer las interfaces de red inalámbrica que posee el equipo atacante

```
iwconfig
```

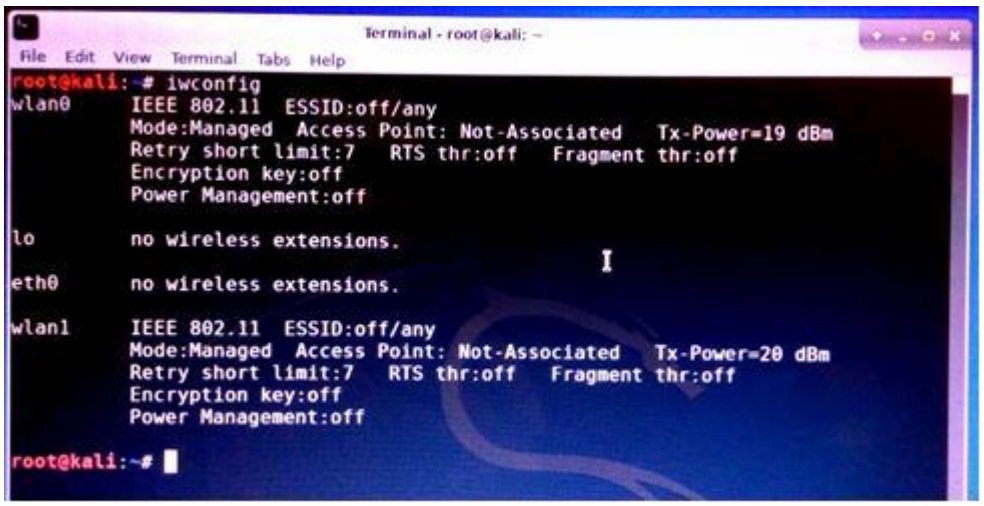

Figura 16. Ataque DoS (paso 1)
Fuente: Herraminenta Kali Linux

2. Conocer los Chipset de las interfaces inalámbricas del atacante

```
airmon-ng
```

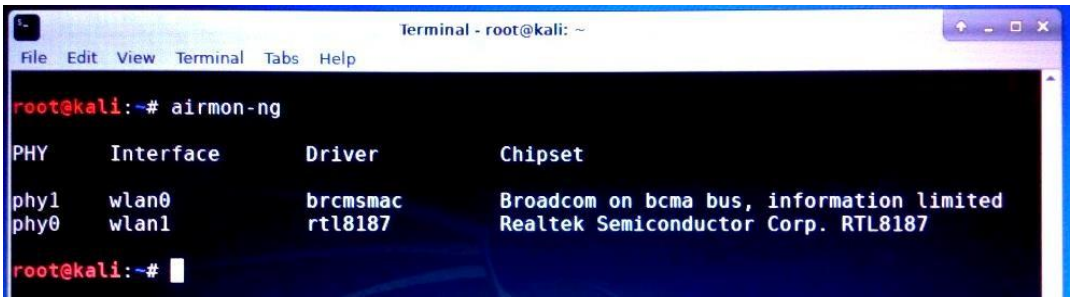

Figura 17. Ataque DoS (paso 2)

Fuente: Herraminenta Kali Linux

3. Verificar qué procesos podrían interferir en el modo Monitor

```
airmon-ng check
```

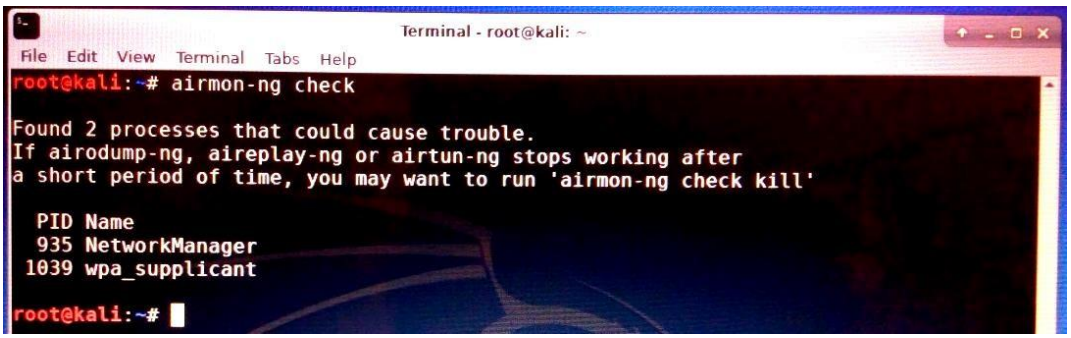

Figura 18. Ataque DoS (paso 3)

Fuente: Herraminenta Kali Linux

4. Eliminar los procesos que interfieren y volver a verificar

```
airmon-ng check kill
airmon-ng check
```

Figura 19. Ataque DoS (paso 4a y 4b)

Fuente: Herraminenta Kali Linux

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5. Establecer en modo Monitor la interface elegida del equipo atacante

```
airmon-ng start wlan1
```

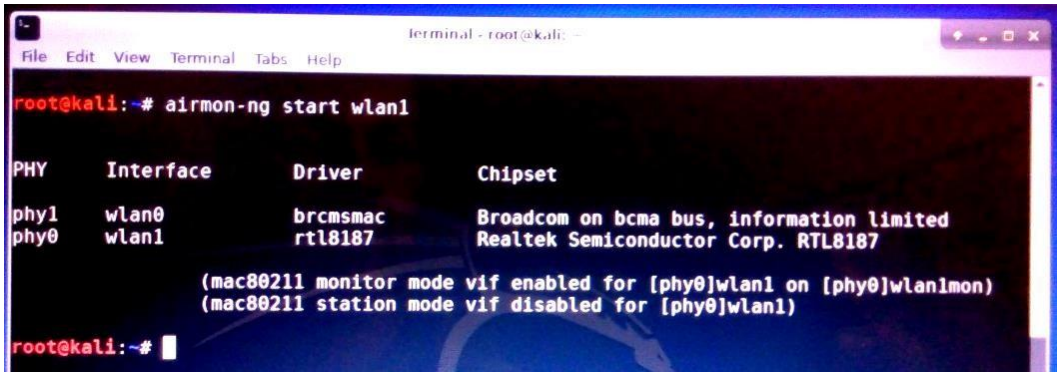

Figura 20. Ataque DoS (paso 5)

Fuente: Herraminenta Kali Linux

6. Proceder con el escaneo de las redes Wi-Fi cercanas

```
airodump-ng wlan1mon
```

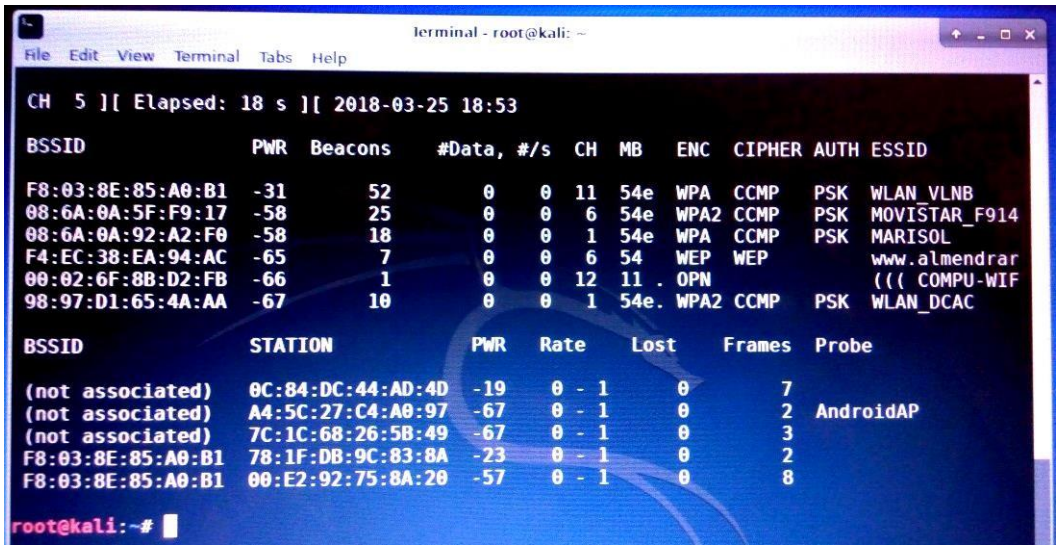

Figura 21. Ataque DoS (paso 6)

Fuente: Herraminenta Kali Linux

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

7. Verificar el Canal de la víctima y enlazarse de manera específica a ese canal

```
airodump-ng –c 11  wlan1mon
```

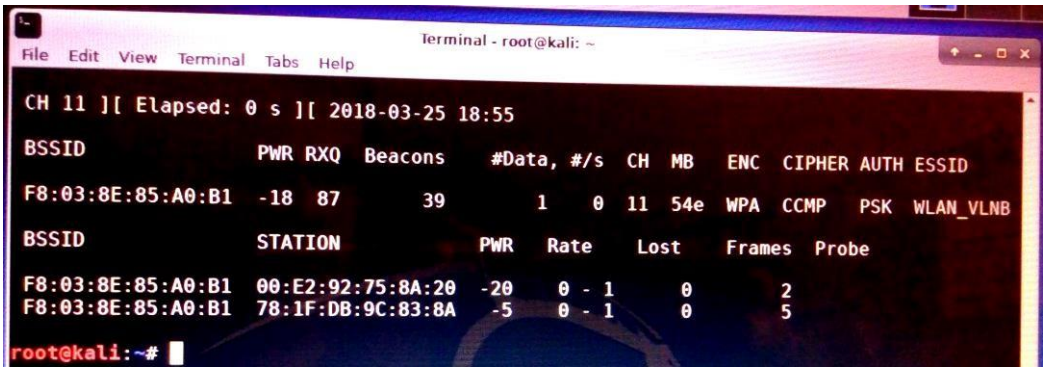

Figura 22. Ataque DoS (paso 7)

Fuente: Herraminenta Kali Linux

8. Verificar el BSSID de la víctima y enviar paquetes de desautenticación

```
aireplay-ng -0 0 –a F8:03:8E:85:A0:B1 wlan1mon
```

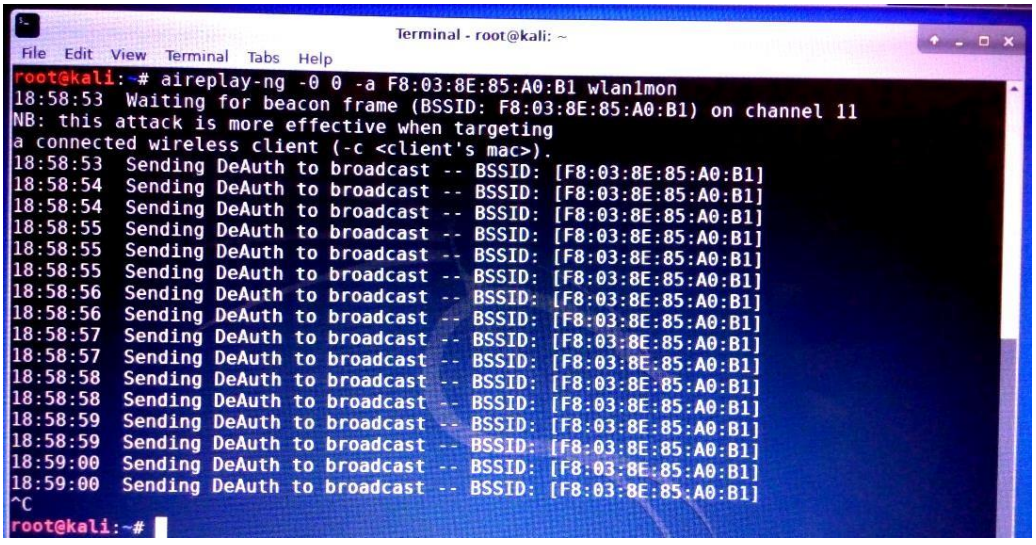

Figura 23. Ataque DoS (paso 8)

Fuente: Herraminenta Kali Linux

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

9. Si se desea atacar a un cliente específico conectado se completa la línea con su identificación MAC

```
aireplay-ng -0 0 -a F8:03:8E:85:A0:B1 -c 00:E2:92:75:8A:20 wlan1mon
```

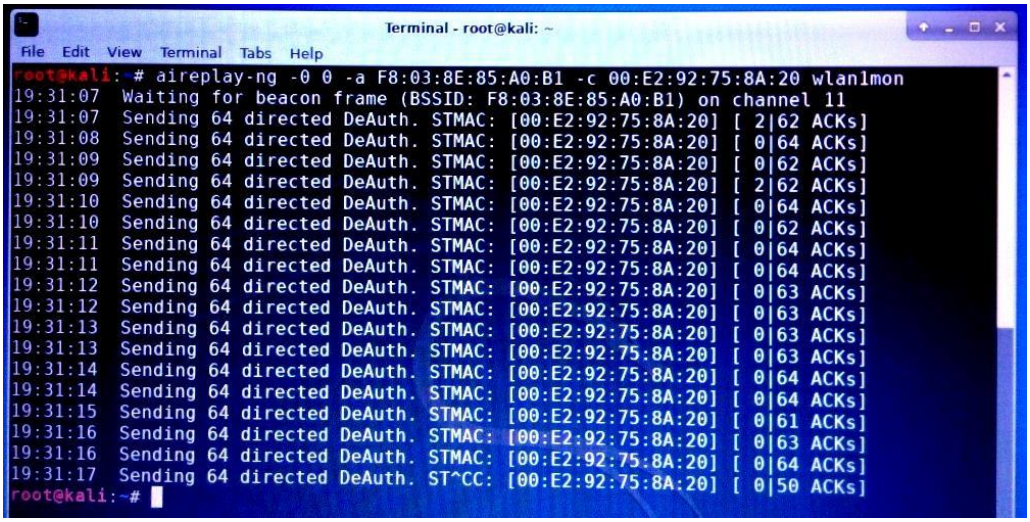

Figura 24. Ataque DoS (paso 9)
Fuente: Herraminenta Kali Linux

3.7.2. Escenario de Pruebas

3.7.2.1. Escenario #1: Pruebas a nivel doméstico

Para este escenario de pruebas, se contemplan los protocolos de seguridad: WEP, WPA y el WPA2 y sus correspondientes mecanismos de cifrado: WEP, TKIP, CCMP. La autenticación la realiza el mismo mecanismo de cifrado.

Software y hardware requerido:

Para este escenario se considera el uso de una computadora portátil (laptop), que actúa como cliente usuario, la misma que se enlaza a un punto de acceso, el cual soporta los protocolos de seguridad descritos en este escenario. También se cuenta con otra computadora portátil, en la cual se conecta una antena adaptador USB Wi-

Fi marca Alfa Networks modelo AWUS036H para una mejor recepción de señales Wi-Fi, que hacen las veces de atacante, para realizar las pruebas de intrusión y craqueo. El software de auditoría, escaneo y ruptura estarán instalados en esta última portátil.

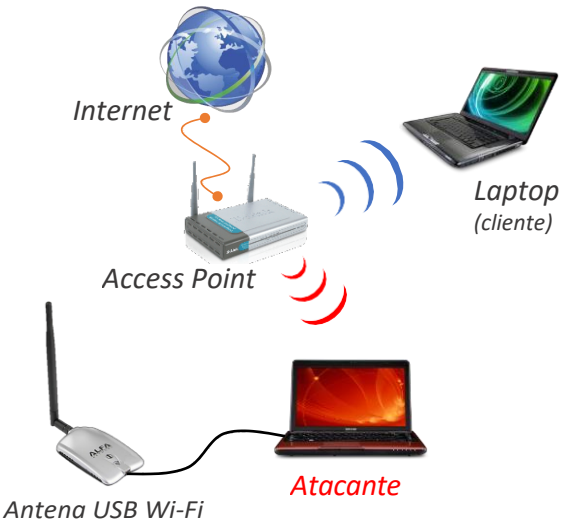

Figura 25. Escenario #1: Pruebas a nivel doméstico

Fuente: Adaptado de https://bit.ly/2ISQJVg

3.7.2.2. Escenario #2: Pruebas a nivel corporativo

Para este escenario de pruebas, se configuran los protocolos de seguridad: WPA y WPA2 y sus correspondientes mecanismos de cifrado: TKIP, CCMP.

Software y hardware requerido:

Los equipos contemplados en este escenario de pruebas comprenden: 1 Servidor de Archivos con Windows Server 2012. 1 punto de acceso, 1 computadora portátil cliente (suplicante) y 1 portátil atacante.

Figura 26. Escenario #2: Pruebas a nivel corporativo

Fuente: Adaptado de https://bit.ly/2JGXzhP

3.7.3. Pruebas realizadas en campo

Las pruebas de campo realizadas contemplan los escenarios doméstico y corporativo, de los cuales se obtuvieron resultados exitosos en un 33% y 20% respectivamente.

Tabla 7
Pruebas de campo realizadas

Escenario	Ataques Realizados	Ataques Exitosos
Nivel Doméstico	100	33
Nivel Corporativo	45	9

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

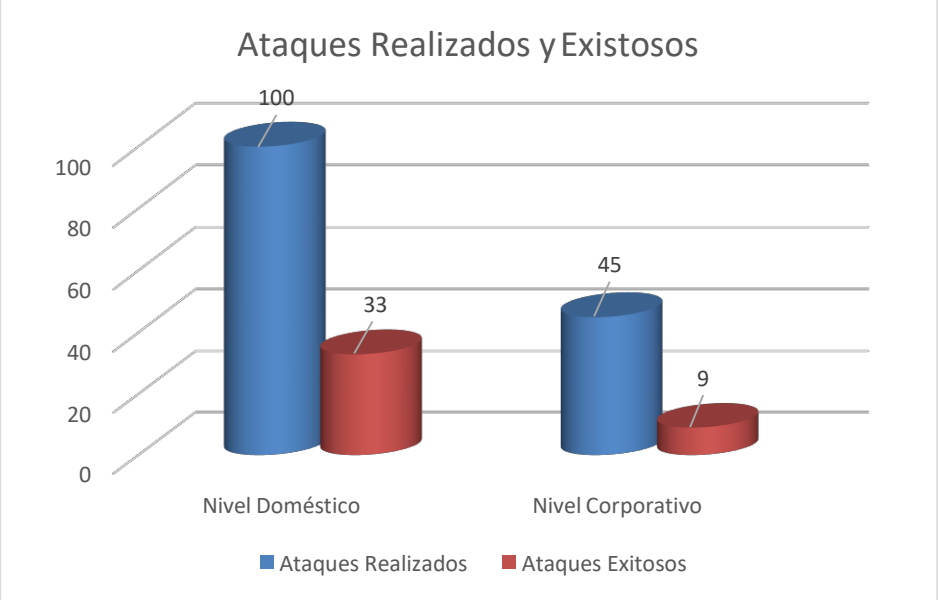

Figura 27. Pruebas de Campo Realizadas

Fuente: Investigación y trabajo de campo (elaboración propia)

Los tipos de ataque realizados fueron: Fuerza Bruta y Denegación de Servicios sobre los protocolos WEP, WPA y WPA2, enmarcados en los escenarios doméstico y corporativo.

Tabla 8
Pruebas de campo realizadas por tipo de ataque / protocolo

Escenario de Prueba	Ataques por Protocolos			Ataques Exitosos por Tipo					
				Fuerza Bruta			Denegación de Servicios		
	WEP	WPA	WPA2	WEP	WPA	WPA2	WEP	WPA	WPA2
Nivel Doméstico	32	35	33	5	4	2	10	7	5
Nivel Corporativo		25	20		3	1		3	2

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

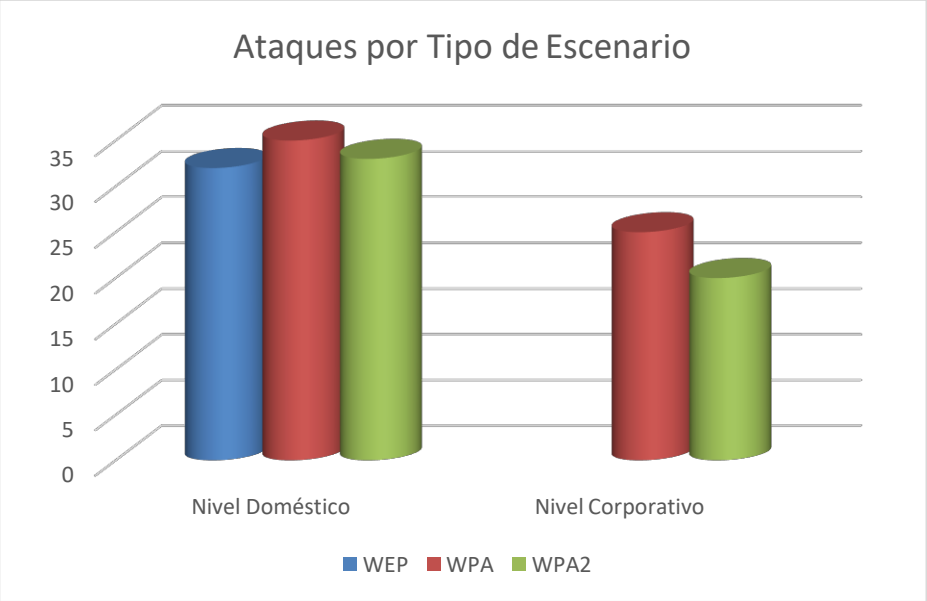

Figura 28. Ataques Realizados por Tipo de Escenario

Fuente: Investigación y trabajo de campo (elaboración propia)

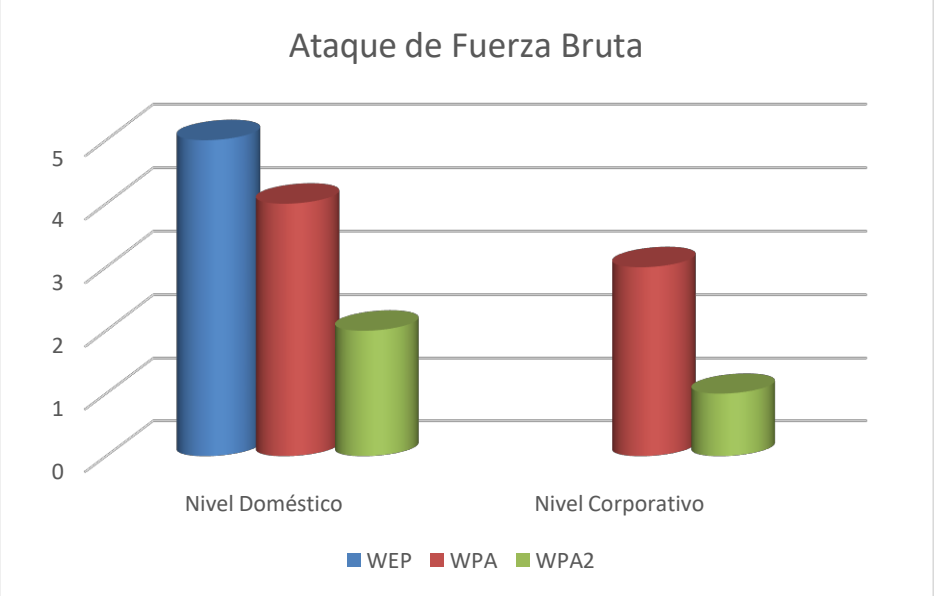

Figura 29. Ataque de Fuerza Bruta

Fuente: Investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

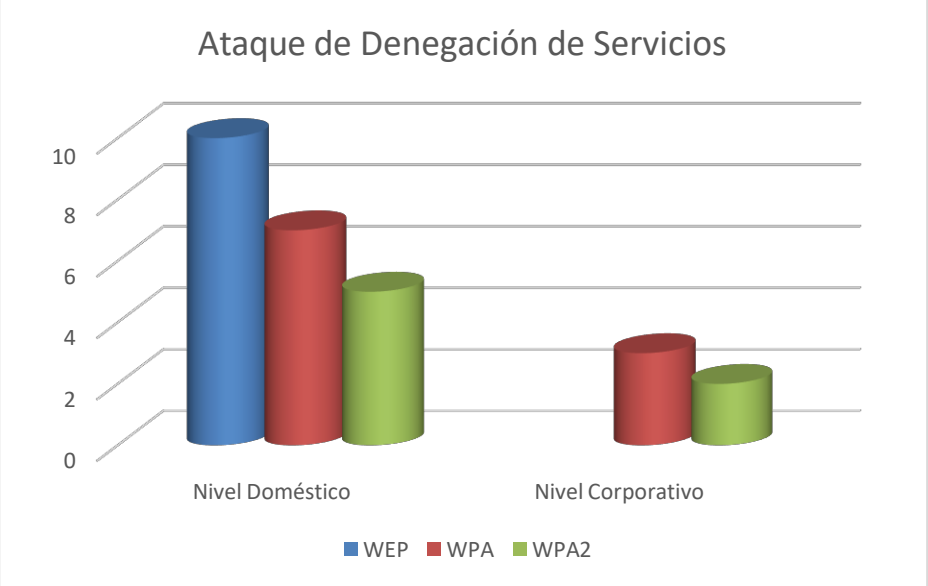

Figura 30. Ataque de Denegación de Servicios

Fuente: Investigación y trabajo de campo (elaboración propia)

3.8. Criterios Éticos

La investigación tiene:

Valor científico: Para que una investigación sea ética debe tener valor, lo que representa un juicio sobre su importancia científica; debe plantear una intervención que conduzca a mejoras o bienestar de la población, o que produzca conocimiento que pueda abrir oportunidades de superación o de solución a problemas, aunque no sea en forma inmediata.

3.9. Criterios de rigor científico

En los criterios de rigor científico se considera que esta investigación tiene:

La credibilidad: se logra cuando los resultados del estudio son reconocidos como verdaderos por los investigadores que lo realizan y participan en el estudio, también por las personas que han experimentado, o estado en contacto con el sujeto

investigador; se procede a través de las observaciones y conversaciones ampliadas con los sujetos de investigación en el estudio. Recolectando información que produzca hallazgos que son reconocidos, por los informantes como una verdadera aproximación sobre lo que ellos piensan.

La conformidad: se entiende como la habilidad de otro investigador de seguir la pista o ruta de lo realizado por el investigador original. Para ello es necesario un registro y documentación completa de las decisiones e ideas, que el investigador haya tenido en relación con el estudio.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

IV. CAPITULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

4.1. Análisis Estadístico e Interpretación de datos

Para realizar el análisis de la variable independiente, se hace referencia a los datos existentes en las especificaciones técnicas de cada protocolo inalámbrico, los mismos que están especificados en el Capítulo II.

Se dará los siguientes valores cuantitativos:

Tabla 9
Cuantificador de indicadores

CUALIDAD	VALORACIÓN
Si	1
No	0

(Datos obtenidos de diversas fuentes (Elaboración propia)

Tabla 10
Escala Cualitativa de cuantificación de indicadores: Variable Independiente

CATEGORIA	ABREVIATURA	VALORACION
Muy Malo	Mm	0
Malo	M	1
Regular	B	2
Muy bueno	Mb	3
Excelente	E	4

(Datos obtenidos de diversas fuentes (Elaboración propia)

4.1.1. Variable Independiente

Análisis de protocolos de protección de redes inalámbricas Wi-Fi.

INDICADOR 1: Método de Cifrado

Escenario #1: Nivel Doméstico

Tabla 11.
Cifrado de Protocolos – Nivel Doméstico

INDICES	WEP		WPA				WPA2			
			TKIP		AES		TKIP		AES	
Algoritmo de cifrado	Mm	0	M	1	E	4	M	1	E	4
Tamaño Susceptible del algoritmo de cifrado	Mm	0	M	1	E	4	M	1	E	4
Tamaño del IV	Mm	0	M	1	Mb	3	M	1	E	4
Reutilización del IV	Mm	0	M	1	Mb	3	M	1	E	4
Envío del IV texto plano	Mm	0	M	1	Mb	3	M	1	E	4

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

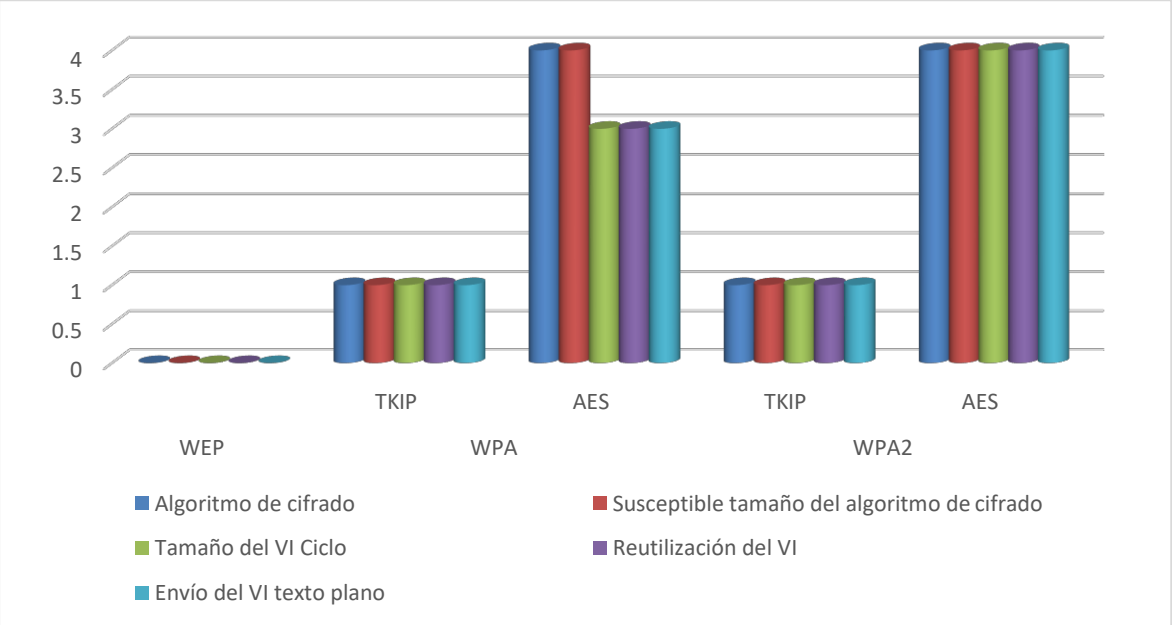

Figura 31. Cifrado de los Protocolos – Nivel Doméstico

Fuente: Investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Escenario #2: Nivel Corporativo

Tabla 12.
Cifrado de Protocolos – Nivel Corporativo

INDICES	WPA				WPA2			
	TKIP		AES		TKIP		AES	
Algoritmo de cifrado	M	1	Mb	3	M	1	Mb	3
Tamaño Susceptible del algoritmo de cifrado	M	1	Mb	3	M	1	Mb	3
Tamaño del IV	M	1	Mb	3	M	1	Mb	3
Reutilización del IV	M	1	Mb	3	M	1	Mb	3
Envío del IV texto plano	M	1	Mb	3	M	1	Mb	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

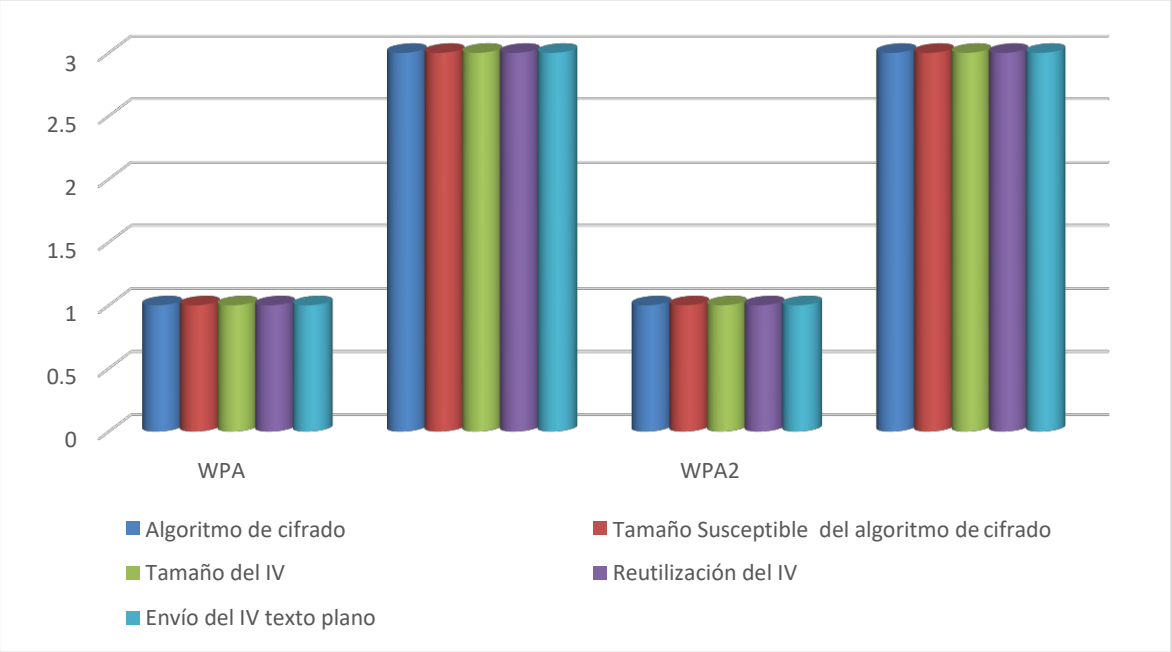

Figura 32. Cifrado de los Protocolos – Nivel Corporativo

Fuente: Investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Interpretación:

En el escenario #1, WEP usa el algoritmo de cifrado de flujo de generación pseudoaleatoria basado en RC4 quien realiza la encriptación haciendo uso de XOR, la corta longitud del vector de inicialización de 24 bits permite la repetición frecuente dando lugar a posibles ataques.

WPA-TKIP y WPA-AES utilizan el algoritmo TKIP como mecanismo de encriptación, solucionan la debilidad del vector de inicialización de WEP con la inclusión del vector con una longitud de 48 bits permitiendo generar una combinación de caracteres de claves diferentes evitando ataques. Las WPA-AES se generan automáticamente y son distribuidas automáticamente evitando su modificación manual cada cierto tiempo.

En el escenario #2, WPA-TKIP y WPA2-TKIP utilizan PSK para realizar la negociación pero no permiten la distribución, en este sistema todos los usuarios de la red tienen una misma contraseña de Wi-Fi definida por el administrador de red. Usan el algoritmo CCMP para mecanismo de encriptación, el cifrado es realizado con AES, algoritmo de 128 bits que hasta hoy no ha sido vulnerado.

WPA2-AES, actualmente las claves son generadas dinámicamente y se distribuyen de forma automática.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

INDICADOR 2: Mecanismos de Entrega de Datos

Escenario #1: Nivel Doméstico

Tabla 13
Mecanismos de Entrega de Datos - Nivel Doméstico

INDICES	WEP		WPA				WPA2			
			TKIP		AES		TKIP		AES	
Mecanismos de Integridad de la cabecera.	Mm	0	M	1	Mb	3	M	1	E	4
Mecanismos de integridad independiente de llave y IV.	Mm	0	M	1	Mb	3	M	1	E	4
Mecanismo de integridad de forma lineal.	Mm	0	M	1	Mb	3	M	1	E	4

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

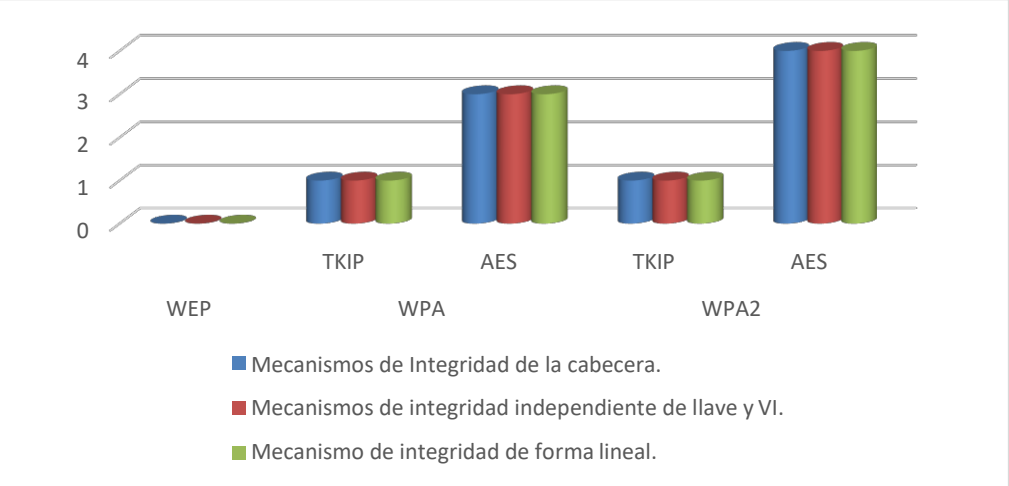

Figura 33. Mecanismos de Entrega de Datos – Nivel Doméstico

Fuente: Investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Escenario #2: Nivel Corporativo

Tabla 14
Mecanismos de Entrega de Datos - Nivel Corporativo

INDICES	WPA				WPA2			
	TKIP		AES		TKIP		AES	
Mecanismos de Integridad de la cabecera.	M	1	Mb	3	M	1	Mb	3
Mecanismos de integridad independiente de llave y IV.	M	1	Mb	3	M	1	Mb	3
Mecanismo de integridad de forma lineal.	M	1	Mb	3	M	1	Mb	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

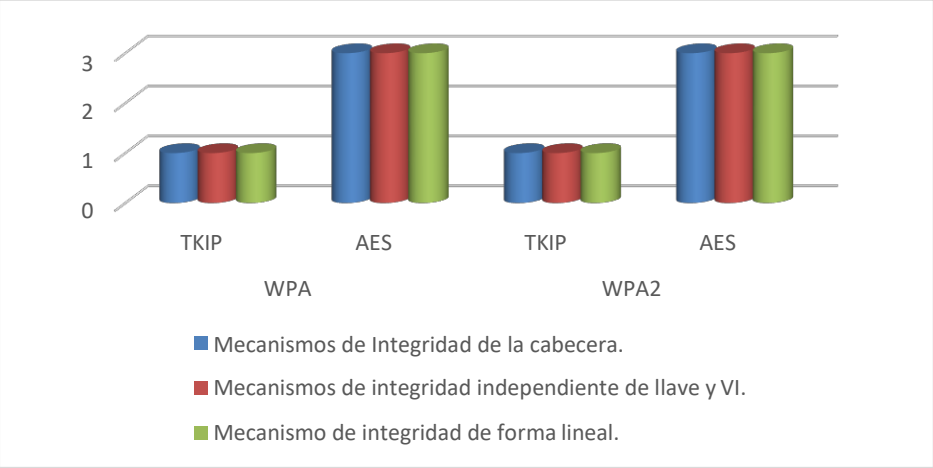

Figura 34. Mecanismos de Entrega de Datos – Nivel Corporativo

Fuente: Investigación y trabajo de campo (elaboración propia)

Interpretación:

En el escenario #1, WEP proporciona un mecanismo de integridad mediante ICV (Integrity Check Value) el cual es generado haciendo un CRC de 32 bits.

Los CRC son independientes de la llave de IV, al conocer el plaintext de un paquete encriptado se facilita la inyección de paquetes. WEP no realiza la

integridad de la cabecera debido al uso de mecanismos de detección de errores y no de integridad.

Los CRC son lineales, al combinarlas con la operación XOR también lineal permite a un atacante interceptar un mensaje y modificarlo.

WPA-TKIP y WPA-AES, el algoritmo Michael es usado para el cálculo de código de integridad que evita que el atacante capture paquetes y que estos sean modificados y reenviados. Este algoritmo fue limitado por Hardware basado en RC4 debido a que no proporcionan seguridad contra ataques de fuerza bruta.

En el escenario #2, WPA2-TKIP y WPA2-AES asegura la cabecera del frame y los datos mediante CCMP. WPA2 cifra el MIC con el cifrado de modo contador de AES.

INDICADOR 3: Autorización

Escenario #1: Nivel Doméstico

Tabla 15.
Autorización – Nivel Doméstico

INDICES	WEP		WPA				WPA2			
			TKIP		AES		TKIP		AES	
Pre - autenticación	NO	0	NO	0	NO	0	SI	1	SI	1
Distribución de clave forma manual	SI	1	SI	1	NO	0	SI	1	NO	0
Autenticación de maquina	SI	1	SI	1	NO	0	SI	1	NO	0
Des asociación	SI	1	SI	1	SI	1	SI	1	SI	1
Trafico	SI	1	NO	0	NO	0	NO	0	NO	0

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

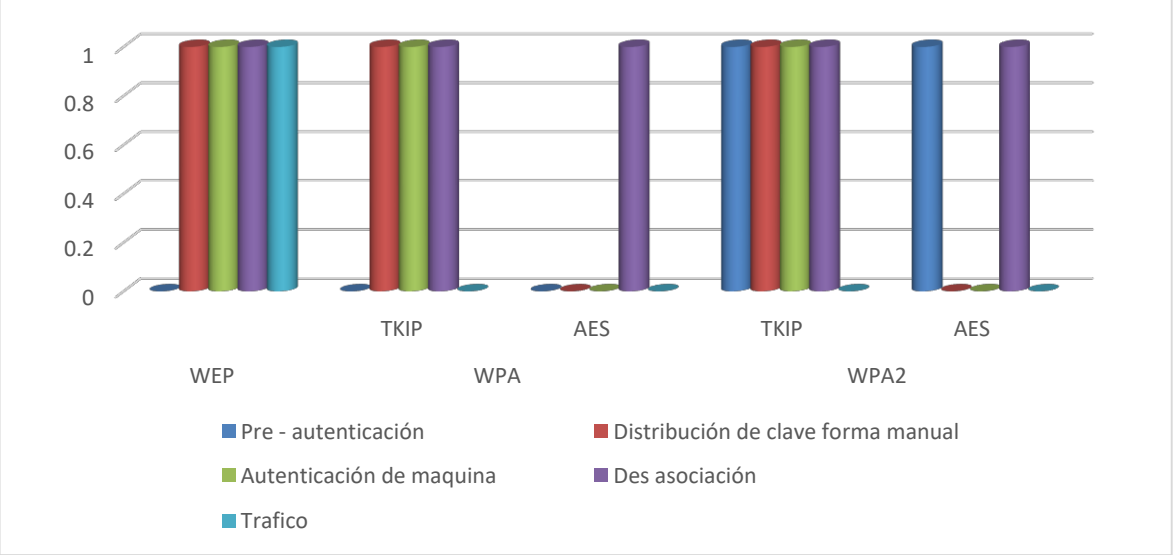

Figura 35. Autorización – Nivel Doméstico

Fuente: Investigación y trabajo de campo (elaboración propia)

Escenario #2: Nivel Corporativo

Tabla 16.
Autorización – Nivel Corporativo

INDICES	WPA				WPA2			
	TKIP		AES		TKIP		AES	
Pre - autenticación	NO	0	NO	0	SI	1	SI	1
Distribución de clave forma manual	SI	1	NO	0	SI	1	NO	0
Autenticación de maquina	SI	1	NO	0	SI	1	NO	0
Des asociación	SI	1	SI	1	SI	1	SI	1
Trafico	NO	0	NO	0	NO	0	NO	0

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

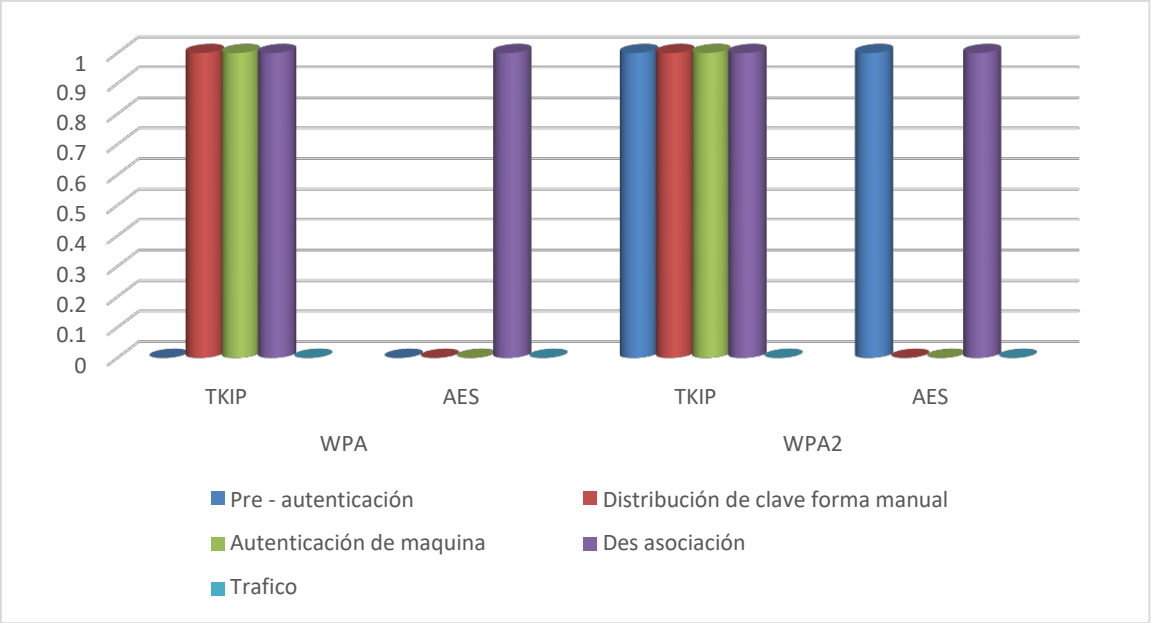

Figura 36. Autorización – Nivel Corporativo

Fuente: Investigación y trabajo de campo (elaboración propia)

Interpretación:

En el escenario #1, los mecanismos usados en WEP son débiles y fáciles de desasociar permitiendo la inyección de tráfico, al realizar una autenticación manual a la máquina y no al usuario, deja una puerta abierta para poder suplantar la MAC en un usuario legal.

En ambos escenarios, WPA-TKIP la configuración de las claves es de forma manual en los AP y clientes, hay que tener en cuenta que pese al mejoramiento del cifrado TKIP deja abierta la vulnerabilidad de parte del usuario debido a que no se generan claves suficientemente fuertes. El mecanismo de integridad mejorada no permite la inyección de tráfico, pero permite disociaciones por las autenticaciones haciendo uso de MAC.

En el escenario #2, WPA-AES hace uso de una configuración robusta verificando a cada usuario y no solo a la MAC, tiene una generación única de claves automáticas dejando de lado las claves compartidas por todos los usuarios de un entorno. Si deseamos vulnerar una infraestructura montada es difícil pero si utilizamos un cifrado ya vulnerado llega a ser susceptible a los ataques en las contraseñas, es susceptible a interferencias por parte del AP.

WPA2 usa dos modos de pre-autenticación dando posibilidad al usuario el establecimiento de procesos de autenticación con puntos de accesos próximos.

WPA2-TKIP autenticación similar a WPA, al contar con una clave distribuida manualmente al usar el cifrado AES el cual en la actualidad no es posible su vulnerabilidad por lo tanto no se puede obtener la clave de acceso. Es susceptible a sus disociaciones por su cifrado.

WPA2-AES catalogado como una de las configuraciones más difíciles de vulnerar en el escenario corporativo, hace uso de un cifrado mejorado respecto a sus predecesores, mediante una configuración más robusta, generando claves automáticas únicas por cada usuario evitando la distribución manual.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 17
Subtotales del Análisis de la Variable Independiente – Ambos Escenarios

INDICADOR	INDICES	NIVEL DOMÉSTICO					NIVEL CORPORATIVO			
		WEP	WPA		WPA2		WPA		WPA2	
			TKIP	AES	TKIP	AES	TKIP	AES	TKIP	AES
Método de Cifrado	Algoritmo de cifrado	0	1	4	1	4	1	3	1	3
	Susceptible tamaño del algoritmo de cifrado	0	1	4	1	4	1	3	1	3
	Tamaño del IV	0	1	3	1	4	1	3	1	3
	Reutilización del IV	0	1	3	1	4	1	3	1	3
	Envío del IV texto plano	0	1	3	1	4	1	3	1	3
Mecanismos de Entrega de Datos	Mecanismos de integridad de la cabecera	0	1	3	1	4	1	3	1	3
	Mecanismos de integridad independiente de llave y IV	0	1	3	1	4	1	3	1	3
	Mecanismos de integridad de forma lineal	0	1	3	1	4	1	3	1	3
Autorización	Pre-autenticación	0	0	0	1	1	0	0	1	1
	Distribución de clave forma manual	1	1	0	1	0	1	0	1	0
	Autenticación de máquina	1	1	0	1	0	1	0	1	0
	Desasociación	1	1	1	1	1	1	1	1	1
	Tráfico	1	0	0	0	0	0	0	0	0
RESULTADOS TOTALES		**4**	**11**	**27**	**12**	**34**	**11**	**25**	**12**	**26**

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Tabla 18
Sumatoria de Análisis de la Variable Independiente – Ambos Escenarios

INDICADOR	WEP*2 (*)	WPA		WPA2	
		TKIP	AES	TKIP	AES
Método de Cifrado	0	10	32	10	35
Mecanismos de Entrega de Datos	0	6	18	6	21
Autorización	8	6	2	8	4
RESULTADOS TOTALES	8	22	52	24	60

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

(*) Los valores de WEP han sido ponderados por 2, para poder homologarlos con los resultados obtenidos en los protocolos WPA y WPA2 en los escenarios 1 y 2

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Dónde:

Puntaje total del Análisis: PT= Σ (Pi máximos por indicador)

Entonces:

PT= 35 + 21 + 8 = 64

Puntaje total de cada Protocolo Analizado: PT_PW= Σ (Pwi)

Porcentaje total de cada Protocolo Analizado: (%PW)= (PT_PW / PT)*100%

Tabla 19
Porcentaje Total de Cada Protocolo Analizado

INDICES	WEP	WPA		WPA2	
		TKIP	AES	TKIP	AES
PT_PW	8	22	52	24	60
PT	64	64	64	64	64
PORCENTAJE POR PROTOCOLO	12.50	34.38	81.25	37.50	93.75

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Tabla 20
Porcentaje por Protocolo de Variable Independiente

WEP	WPA		WPA2	
	TKIP	AES	TKIP	AES
13%	34%	81%	38%	94%

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

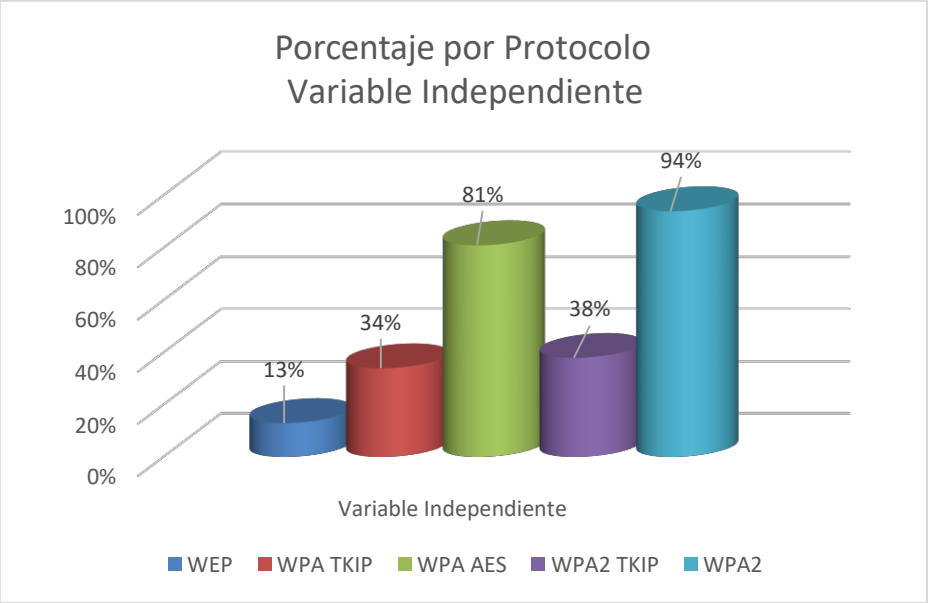

Figura 37. Porcentaje por Protocolo de Variable Independiente

Fuente: Investigación y trabajo de campo (elaboración propia)

Con los datos expuestos se puede deducir que en el escenario #1, el protocolo WEP es el más vulnerable a ataques de contraseñas, ataques de inyección, ataques de fragmentación, denegación de servicios, etc.

WPA-TKIP mitigan de forma directa los ataques mencionados anteriormente no obstante cabe indicar que WPA en cualquiera de sus variantes sigue siendo vulnerable a ataques de contraseñas a causa de que el algoritmo de cifrado ha sido vulnerado al ataque de denegación de servicios DoS.

WPA2 TKIP/ AES al igual que su antecesor mitigan los ataques de forma directa debido a que hace uso de un mejor algoritmo de encriptación el cual no ha sido quebrantado.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

4.1.2. Variable Dependiente

Detección de Vulnerabilidades Frente a Posibles Ataques que Atenten Contra la Seguridad de la Información.

Tabla 21
Escala Cualitativa de cuantificación de indicadores: Variable Dependiente

CATEGORIA	ABREVIATURA	VALORACION	PORCENTAJE
Totalmente Inadecuado	TI	0	0%
Inadecuado	I	1	25%
Poco Adecuado	PA	2	50%
Adecuado	A	3	75%
Muy Adecuado	MA	4	100%

(Datos obtenidos de diversas fuentes (Elaboración propia)

INDICADOR 1: Confidencialidad

Escenario #1: Nivel Doméstico

Tabla 22
Confidencialidad - Nivel Doméstico

INDICES	WEP		WPA				WPA2			
			TKIP		AES		TKIP		AES	
Algoritmo de cifrado mejorado	I	1	I	1	PA	2	A	3	A	3
Tamaño de algoritmo cifrado	I	1	PA	2	PA	2	A	3	A	3
Cifrado automático	I	1	PA	2	PA	2	A	3	A	3
IV cifrado y mejorado	I	1	PA	2	PA	2	A	3	A	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

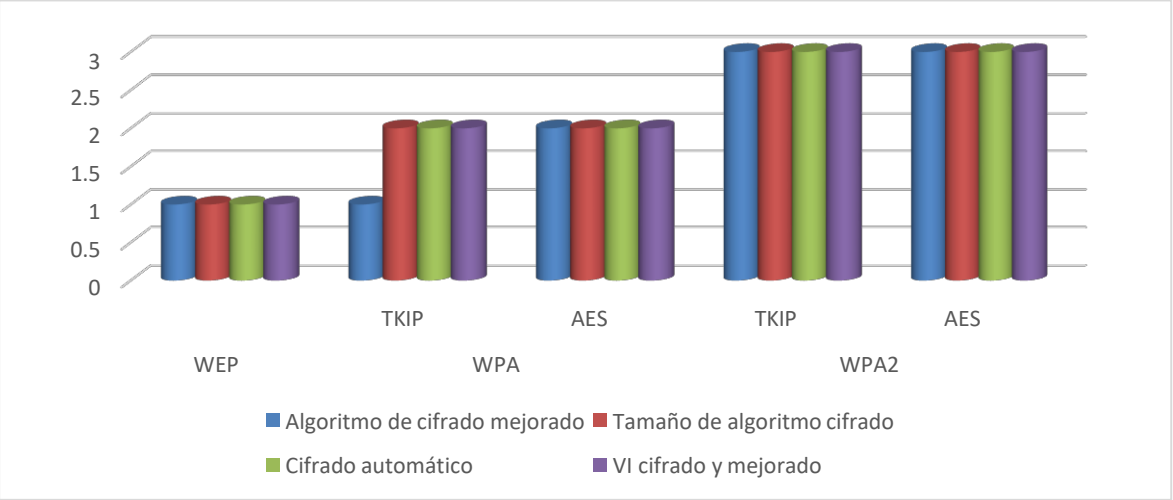

Figura 38. Confidencialidad – Nivel Doméstico

Fuente: Investigación y trabajo de campo (elaboración propia)

Escenario #2: Nivel Corporativo

Tabla 23
Confidencialidad - Nivel Corporativo

INDICES	WPA				WPA2			
	TKIP		AES		TKIP		AES	
Algoritmo de cifrado mejorado	I	1	PA	2	A	3	A	3
Tamaño de algoritmo cifrado	PA	2	PA	2	A	3	A	3
Cifrado automático	PA	2	PA	2	A	3	A	3
IV cifrado y mejorado	PA	2	PA	2	A	3	A	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

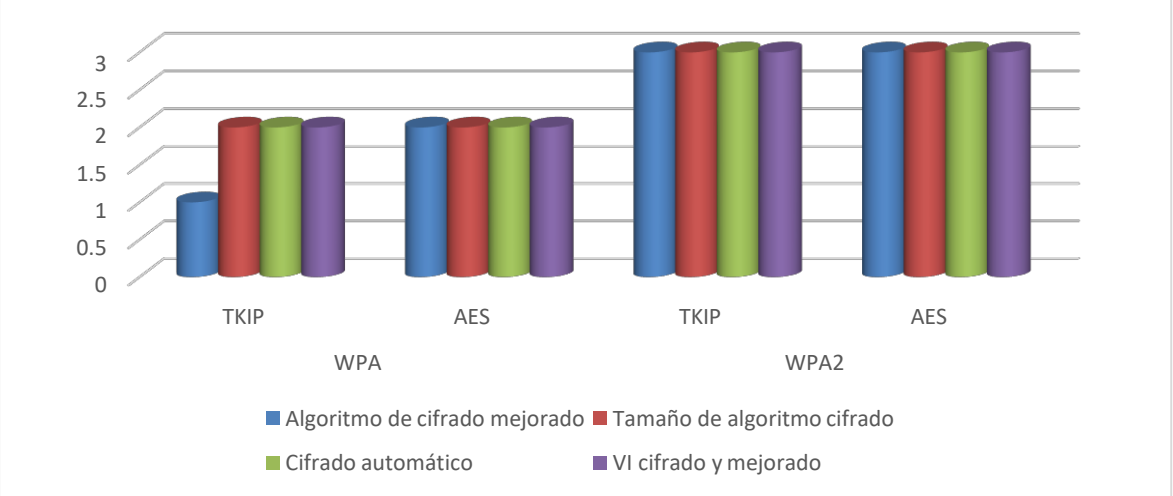

Figura 39. Confidencialidad – Nivel Corporativo

Fuente: Investigación y trabajo de campo (elaboración propia)

Interpretación:

Como se aprecia en el Gráfico anterior en el escenario #1, WEP continúa teniendo problemas en el algoritmo de cifrado, el tamaño del mismo y el envío en plano del IV. A través del ataque por inducción chopchop y fuerza bruta para vulneración de contraseñas, se logra desencriptar la clave de acceso, como de datos. En conclusión, resulta inadecuado para el cifrado de datos.

En ambos escenarios WPA-TKIP muestran una mejora importante, sin embargo, al continuar usando RC4, igual que en el caso de WEP, resulta poco adecuada para la protección contra el ataque de contraseñas. El cifrado aumenta a 128 bits, el IV aumenta a 48 bits y se usa en el cifrado, el cual se genera de manera dinámica por paquete, lo que lo vuelve una opción adecuada, ya que pone de lado a los ataques de inducción chopchop y estadístico.

En el escenario #2 WPA2-TKIP usa el algoritmo simétrico de bloques AES en el cifrado. Incrementa el tamaño de cifrado a 128 y IV a 48 bits, el cifrado es dinámico por cada paquete y resulta adecuado para la protección de datos impidiendo el ataque de contraseñas por fuerza bruta y los ataques de inducción chopchop y estadístico no representan mayor amenaza para este protocolo.

INDICADOR 2: Integridad

Escenario #1: Nivel Doméstico

Tabla 24
Integridad - Nivel Doméstico

INDICES	WEP		WPA				WPA2			
			TKIP		AES		TKIP		AES	
Integridad de la cabecera	TI	0	I	1	I	1	A	3	A	3
Integridad de cifrado	TI	0	I	1	I	1	A	3	A	3
Integridad dependiente de la llave y IV	TI	0	I	1	I	1	A	3	A	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

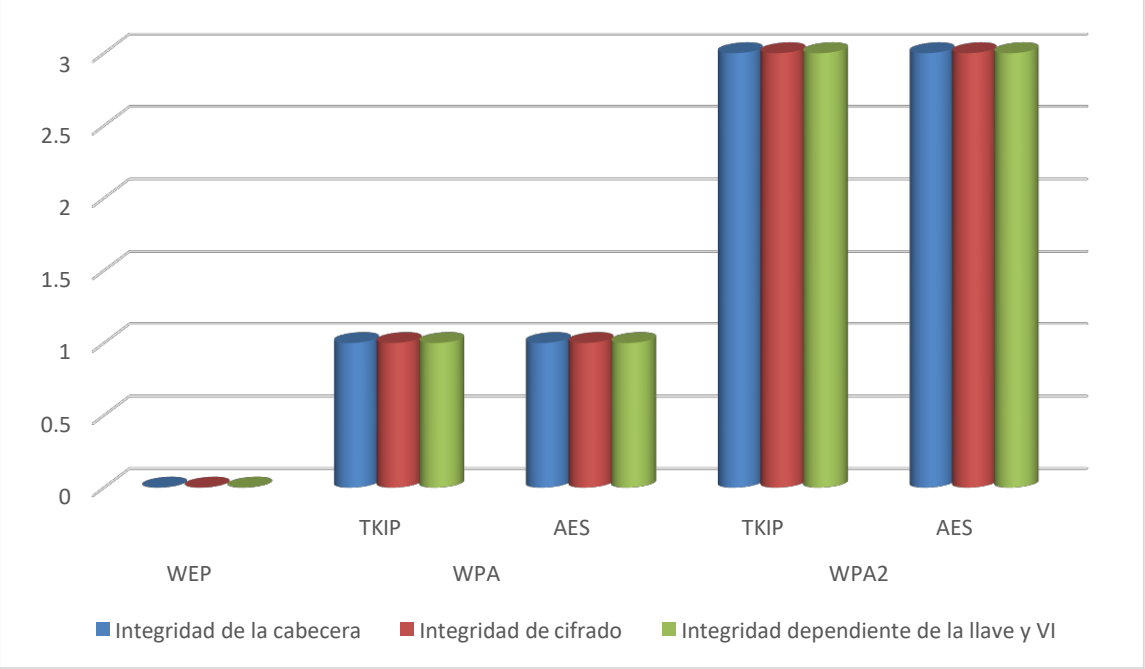

Figura 40. Integridad – Nivel Doméstico

Fuente: Investigación y trabajo de campo (elaboración propia)

Escenario #2: Nivel Corporativo

Tabla 25
Integridad - Nivel Corporativo

INDICES	WPA				WPA2			
	TKIP		AES		TKIP		AES	
Integridad de la cabecera	I	1	I	1	A	3	A	3
Integridad de cifrado	I	1	I	1	A	3	A	3
Integridad dependiente de la llave y IV	I	1	I	1	A	3	A	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

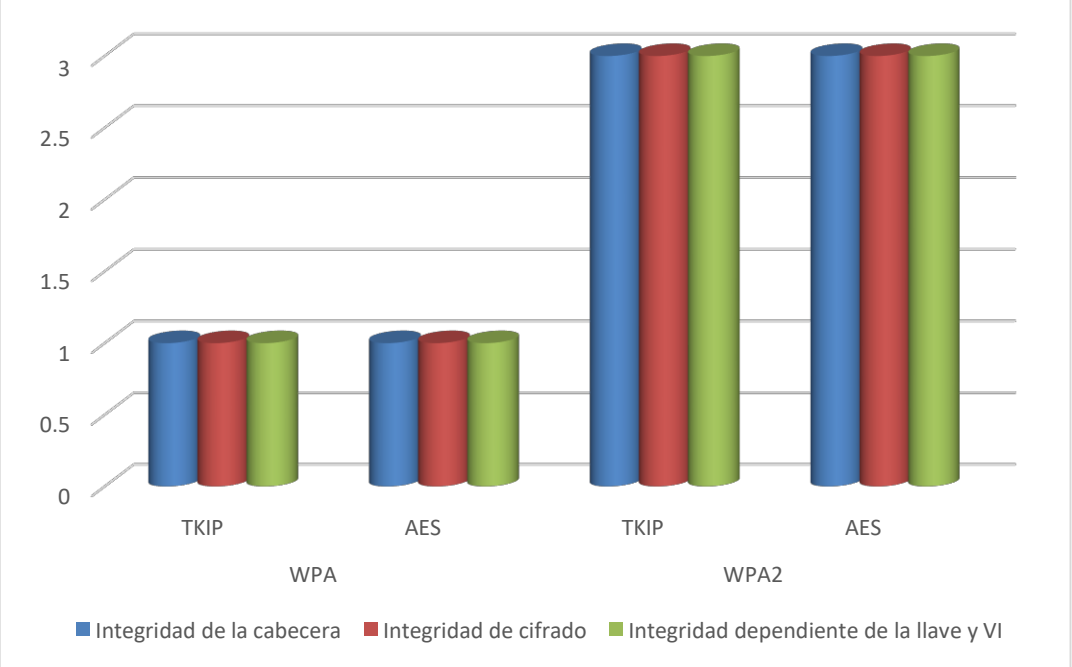

Figura 41. Integridad – Nivel Corporativo

Fuente: Investigación y trabajo de campo (elaboración propia)

Interpretación:

El uso de WEP en el escenario #1, resulta totalmente inadecuado, dado que los ataques por inyección y/o fragmentación son altamente probables. No se aprecia una mejoría en el mecanismo de integridad MIC el mismo que no es cifrado y no depende de la llave ni del IV, es decir, no cuenta con integridad en la cabecera de datos.

En ambos escenarios WPA-TKIP significativamente mejor ante una prueba de redundancia cíclica basa en hash lineal, donde los datos son protegidos con una clave MIC, dependiendo de la llave y el IV, que se fusionan para la generación de claves maestras de cifrado.

En el escenario #2 WPA2-TKIP resulta ser un mecanismo de integridad adecuado, poniendo a un lado los ataques de inyección y fragmentación. El CCM tiene un modo de funcionamiento combinado que utiliza la misma clave

de cifrado para obtener confidencialidad, así como para crear un valor de Comprobación de integridad criptográficamente seguro, autenticidad de paquetes y la secuencia de verificación de trama.

INDICADOR 3: Autentificación

Escenario #1: Nivel Doméstico

Tabla 26
Autentificación - Nivel Doméstico

INDICES	WEP		WPA				WPA2			
			TKIP		AES		TKIP		AES	
Soporta negociación de pre-autenticación	TI	0	TI	0	TI	0	A	3	A	3
Clave automática	TI	0	TI	0	PA	2	I	1	A	3
Autenticación de usuario	TI	0	TI	0	PA	2	I	1	A	3
Autenticación Mutua	TI	0	TI	0	PA	2	I	1	A	3
Uso Protocolos de autenticación	TI	0	TI	0	PA	2	I	1	A	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia

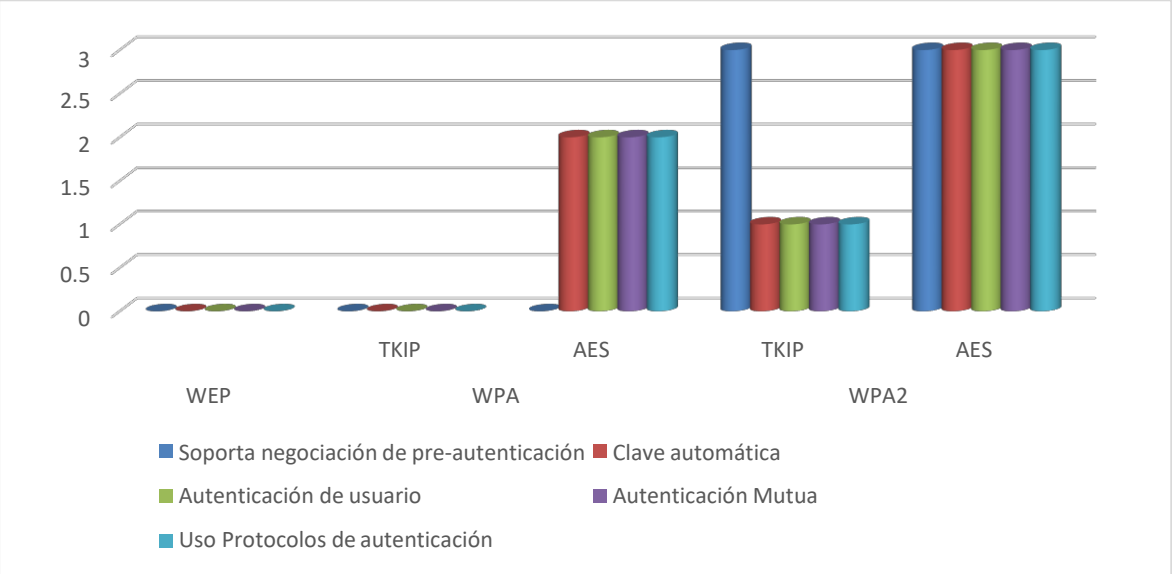

Figura 42. Autentificación – Nivel Doméstico

Fuente: Investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Escenario #2: Nivel Corporativo

Tabla 27
Autentificación - Nivel Corporativo

INDICES	WPA				WPA2			
	TKIP		AES		TKIP		AES	
Soporta negociación de pre-autenticación	TI	0	TI	0	A	3	A	3
Clave automática	TI	0	PA	2	I	1	A	3
Autenticación de usuario	TI	0	PA	2	I	1	A	3
Autenticación Mutua	TI	0	PA	2	I	1	A	3
Uso Protocolos de autenticación	TI	0	PA	2	I	1	A	3

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

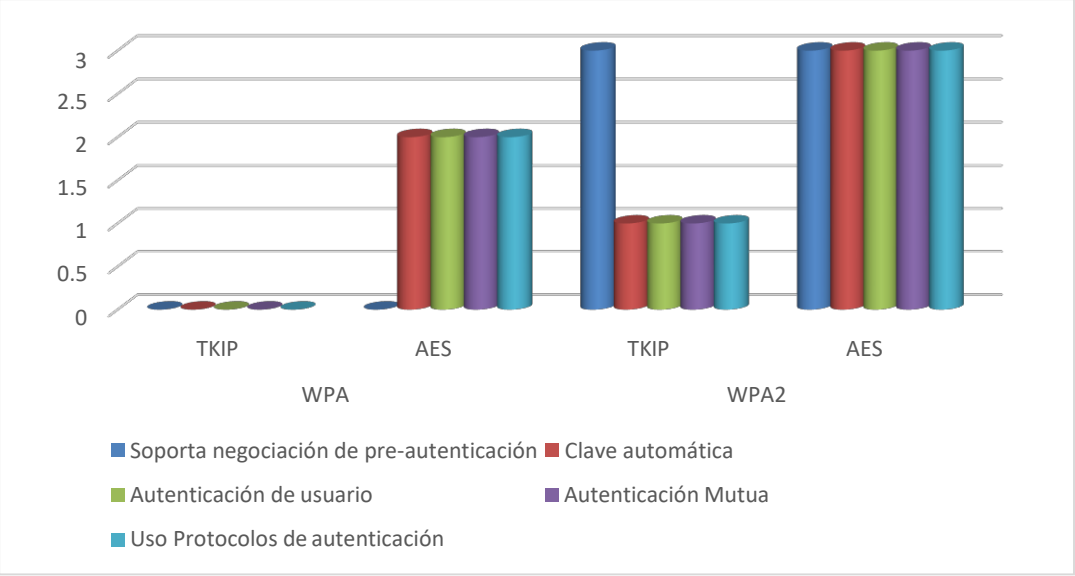

Figura 43. Autentificación – Nivel Corporativo

Fuente: Investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Interpretación:

Resulta totalmente inadecuado el uso de WEP para la autenticación en el escenario #1, puesto que no se distribuye automáticamente, dejando que esta sea configurada en cada usuario, esta se realiza mediante la clave pre-compartida en el medio. Los ataques de fragmentación e inyección y de contraseñas son altamente factibles.

En los protocolos WPA y WPA2 TKIP al igual que en el WEP, no existe la distribución automática de claves y esta es pre-compartida en el medio. No existe autenticación mutua, no existe un servidor, los protocolos de autenticación no están presentes, por ello la clave TKIP cumple este rol. Los ataques de contraseña de fuerza bruta y diccionarios son factibles.

En el escenario #2 WPA2 permite la pre-autenticación, estableciendo la autenticación con AP cercanos previos a completar la autenticación con el seleccionado, impidiendo falsear un AP y evitando ataques de fragmentación e inyección.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Tabla 28
Subtotales del Análisis de la Variable Dependiente – Ambos Escenarios

INDICADOR	INDICES	NIVEL DOMÉSTICO					NIVEL CORPORATIVO			
		WEP	WPA		WPA2		WPA		WPA2	
			TKIP	AES	TKIP	AES	TKIP	AES	TKIP	AES
Confidencialidad	Algoritmo de cifrado mejorado	1	1	2	3	3	1	2	3	3
	Tamaño de algoritmo de cifrado	1	2	2	3	3	2	2	3	3
	Cifrado automático	1	2	2	3	3	2	2	3	3
	IV cifrado y mejorado	1	2	2	3	3	2	2	3	3
Integridad	Integridad de la cabecera	0	1	1	3	3	1	1	3	3
	Integridad de cifrado	0	1	1	3	3	1	1	3	3
	Integridad dependiente de la llave y IV	0	1	1	3	3	1	1	3	3
Autentificación	Soporta negociación de preautenticación	0	0	0	3	3	0	0	3	3
	Clave automática	0	0	2	1	3	0	2	1	3
	Autenticación de usuario	0	0	2	1	3	0	2	1	3
	Autenticación mutua	0	0	2	1	3	0	2	1	3
	Uso de protocolos de autenticación	0	0	2	1	3	0	2	1	3
RESULTADOS TOTALES		**4**	**10**	**19**	**28**	**36**	**10**	**19**	**28**	**36**

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Tabla 29
Sumatoria de Análisis de la Variable Dependiente – Ambos Escenarios

INDICADOR	WEP*2 (*)	WPA		WPA2	
		TKIP	AES	TKIP	AES
Confidencialidad	8	14	16	24	24
Integridad	0	6	6	9	9
Autenticación	0	0	16	14	30
RESULTADOS TOTALES	8	20	38	47	63

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

(*) Los valores de WEP han sido ponderados por 2, para poder homologarlos con los resultados obtenidos en los protocolos WPA y WPA2 en los escenarios 1 y 2

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Dónde:

Puntaje total del Análisis: PT= Σ (Pi máximos por indicador)

Entonces:

PT= 24 + 9 + 30 = 63

Puntaje total de cada Protocolo Analizado: PT_PW= Σ (Pwi)

Porcentaje total de cada Protocolo Analizado: (%PW)= (PT_PW / PT)*100%

Tabla 30
Porcentaje Total de Cada Protocolo Analizado

INDICES	WEP	WPA		WPA2	
		TKIP	AES	TKIP	AES
PT_PW	8	20	38	47	63
PT	63	63	63	63	63
PORCENTAJE POR PROTOCOLO	12.70	31.75	60.32	74.60	100

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Tabla 31
Porcentaje por Protocolo de Variable Dependiente

WEP	WPA		WPA2	
	TKIP	AES	TKIP	AES
13%	32%	60%	75%	100%

Datos obtenidos de la investigación y trabajo de campo (elaboración propia)

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

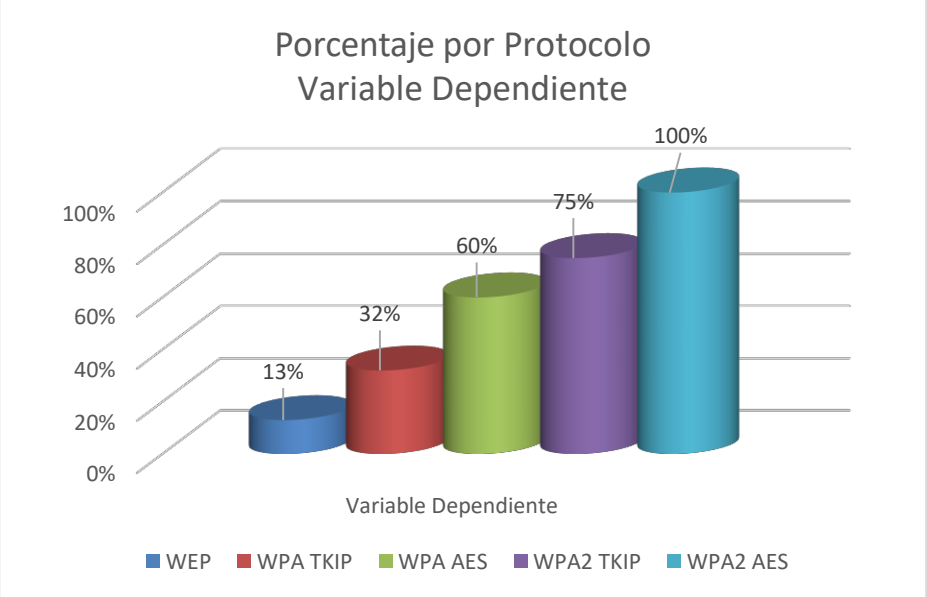

Figura 44. Porcentaje por Protocolo de Variable Dependiente

Fuente: Investigación y trabajo de campo (elaboración propia)

WEP tiene un 13 % de seguridad, WPA-TKIP en un 32% y WPA-AES en 60%, WPA2-TKIP es seguro en un 75% y WPA2-AES en un 100%.

4.2. Discusión de Resultados

En la evaluación se establecieron dos ambientes de prueba, demostrando que en ambos escenarios el protocolo WEP ofrece seguridad en un 13% y es vulnerable a todos los ataques analizados.

WPA-TKIP por ser un protocolo de transición es susceptible en cualquiera de sus variantes a ataques de contraseña (fuerza bruta, de diccionario) ofreciendo seguridad en un 34% en la variable independiente y un 32% en la variable dependiente.

WPA-AES ofrece seguridad de un 81% en la variable dependiente para ambos escenarios y un 60% en la variable dependiente por el algoritmo de cifrado RC4, también es vulnerable al ataque de denegación de servicios.

WPA2-TKIP es vulnerable en cualquiera de sus variantes al ataque de denegación de servicios, proporcionando seguridad en una 38% en la variable independiente y un 75% en la variable dependiente. Del mismo modo WPA2-AES en su variable independiente nos ofrece seguridad de un 94% y un 100% en su variable dependiente, siendo esta la última opción más segura.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

V. CAPITULO V: PROPUESTA DE INVESTIGACIÓN

La presente es una propuesta de solución para la implementación de red inalámbrica Wi-Fi, que cuente con un adecuado sistema de seguridad, basados en su escenario de desempeño, por un lado los ambientes de pequeñas oficinas u hogares oficina, (llamados ambientes SOHO por sus siglas en inglés *Small Office – Home Office*), y por otro lado el ámbito EMPRESARIAL o corporativo.

En toda implementación de red inalámbrica existen de manera inherente, riesgos a los cuales están expuestas estás tecnologías, los cuales mencionaremos a continuación:

Interceptación y Escucha. Esta amenaza atenta directamente contra la confidencialidad de la información. El intruso puede "ver" el tráfico en la red, realizar capturas de claves, leer correos, etc.

Acceso no Autorizado a la Red. Utilizado por el intruso para ingresar a sistemas que normalmente no están permitidos desde el exterior. Si este logra ingresar al sistema, este podrá violar todo en el interior.

Intrusión. Personas no autorizadas podrían ingresar a una red inalámbrica Wi-Fi con poca o nula seguridad para acceder a Internet, haciendo uso de los recursos de alguien más. Esta condición es perjudicial para la calidad del servicio de los usuarios, así como su disponibilidad.

Denegación de Servicio.

Por medio de ataques de generación de tráfico aleatorio excesivo, puntos de acceso falsos.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Man-in-the-Middle. Un atacante podría instalar un AP inalámbrico confundiéndose con los AP legítimos, provocando que un número de usuarios se conecte al del atacante, reenviando este el tráfico a los AP legítimos.

Infección. Un visitante podría conectarse a la red y servir como punto de acceso para virus, troyanos y otros tipos de gusanos.

5.1. Propuesta para Pequeñas Oficinas y Hogares (SOHO)

Hoy en día resulta bastante común encontrar en las diferentes tiendas de electrónica como Radio Shack o las famosas galerías de computación que están dispersas por nuestras ciudades (por ejemplo en Lima: Las Galerías Garcilaso), múltiples ofertas de diversos componentes para implementar de manera domésticas una pequeña red inalámbrica Wi-Fi. Access Point a muy bajos precios pueden ser adquiridos y así tener interconectados diversos dispositivos dentro del mismo ámbito de trabajo.

Se debe tener en cuenta que los mecanismos de protección para este tipo de improvisadas redes domésticas, deben ser igual de rigurosas que en las grandes redes empresariales. En ocasiones, estas WLAN caseras, llegan a cubrir entornos superiores a los deseados, de tal modo que si no se emplean los mecanismos de seguridad adecuados, cualquier usuario podría hacer uso no autorizado de la red y tener acceso a algunos servicios.

A continuación detallaremos las normas de diseño para garantizar seguridad a una pequeña red Wi-Fi, el protocolo de seguridad más adecuado es el WPA2-PSK.

Los elementos de una arquitectura de solución para redes WLAN de tipo SOHO,

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

en los cuales podemos implementar mecanismos de seguridad WPA2-TKIP son: Usuario, Access Points, Protocolos, cuyas consideraciones a seguir se detallan a continuación:

5.1.1. Usuario (Consideraciones)

Reserva y confidencialidad en la divulgación de contraseñas.

Prudencia al almacenar las claves de acceso (no usar notas escritas y dejarlas al alcance de cualquier otro usuario)

Uso de contraseñas fuertes (largas, con caracteres especiales, etc)

Uso de antivirus y firewalls y actualizarlos periódicamente.

5.1.2. Access Point (Consideraciones)

Adquirir Access Points actualizables, cambiarles los parámetros por default.

Configurar el cifrado a WPA2-TKIP

Fijar de manera física los Access points.

Deshabilitar el broadcast SSID para evitar el acceso a usuarios no deseados.

Hacer uso de las listas de control de acceso (ACL), solo para aquellos usuarios cuyas MAC estén registradas en la lista de control. Activar el filtrado MAC.

Implementar Access Points que bloqueen la intercomunicación de usuarios conectados mediante la opción “intracell blocking”

Reducir el nivel de cobertura del AP solo al ámbito necesario de trabajo

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

5.1.3. Protocolos de Seguridad (Consideraciones)

Si bien es cierto que no podemos asegurar que el protocolo IEEE 802.11 con WPA2-PSK es 100% seguro, una buena generación de contraseñas puede aportar mucho en la seguridad del mismo:

La generación de claves de más de 8 caracteres, prácticamente impiden su ruptura, debido al tiempo que tomarían los programas para descubrirla.

Hacer uso de generadores de contraseñas. Hoy en días existen muchas opciones online para generar contraseñas WEP, WPA y WPA2, también existen aplicaciones descargables como el Wireless Key generator, con el cual se pueden generar claves aleatorias y asignarlas al router.

Gracias a estas aplicaciones es posible generar contraseñas muy complejas, a veces tan complejas que resulta muy difícil memorizarlas, sin embargo vale la pena considerarlas a fin de asegurar la integridad de nuestras redes inalámbricas Wi-Fi.

5.2. Propuesta EMPRESARIAL (Corporativa)

Cuando de una empresa se trata, es muy importante observar las políticas de seguridad establecidas, a fin de que toda implementación tecnológica se encuentra alineada a las mismas. Cabe señalar que la excesivas normas de seguridad de las compañías podrías reducir la eficiencia de funcionamiento de las redes inalámbricas Wi-Fi. Aquí se señalan las normas básicas de diseño para garantizar la seguridad en una red EMPRESARIAL. La solución más adecuada de seguridad está basada en WPA2-ENT con IEEE 802.1x y el protocolo EAP-TTLS para autenticación de los usuarios.

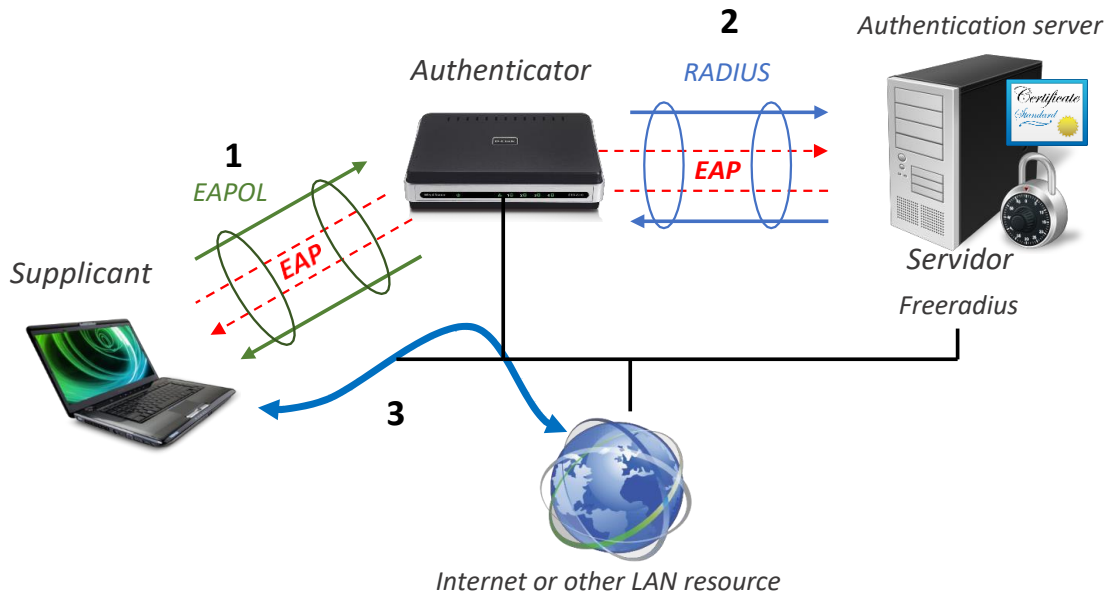

Figura 45. Elementos de solución WPA2 ENT / EAP-TTLS

Fuente: Adaptado de https://bit.ly/2EKDlQL

5.2.1. Políticas Generales Empresariales

Ingeniería Social

La concientización de los usuarios para que no "compartan" información sensible, como las contraseñas, es vital para los sistemas de seguridad. Reducir al mínimo posible la divulgación de información crítica.

Entorno de red

Toda nueva implementación debe respetar las políticas de seguridad existentes.

Control de contraseñas. Debe existir un personal (o software) que controle la complejidad y características mínimas de las contraseñas, las mismas que deben ser obligatoriamente cambiadas periódicamente.

La realización de inspecciones físicas de manera periódica es otro factor

importante para detectar la presencia de Access points no autorizados.

Uso de perfiles de usuario administrador que controlen el accesos de usuarios internos y externos.

Arquitectura de red

Las redes WLAN deben estar asignadas a una subred dedicada y no compartida con una red LAN. Entre una WLAN y una LAN debe estar presente una estructura de Firewall adecuada, así como también mecanismos de autenticación.

A fin de proteger los servidores del entorno Empresarial de los ataques de denegación de servicio, los servicios deben ubicarse en una zona desmilitarizada (DMZ).

Access Point

Adquirir Access Points actualizables, cambiarles los parámetros por default.

Configurar el cifrado WPA2-TKIP

Si los AP soportan varios mecanismos de seguridad, configurar solo uno.

Deshabilitar el broadcast SSID para evitar el acceso a usuarios no deseados.

Hacer uso de una VLAN propia para la red Wi-Fi en los equipos que lo permitan. Se recomienda mantenerla separada de la red cableada en todo momento.

Consideraciones Físicas de la Señal

Emplear materiales de construcción que no permitan la propagación de la señal fuera del recinto de trabajo.

Considerar el uso de equipos que inhiban la señal inalámbrica en lugares donde no se requiera.

Fijar de manera física los Access points y ubicarlos en zonas donde no sufran daños ni averías.

No permitir el ingreso de equipos electrónicos a personal no autorizado.

Los APs deben brindar una señal aceptable en cualquier ubicación.

Mejorar los APs para implementación de las normas 802.11x

5.2.2. Arquitectura de Red

Observando las consideraciones anteriormente citadas, los componentes que se incluyen en una infraestructura segura para red inalámbrica Wi-Fi Empresarial son los siguientes:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

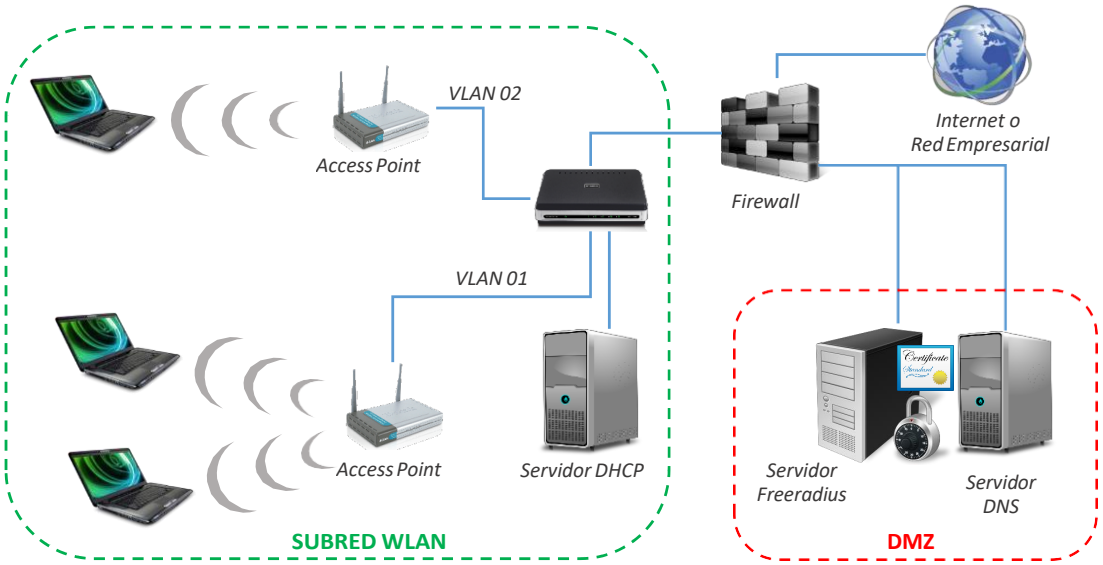

Figura 46. Arquitectura de Red Empresarial

Fuente: Adaptado de https://bit.ly/2qw9czy

Como se aprecia en la imagen anterior, se consideran algunos elementos importantes para la seguridad de la red, como son:

Switches de capa 2 o 3. Que proporcionan conectividad Ethernet entre los APs y la red empresarial, la segmentación en diferentes VLANs coopera en una mejor administración y confidencialidad entre usuarios.

Firewall. Que gestiona el acceso de los usuarios Wi-Fi a la red cableada, actuando como puente entre las VLANs o como un elemento de control. La implementación de un Firewall es útil para crear políticas de acceso más seguras.

Servidor DHCP. El cual brinda un direccionamiento dinámico de IPs a los clientes inalámbricos.

Los componentes fundamentes para una implementación de solución WPA2 Empresarial son:

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Suplicante

Solicita la autenticación, el cliente, solución basada en el framework de autenticación EAP (Extensible Authentication Protocol). La solución wpa_suplicant es un suplicante para WPA Linux, BSD, Mac OS y Windows con soporte para WPA y WPA2 (IEEE 802.11i / RSN). Adecuado tanto para PCs como para laptops y sistemas embebidos.

Autenticador

Elemento al que se conectará el suplicante. Transfiere la información al servidor de autenticación. Los APs se configuran para aceptar solo a las conexiones WPA2 y rechazar a las demás. Los dispositivos de la arquitectura deben soportar este mecanismo de seguridad.

Servidor de Autenticación

Elemento que evalúa la autenticación del suplicante enviando una respuesta al autenticador. Proporciona la autenticación de los usuarios a la red WLAN, encargada de generar las claves dinámicas utilizadas en el mecanismo WPA2 y enviarlas a los APs. Freeradius es el servidor RADIUS más popular en código abierto, compatible con todos los protocolos de autenticación, es veloz y con potente en características modulares y escalables.

Otras consideraciones a tener en cuenta al implementar una arquitectura segura de red inalámbrica Wi-Fi son:

El sistema de gestión de contraseñas de administración de APs debe ser equivalente a la gestión de contraseñas de cualquier otro servidor.

Se deben emplear canales seguros (SSH, SSL, etc) para la administración de APs. Gestionar y monitorear los APs.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Segregación de redes, DMZs, Firewalls y asignación de VLANs para los clientes de Wi-Fi, para un mayor control de acceso.

Auditoría y monitoreo de los registros de acceso del servicio RADIUS.

5.2.3. Controlador de APs

Su implementación facilita la gestión y mantenimiento de la red Wi-Fi, aumentando así también los niveles de seguridad. Algunas de las bondades encontradas en estos controladores se mencionan a continuación: *Firewall*. Que controla el tráfico de la red cableada a la inalámbrica, basada en direcciones de origen y/o destino, aplicaciones, etc. *La Comunicación por Túnel.* Permite que los APs estén conectados a segmentos diferentes de red, así el tráfico de los clientes siempre accederá a la red por el mismo punto, es decir al que esté conectado el controlador. *Gestión por Usuario*. Posibilita asignar diferentes accesos a los usuarios en función de sus credenciales, de una manera más detallada y compleja. *Gestión del Ancho de Banda*. Regula el ancho de banda disponible en función de la aplicación o usuario.

5.2.4. Sistema de Prevención de Intrusos en Red Inalámbrica (WIPS)

Los WIPS monitorean el espectro de radio de la red inalámbrica Wi-Fi, con la finalidad de detectar ataques y/o fallos, como son: APs infiltrados, APs mal configurados, ataques de denegación de servicio, etc. Los WIPS detectan el comportamiento inusual de los clientes, parámetros y configuraciones erróneas. En caso de detectarse un equipo infiltrado el WIPS notificará al administrador de la red, bloqueando inicialmente al punto infiltrado.

5.2.5. Herramientas de Gestión

La elección de un software de gestión de redes es algo de importancia, ya que este debe mostrar la cobertura de la red inalámbrica Wi-Fi, localizar los APs y detectar las configuraciones de seguridad de las redes disponibles. Existen soluciones comerciales como Open Source para gestionar las redes inalámbricas, permitiendo evaluar el rendimiento de la red según la aplicación y no tan solo por la señal recibida. Soluciones como: Chanalyzer Pro, Wireshark, Iperf, Airmagnet, InSSIDer disponibles en el mercado son muy buenas alternativas como aplicaciones de gestión y análisis.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

VI. CAPITULO VI: CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

Al realizar el estudio de las posibilidades, limitaciones y seguridades de las tecnologías inalámbricas para redes Wi-Fi, se pudo conocer a detalle su funcionamiento y deficiencias mediante el análisis comparativo de las vulnerabilidades.

Concluimos que el protocolo WEP ofrece un mínimo de 13% de protección y representa la mayor cantidad de vulnerabilidades a todos los ataques analizados, mientras que WPA2-AES cuenta con un promedio del 97% de protección, determinando a este protocolo como la mejor opción para asegurar de las vulnerabilidades analizadas.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

RECOMENDACIONES

Se recomienda excluir el uso de los protocolos WEP o WPA en entornos SOHO como mecanismos de seguridad ya que se verificó que son vulnerables; en caso que los equipos no soporten el protocolo WPA2 tener en cuenta las consideraciones para la generación de claves.

No solo se debe tener como opción el uso del Protocolo WPA2 AES, como único mecanismo seguro, tener en cuenta seguridades complementarias como son firewalls, VLANs, sistema de detección de intrusos que permitan excluir, filtrar y monitorear cualquier cambio inadecuado en la WLAN para su correctivo inmediato.

El uso de herramientas de gestión inalámbricas libres está aún dependiente de un porcentaje minoritario de compatibilidad de hardware, se debería tener en cuenta este aspecto al momento de querer monitorizar una red Wi-Fi ya que no todas las tarjetas inalámbricas permiten poder configurarlas para este propósito.

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

REFERENCIAS

Vano, M., Piessens F., (2017), Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. Recuperado de: https://papers.mathyvanhoef.com/ccs2017.pdf.

Monsalve, J., Aponte, F., Chaparro, F., (2015), Análisis de seguridad de una muestra de redes WLAN en la ciudad de Tunja, Boyacá, Colombia. *DYNA, 82 (189), 226-232,* doi: https://doi.org/10.15446/dyna.v82n189.43259

Giménez, J. (2014). *Seguridad en equipos informáticos***.** Madrid, España: IC Editorial.

Moreno, J., Santos, M. (2014). Sistemas Informáticos y Redes Locales. España

Begoña L. (2012). *Seguridad en Comunicaciones Sin Hilo: Riesgos y Amenazas Wi-Fi* (tesis de pregrado). Universitat Oberta de Catalunya, España.

Suarez, M. (2012). *Mecanismos De Seguridad En Redes Inalámbricas*. México

Ruz, J., Riveros, B., Varas, A., (2012) Redes WPA/WPA2. Chile

Campus Universitario Km. 5 Carretera a Pimentel - Chiclayo - Perú
Teléf: (+51)(74) 481610 / 481620 - Fax: 203861
www.uss.edu.pe

Pellejero, I., Andreu, A., Lesta. A., (2005), *Seguridad en redes WLAN. Conozca lo esencial para su empresa.* Colección Guías Técnicas, España: Enpresa Digitala.

Karygiannis, T., (2002), Wireless Network Security 802.11, Bluetooth and Handheld Devices. EU: NIST Publications. Recuperado de https://www.nist.gov/publication-type/nist-pubs

Esmoris, D., (2009), *Control de Acceso a Redes* (tesis de pregrado). Universidad Nacional de La Plata, Argentina.

Revelo, J., Pazmiño, E., (2008), Análisis de WPA/WPA2 vs WEP. Ecuador: CYBSEC Security Systems. Recuperado de http://www.cybsec.com/upload/

Iniesta M., (2010). *Seguridad WI-FI. Agresiones posibles* (tesis de pregrado) Universidad Politécnica de Valencia. España.

SaC de Paz, J., (2010), *Estudio de vulnerabilidad en los cifrados WEP, WPA y su impacto en las redes inalámbricas de área local* (tesis de pregrado). Universidad de San Carlos de Guatemala, Guatemala.