PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR



FACULTAD DE INGENIERIA

MAESTRÍA EN REDES DE COMUNICACIONES

INFORME FINAL CASO DE ESTUDIO PARA UNIDAD DE TITULACION ESPECIAL

TEMA

PROPUESTA DE MEJORA EN LA SEGURIDAD DE REDES INALÁMBRICAS, UTILIZANDO LOS ESTÁNDARES DEFINIDOS POR NIST. CASO DE ESTUDIO: RED WIFI DE LA IES.

AUTOR: VÍCTOR HUGO GÁLVEZ CAZA

DIRECTOR: Mgt. ALBERTO PAZMIÑO PROAÑO

Quito, Agosto 2017

AUTORÍA

Yo, Víctor Hugo Gálvez Caza, portador de la cédula de ciudadanía No. 1707796536, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se he respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

_____

Víctor Hugo Gálvez Caza

CONTENIDO

Pág.

1. INTRODUCCION. 1
2. JUSTIFICACION 3
3. ANTECEDENTES 5
4. OBJETIVOS 7
5. ALCANCE 8
6. DESARROLLO CASO DE ESTUDIO 9
   6.1. Redes inalámbricas. Generalidades. 9
      6.1.1. Definición de red inalámbrica de área local (WLAN). 9
      6.1.2. Topología y Configuración de la WLAN 11
   6.2. Normalización IEEE para WLAN. 14
      6.2.1. IEEE 802.11. 15
   6.3. Hardware de Red Inalámbrica 17
   6.4. Seguridad de red de área local inalámbrica (WLAN). Redes Abiertas 21
      6.4.1. Ataque Denegación de Servicio (DoS) 21
      6.4.2. Descubrir ESSID ocultos. 21
      6.4.3. Ataque Man in the middle 22
      6.4.5. WEP – Privacidad Equivalente al Cable 22
      6.4.6. WPA 23
      6.4.7. WPA2 24
      6.4.8. Privacidad e Integridad con TKIP 25
      6.4.9. Autenticación mediante 802.1X/EAP 25
      6.4.10. Extensible Authentication Protocol - EAP. TLS. 27
      6.4.11. Ataque WPA – PSK 28
      6.4.12. Portales cautivos 29
      6.4.13. Rogue Access Point (AP) 30
   6.5. Aplicación de NIST en la Gestión de Seguridades de Redes WIFI 34
      6.5.1 NIST. Propósito 34
      6.5.2. Aplicación de NIST en la Gestión de Seguridades de Redes WIFI 34
      6.5.3. Autenticación. 38
      6.5.4. Arquitectura de WLAN según estándar NIST. 39

6.5.5. Implementación, evaluación y mantenimiento de la configuración WLAN 43
6.5.6. Monitoreo de ataques. 44
7. RESULTADOS 47
7.1. DESARROLLO LISTAS DE VERIFICACIÓN 47
8. CONCLUSIONES Y RECOMENDACIONES. 56
8.1. CONCLUSIONES. 56
8.2. RECOMENDACIONES. 61
9. GLOSARIO DE TÉRMINOS 63
BIBLIOGRAFÍA 67
ANEXOS 72

CONTENIDO DE ILUSTRACIONES

Ilustración **Pág.**

Ilustración 1. Organigrama Estructural de la Institución de Educación Superior (IES). 5
Ilustración 2. Configuración punto a punto o Ad–Hoc..... 12
Ilustración 3. Configuración en Modo Punto de Acceso o Modo Infraestructura. 13
Ilustración 4. Bridge 19
Ilustración 5. Switch. 19
Ilustración 6. Routers. Diagrama de Funcionamiento. 20
Ilustración 7. Vista simplificada de la arquitectura WLAN. 35
Ilustración 8. Falta de seguridad de extremo a extremo de las funciones de seguridad WLAN WEP. 36
Ilustración 9. Autenticación de clave compartida. 39

CONTENIDO DE TABLAS

Tabla		Pág.
1	Norma IEEE 802…….	15
2	Parte Técnica……..	48
3	Diseño Lógico de Red…….	49
4	Configuración, autenticación y cifrado……...	50
5	Administración de Recursos Humanos……...	52
6	Comparación NIST…….	54

CONTENIDO DE GRÁFICOS

Gráfico		Pag.
1	Parte Técnica……..	48
2	Diseño Lógico de Red…….	49
3	Configuración, autenticación y cifrado……...	50
4	Administración de Recursos Humanos……...	52
5	Comparación NIST…….	54

1. INTRODUCCION

En la actualidad, la telefonía inalámbrica y su constante evolución han capturado la atención de los profesionales de esta área del conocimiento, forzado esto por el deseo y necesidad de los usuarios de romper las conexiones físicas y garantizar un máximo de movilidad. Lo anterior ha generado un continuo mejoramiento de las redes inalámbricas alrededor del mundo, dando como resultado sistemas de comunicación complejos y cada vez más eficientes.

Los sistemas de comunicación inalámbricos han evolucionado de forma constante a lo largo de las últimas décadas, pasando de ser una generación caracterizada por transferencia de datos por vía analógica, hasta lograr la comunicación utilizando archivos digitalizados de voz y datos con altas velocidades de transmisión y el uso generalizado de banda ancha. La utilización conjunta de estos elementos ha impulsado en la actualidad los modernos sistemas de comunicación alámbricos e inalámbricos, caracterizados por altas velocidades de transmisión de datos y mayor calidad en el procedimiento.

Sin embargo, aun con las ventajas tecnológicas existentes, la acelerada evolución y tecnificación de las redes han generado limitantes de interés, que han debido ser abordadas por los técnicos en el área alrededor del mundo. En este contexto se destaca, el escaso control por medio de barreras físicas de las ondas de radio en la actualidad, por lo cual estas pueden ser captadas desde cualquier punto incluido en su zona específica de cobertura.

Se generan así las vulnerabilidades y potenciales riesgos de seguridad de las redes WLAN, los cuales han sido convenientemente estudiados, surgiendo estándares internacionales como, el publicado por el Instituto Nacional de Estándares y Tecnología (NIST), que definen los protocolos de seguridad que pueden ser aplicados en las organizaciones alrededor del mundo a fin de garantizar la seguridad de las WLAN utilizadas, optimizando así su funcionamiento y aprovechando al máximo sus ventajas operativas.

En este orden de ideas y dada la importancia de lo descrito, surge la intención de desarrollar el presente trabajo investigativo denominado Propuesta de Mejora En la Seguridad de Redes Inalámbricas, utilizando los Estándares definidos por NIST. Caso de Estudio: Red WIFI de una Institución de Educación Superior (IES), el cual persigue analizar las vulnerabilidades de estas redes inalámbricas según el estándar mencionado, describir los problemas concretos que afrontan en el tema de seguridad y proponer estrategias de optimización.

2. JUSTIFICACION

El acceso sin necesidad de cables, es la razón que hace tan populares a las redes inalámbricas, convirtiéndose a la vez el problema más grande de este tipo de redes en cuanto a seguridad se refiere. Lo grave de esta situación es que muchos administradores de redes parecen no haberse dado cuenta de las implicaciones negativas de poseer puntos de acceso inalámbrico en la misma red. En este escenario, un punto de acceso inalámbrico mal configurado se convierte en una puerta que vulnera por completo la seguridad informática de la red, siendo imprescindible implementar técnicas que protejan de una forma más efectiva la seguridad en las redes. Es allí donde el NIST como estándar, desarrollado en Estados Unidos y utilizado internacionalmente, su conocimiento y aplicación en las organizaciones e instituciones del país cobra vital relevancia.

Tomando como base lo descrito y debido a la definitiva importancia de su estudio, surge la necesidad de desarrollar la presente investigación, tomando como unidad de análisis una institución de educación superior (IES), en la cual fueron detectados evidentes problemas en la red WIFI tanto desde el punto de vista tecnológico como académico. En el aspecto tecnológico se evidencia que para el ingreso a la red WIFI los estudiantes y docentes deben colocar su usuario y contraseña en la página web que se les presenta, misma que no se encuentra encriptada. Por otra parte, no se utilizan las contraseñas LDAP definidas para cada uno de los usuarios dando la facilidad para que cualquier persona que no pertenece a la IES pueda capturar esta información y conectarse a la red.

Por otra parte, no existe un tiempo de inactividad en el uso de la plataforma y de conexión a la red, lo que deja a disposición de cualquier usuario su permanencia en el browser e ingreso a la información de la IES. Igualmente, no existe un refrescamiento de claves en la administración de usuarios de la red, eliminación de usuarios en la cuenta de correo ya que no están en el dominio de la IES, ni existe el puerto seguro para la conexión de equipos externos que no pertenecen a la universidad. Desde el punto de vista académico, los equipos dentro de la organización usan conexiones duales que ponen en riesgo la integridad de los datos.

Tomando como base este diagnóstico inicial, destaca la importancia de proponer mejoras en la seguridad de las redes inalámbricas de la institución educativa objeto de estudio, utilizando para ello los estándares NIST reconocidos mundialmente, siendo este el principal objetivo de esta investigación. La definición de los lineamientos de seguridad, ajustados a las condiciones y recursos de la IES, permitirá el cumplimiento de los objetivos inicialmente trazados.

3. ANTECEDENTES

Tal y como se ha indicado, la investigación a realizar será llevada a cabo en las instalaciones de una Institución de Educación Superior (IES), la cual, desde el punto de vista operativo, cuenta con áreas de trabajo que incluyen mesa de servicios, administración de base de datos, departamento técnico, coordinación académica y el Departamento de Nuevas Tecnologías, en el cual funciona el Instituto de Informática y Computación (IDIC), seleccionado como caso de estudio (Ilustración 1).

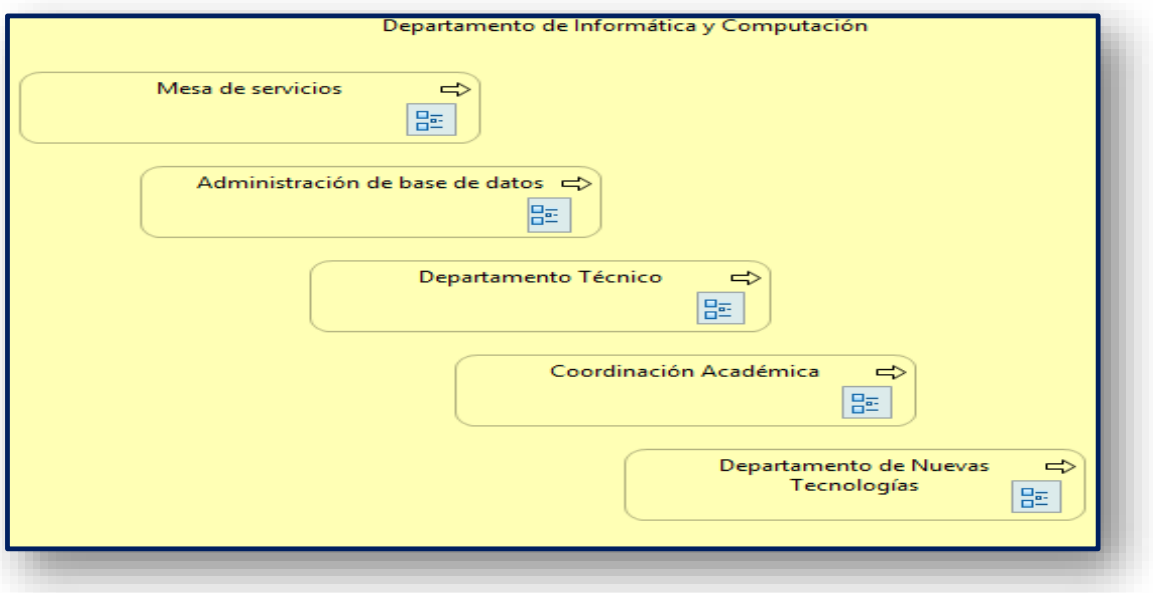


Ilustración 1. Organigrama Estructural de la Institución de Educación Superior (IES).

Fuente: Institución de Educación Superior (IES) (2017).

La *Mesa de servicios*, tiene como función recibir incidentes tanto de software como de hardware por medio de llamada telefónica, mail, sistema de trámites o personalmente y brindando una solución inmediata al problema planteado o caso contrario, enviando el incidente a personal técnico pertinente. La *Administración de base de datos* tiene a su cargo los procesos de diseño, implantación, monitoreo, seguridad y planificación de las bases de datos de la Universidad.

Por su parte, el *Departamento Técnico*, se encarga de brindar soporte a la Universidad en todo lo relativo con el planeamiento, adquisición, administración y mantenimiento de hardware. Igualmente, entre sus funciones se encuentra ofrecer, dada la experiencia de los técnicos, a la empresa ecuatoriana asesoría e instalación de software, Networking, cableado estructurado, Internet, coordinar las relaciones con organismos nacionales e internacionales utilizando las tecnologías de la información y comunicación vigentes, administrar los recursos de redes de la Universidad tales como: Cableado estructurado, Networking, Telefonía IP, Video Conferencia y fomentar y coordinar las relaciones de la Universidad con otros centros de información.

Adicionalmente, se encarga de planificar y ejecutar programas de mantenimiento preventivo y correctivo usados en la red y demás sistemas de comunicación, planificar y ejecutar programas de renovación tecnológica, a fin de garantizar la actualización necesaria para mantener los niveles de calidad que requiere la Institución y planificar y coordinar la incorporación de la Universidad al backbone nacional del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado y su posterior integración a las Redes Avanzadas Latinoamericanas y europeas de Ciencia y Tecnología: a) Área de Redes: Encargado de la gestión de la red de la IES, b)Área de Hardware: Encargado de realizar el mantenimiento y soporte técnico a usuarios de la IES.

La Coordinación Académica, se encarga de proporcionar el servicio de laboratorios a todos los programas de la Universidad que utilizan herramientas

informáticas en el proceso de aprendizaje. Mientras que el *Departamento de nuevas Tecnologías,* se encarga de analizar e incorporar soluciones a nuevas necesidades educativas que pueden ser satisfechas en el ámbito del Campus Virtual.

4. OBJETIVOS

4.1 Objetivo General

Mejorar la Gestión de Seguridades para la red WIFI de una Institución de Educación Superior basado en los estándares definidos por NIST.

4.2. Objetivos Específicos

- Estudiar las recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST) relacionadas con los mecanismos de seguridad en la red WIFI IESONAIR.
- Diagnosticar los mecanismos de seguridad de la red WIFI IESONAIR utilizados en la Institución de Educación Superior (IES), seleccionada como objeto de estudio.
- Comparar los mecanismos de seguridad de la red WIFI IESONAIR recomendados por el Instituto Nacional de Estándares y Tecnología (NIST), con el procedimiento cumplido en la Institución de Educación Superior (IES) seleccionada.
- Proponer un modelo de gestión para optimizar la seguridad de la red WIFI IESONAIR de la Institución de Educación Superior (IES) Universidad seleccionada, con base en los estándares recomendados por Instituto Nacional de Estándares y Tecnología (NIST).

5. ALCANCE

En la red WIFI de la IES seleccionada se propondrá el modelo de gestión de seguridad en la que se definirán lineamientos que permitan optimizar la seguridad de la red inalámbrica de la institución, de allí la importancia de su estudio. Estas estrategias, al ser convenientemente implementadas, permitirán asegurar la protección de la red, la información delicada y los puntos de acceso a la red WIFI. Igualmente, permitirán mitigar los riesgos en los puntos de acceso de la red, identificar y autenticar la información en la red mediante el LDAP y controlar el acceso de personas no autorizadas a la red de la IES.

Para ello se utilizarán las recomendaciones del Instituto Nacional de Estándares y Tecnología (NIST) para la seguridad de las redes WIRELESS en lo que respecta a la gestión de la seguridad de la información de la red WIFI IESONAIR de la IES.

6. DESARROLLO CASO DE ESTUDIO

6.1. Redes inalámbricas. Generalidades.

6.1.1. Definición de red inalámbrica de área local (WLAN).

Tomando en cuenta lo establecido por Madrid (2004) una red inalámbrica (wireless network, por sus siglas en inglés) es aquella utilizada en el mundo informático para distinguir la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada o alámbrica. La transmisión y la recepción se realizan a través de puertos. Indica el autor mencionado que una de sus principales ventajas es la reducción significativa de los costos operativos, ya que se elimina el cableado Ethernet y conexiones físicas entre nodos. Sin embargo, tiene una desventaja considerable ya que, para este tipo de red, el protocolo de seguridad debe ser mucho más exigente y robusto, a fin de evitar intrusos. Según su cobertura, las redes inalámbricas se pueden clasificar en diferentes tipos: Wireless Personal Área Network (WPAN), Wireless Metropolitan Área Network (WMAN), Wireless Wide Área Network (WWAN) y Wireless Local Área Network (WLAN).

Ahora bien, en este contexto y tomando como base las palabras de Camargo (2011), las redes inalámbricas de área local, WLAN por sus siglas en inglés (Wirless Local Area Network), representan:

> Un sistema de comunicación que transmite y recibe datos utilizando ondas electromagnéticas (aunque también es posible con luz infrarroja), en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN convencionales, y que proporciona conectividad inalámbrica de igual a igual (peer to peer), dentro de un edificio o en un área de cobertura. Las WLAN se encuadran dentro de los estándares desarrollados por el IEEE (Instituto de Ingenieros

> Eléctricos y Electrónicos) para redes locales inalámbricas. Comúnmente cubren distancias de los 10 a los 100 de metros. Esta pequeña cobertura contiene una menor potencia de transmisión que a menudo permite el uso de bandas de frecuencia sin licencia (p. 63).

Por su parte Rocha (2009), afirma que una red de área local inalámbrica (WLAN) implementa un sistema flexible de comunicación de datos con frecuencia aumentando en lugar de reemplazar una LAN cableada dentro de un edificio o campus. Estas redes utilizan radiofrecuencia para transmitir y recibir datos sobre el aire, minimizando la necesidad de conexiones por cable, estando constituidas por los denominados puntos de acceso (PA) y los dispositivos de cliente (DC). Los PA actúan como un concentrador que recoge y remite la información recibida vía radio a los DC, los cuales frecuentemente son un PC o PDA con una tarjeta de red inalámbrica, instalada en un slots libre o bien enlazada a los puertos USB de los equipos.

Sobre el tema indica Martínez (2016) por su parte, que una red inalámbrica posee una serie de características entre las que se cuentan:

Movilidad: por medio de la cual se proporciona a los usuarios de una LAN acceso a la información en tiempo real independientemente del lugar donde se ubique dentro de una empresa u organización, lo cual confiere mayores oportunidades servicio, crecimiento exponencial y en general de crecimiento, en comparación con una red alámbrica.

Simplicidad y rapidez en la instalación: lo que facilita el procedimiento a realizar y evita la exposición del cableado a través de paredes y/o techos, respetando la integridad de la infraestructura.

Flexibilidad en la instalación: permitiendo a la red acceder a lugares donde esto se dificulta con una red alámbrica.

Costo de propiedad reducido: si bien el costo inicial de instalación de una red inalámbrica suele resultar más elevado en comparación con una inalámbrica, en líneas generales la inversión resulta ser más baja al analizar los costos totales generados en el ciclo de vida de la misma.

Escalabilidad: los sistemas de WLAN pueden configurarse en diversas topologías a fin de cubrir los requerimientos de aplicaciones o de instalaciones determinadas, siendo muy fácil cambiar la configuración, así como la incorporación de usuarios a la red.

6.1.2. Topología y Configuración de la WLAN

López (2002) menciona que, la complejidad de una red de área local inalámbrica varía, dependiendo de las necesidades a cubrir y en función de los requerimientos del sistema que se quiera implementar. Concuerda Camargo (2011) quien por su parte opina que la versatilidad y flexibilidad de las redes inalámbricas es el motivo por el cual la complejidad de una LAN implementada con esta tecnología sea tremendamente variable, ayudando esta gran variedad de configuraciones a que "este tipo de redes se adapte a casi cualquier necesidad" (p. 67). Según Camargo (2011), estas configuraciones se pueden dividir en dos grandes grupos, las redes Peer to Peer y las que utilizan Puntos de Acceso. Tomando como base lo establecido por Camargo (2011), se resumen a continuación las principales características de los dos grupos mencionados.

La *Configuración Peer-to-Peer (Ad-Hoc)*: también conocidas como redes ad-

hoc, es la configuración más sencilla ya que en ella los únicos elementos necesarios son terminales móviles equipados con los correspondientes adaptadores para comunicaciones inalámbricas. En este tipo de redes, el único requisito deriva del rango de cobertura de la señal, ya que es necesario que los terminales móviles estén dentro de este rango para que la comunicación sea posible. Por otro lado, estas configuraciones son muy sencillas de implementar y no es necesario ningún tipo de gestión administrativa de la red (Ilustración 2).

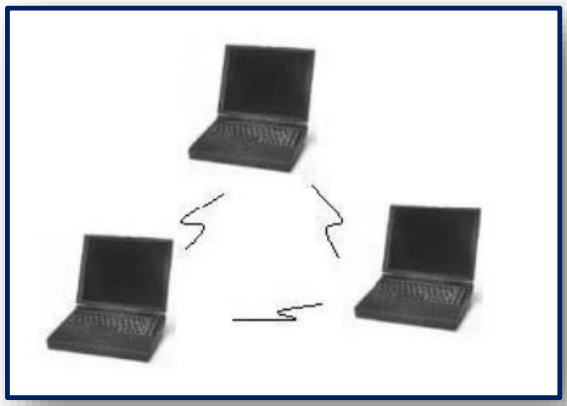


Ilustración 2. Configuración punto a punto o Ad–Hoc.
Fuente: Oliver y Escudero (1999).

Siguiendo con el análisis de Camargo (2011*), la Configuración en modo Punto de Acceso* (Ilustración 3), también conocidas como *configuraciones en Modo Infraestructura*, utilizan el concepto de celda ya usado en otros sistemas de comunicación inalámbrica como la telefonía móvil. Una celda podría entenderse como el área en el que una señal radioeléctrica es efectiva.



Ilustración 3. Configuración en Modo Punto de Acceso o Modo Infraestructura.
Fuente: Camargo (2011).

De acuerdo con Camargo (2011), a pesar de que en el caso de las redes inalámbricas esta celda suele tener un tamaño reducido, mediante el uso de varias fuentes de emisión, es posible combinar celdas para cubrir de forma casi total un área más extensa. La estrategia empleada para aumentar el número de celdas, y por lo tanto el área cubierta por la red, es:

> La utilización de los llamados Puntos de Acceso, que funcionan como repetidores, y por tanto son capaces de doblar el alcance de una red inalámbrica, ya que ahora la distancia máxima permitida no es entre estaciones, sino entre una estación y un punto de acceso. Los Puntos de Acceso son colocados normalmente en alto, pero solo es necesario que estén situados estratégicamente para que dispongan de la cobertura necesaria para dar servicio a los terminales que soportan. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un radio de al menos treinta metros y hasta varios cientos de metros (p. 68).

6.2. Normalización IEEE para WLAN.

Explica Escudero (2007) que el Instituto de Ingenieros Eléctricos y Electrónicos, IEEE por sus siglas en inglés, es una organización internacional sin fines de lucro, líder en el campo de la promoción de estándares internacionales, particularmente en el campo de las telecomunicaciones, la tecnología de información y la generación de energía. El IEEE tiene en su haber 900 estándares activos y otros 400 en desarrollo, siendo algunos de los productos del IEEE más conocidos el grupo de estándares para redes LAN/MAN IEEE 802 que incluye el de Ethernet (IEEE 802.3) y el de redes inalámbricas (IEEE 802.11).

Establece el autor mencionado que la norma 802 desarrollada por el IEEE, versa sobre la arquitectura de redes de datos LAN (Local Área Network), y establece un estándar de tecnología en el mercado mundial, garantizando que los productos compatibles con la norma 802 sean también compatibles entre sí. La norma posee apartados que describen y especifican las distintas funciones que se implementan en una comunicación de datos de red (Tabla 1). Actualmente son cuatro los estándares reconocidos dentro de esta familia: la especificación *802.11 original*; *802.11a* (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; *802.11b*, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y *802.11g*, compatible con él, pero que proporciona aún mayores velocidades.

Tabla 1. Norma IEEE 802.

Apartado	Descripción
802.1	Describe las funciones de Bridging.
802.2	Controla el enlace lógico.
802.4	Método de control de tráfico Token-Passing.
802.5	Método de control de tráfico Token-Ring.
802.10	Seguridad en comunicaciones de datos, etc.
802.11	Describe y especifica una interface inalámbrica para comunicaciones de

Fuente: Escudero (2007).

De acuerdo con Huidobro (2000), al día de hoy son cuatro los estándares registrados:

> La descripción *802.11 original*; *802.11a* (evolución a 802.11 e/h), que define una conexión de alta velocidad basada en ATM; *802.11b*, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y *802.11g*, compatible con él, pero que suministra aún mayores velocidades. (p. 112).

Se desprende de lo descrito la importancia de las normas establecidas y la estandarización en el campo de las telecomunicaciones, destacando así la presencia de normativas específicas que deben ser acatadas y son reconocidas a nivel mundial.

6.2.1. IEEE 802.11.

Explica Camargo (2011) que en Junio de 1997, el Institute of Electrical and Electronic Engineers (IEEE), finalizó el estándar inicial para redes inalámbricas, IEEE 802.11, el cual especifica una frecuencia de operación de "2.4 GHz con velocidades de transmisión de 1 y 2 Mbps. Desde esta versión inicial, el IEEE 802.11 WG (Working Group) ha llevado a cabo diferentes revisiones a través de diferentes grupos de trabajo especializados en distintas áreas" (p. 67). Concuerda Diaz (2007)

quien indica que la tecnología especifica que contiene el modelo 802.11 es el denominado espectro de dispersión de secuencia directa (DSSS), el cual se aplica a los dispositivos inalámbricos que "operan dentro de un intervalo de 1 a 2 Mbps. Siendo un sistema de DSSS puede transmitir hasta 11 Mbps, pero si opera por encima de los 2 Mbps se considera que no cumple con la norma" (p. 1).

Por su parte, Lombas (2013), establece que "el segundo estándar aprobado fue el *802.11b* también denominado de Wi-Fi™ o inalámbrico de alta velocidad y se refiere a los sistemas DSSS que operan a 1, 2; 5,5 y 11 Mbps" (p. 4). Indica el autor que:

> Todos los sistemas 802.11b cumplen con la norma de forma retrospectiva, ya que también son compatibles con 802.11 para velocidades de transmisión de datos de 1 y 2 Mbps sólo para DSSS. Esta compatibilidad retrospectiva es de suma importancia ya que permite la actualización de la red inalámbrica sin reemplazar las NIC o los puntos de acceso (p. 5).

Establece por su parte Avendaño (2013) que los dispositivos de 802.11b logran una mayor tasa de transferencia de datos ya que utilizan una codificación diferente a la del 802.11, lo cual permite transferir una mayor cantidad de datos en el mismo periodo de tiempo. En la actualidad, la mayoría de los dispositivos 802.11b no logran la tasa de transferencia de 11 Mbps y, trabajando en un rango de 2 a 4 Mbps. Es conveniente acotar que la banda de frecuencia 2.4 Ghz, manejada por la 802.11b, es de uso libre, siendo comercializada masivamente en la actualidad en gran cantidad de productos y aplicaciones.

Indica por su parte Silva (2011) que el estándar *802.11a* (Wi-Fi 5), abarca

los dispositivos WLAN que operan en la banda de transmisión de 5 GHZ, el cual no permite la interoperabilidad de los dispositivos 802.11b ya que éstos operan dentro de los 2,4 GHZ. El estándar 802.11a provee una tasa de transferencia de datos de 54 Mbps, alcanzando con una tecnología conocida como "duplicación de la velocidad" los 108 Mbps. Lo anterior es indicativo de la evolución alcanzada, lo que permite suponer que en un futuro cercano pueda igualmente ofrecer soluciones al mercado de datos inalámbricos. Finalmente, Silva (2011) establece que el estándar *802.11g* ofrece una tasa de transferencia similar a la alcanzada por el estándar 802.11a pero compatible con los dispositivos 802.11b utilizando tecnología de modulación por multiplexión por división de frecuencia ortogonal (OFDM).

6.3. Hardware de Red Inalámbrica

Indica Claver (2015) que el Hardware de red es aquel que normalmente se refiere a los equipos que facilitan el uso de una red informática. Típicamente, esto incluye routers, switches, hubs, gateways, puntos de acceso, tarjetas de interfaz de red, cables de redes, puentes de red, módems, adaptadores RDSI, firewalls y otros dispositivos hardware relacionados. Tomando como base lo establecido por el autor, a continuación, se describen brevemente los componentes del hardware de una red inalámbrica incluyendo punto de acceso, bridges, Switch, y Router.

El *punto de acceso* opera en las capas 1 y 2 del modelo de referencia OSI. Aquí es también donde operan el bridge inalámbrico y el bridge de grupos de trabajo. Es un dispositivo WLAN que puede actuar como punto central de una red inalámbrica

autónoma. Puede utilizarse también como punto de conexión entre redes inalámbricas y cableadas. La funcionalidad de roaming proporcionada por múltiples APs permite a los usuarios inalámbricos desplazarse libremente a través de la instalación, a la vez que se mantiene un acceso sin fisuras e ininterrumpido a la red. Normalmente un WAP (Wireless Access Point) también puede conectarse a una red de cables, y puede transmitiendo datos entre los dispositivos inalámbricos y aquellos conectados a la red cableada.

Muchos WAPs pueden ser conectados unos con otros formando una red de mayores dimensiones, lo cual permite realizar un "roaming". Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos. Este o su antena son normalmente colocados en alto, pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada. Los puntos de acceso inalámbricos tienen un radio de cobertura aproximado de 100m, aunque esto varía bastante en la práctica entre un modelo y otro; y según las condiciones ambientales y físicas del lugar. Los puntos de acceso se agrupan en dos categorías.

Los *bridges* (Ilustración 4) están diseñados para conectar dos o más redes ubicadas en general en diferentes edificios. Proporciona elevadas velocidades de datos y un throughput superior para aplicaciones intensivas en cuanto a los datos, de línea de visión. Los bridges conectan sitios difíciles de cablear, pisos no continuos, oficinas satelitales, instalaciones de campus de escuelas o corporaciones, redes temporales y depósitos. Pueden configurarse para aplicaciones punto a punto o punto multipunto y

trabaja a través de una tabla de direcciones MAC definidas en cada segmento a que está conectado. Así, cuando define que un nodo un segmento involucrado está transmitiendo datos a un nodo del otro segnmento, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.



Ilustración 4. Bridge.

Fuente: Intel (2013).

Un Switch (Ilustración 5) puede ser definido como un puente multipuerto, ya que a diferencia de los puentes típicos (dos puertos que enlazan dos segmentos de red), el Switch puede tener varios puertos, dependiendo de la cantidad de segmentos de red que a conectar. De forma similar a los puentes, los Switchs asimilan información específica sobre los paquetes de datos recibidos de los distintos computadores de la red, utilizando esa información para crear tablas de envío que definen el destino de los datos enviados de un computador a otro.



***Ilustración* 5.** Switch.
Fuente*:* Zyxel (2017).

Puede afirmarse que pese a tener aspectos comunes, un Switch es más sofisticado que un puente. Este último es capaz definir si envía o no una trama al otro segmento de red, basándose en la dirección MAC destino, mientras que el Switch pose gran cantidad de puertos conectados a muchos segmentos de red, siendo capaz de seleccionar el dispositivo de destino a conectarse. Los anterior ha permitido la difusión de esta tecnología ya que optimizan el rendimiento, velocidad y ancho de banda de la red.

Los *routers* (Ilustración 6) provee conectividad a la WAN y a su vez permite enrutar paquetes de datos desde su origen hasta su destino en la LAN, en cuyo ambiente el router contiene broadcast, brinda servicios locales de resolución de direcciones (ARP), y segmenta la red manejando una estructura de subred, para lo cual debe conectarse tanto a la LAN como a la WAN.

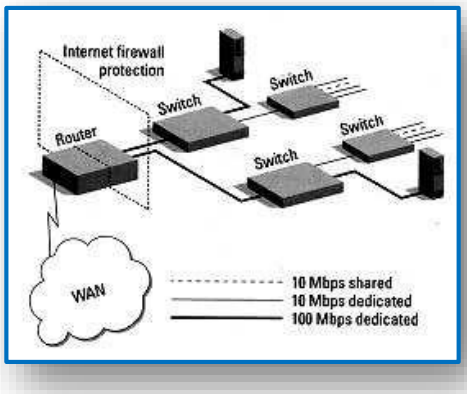


Ilustración 5. Routers. Diagrama de Funcionamiento.
Fuente*:* Sepúlveda (2011).

De acuerdo con Claros (2010), trabaja en la capa 3 del modelo OSI presentando mayor cantidad de facilidades de software que un Switch ya que funciona en una capa mayor. Igualmente, el enrutador distingue entre los diferentes protocolos de red (IP o DEC entre otros), lo que le permite decidir de forma inteligente al momento de reenviar los paquetes, siendo el responsable de establecer y conservar bien sea de forma

estática o dinámica, tablas de ruteo para cada capa de protocolo de red. Así, el enrutador elije la dirección destino y decide el envío según el protocolo establecido en la tabla mencionada.

La inteligencia de un enrutador permite seleccionar la mejor ruta, basándose sobre diversos factores, más que por la dirección MAC destino. Estos factores pueden incluir la cuenta de saltos, velocidad de la línea, costo de transmisión, retraso y condiciones de tráfico. La desventaja es que el proceso adicional de procesado de frames por un enrutador puede incrementar el tiempo de espera o reducir el desempeño del enrutador cuando se compara con una simple arquitectura de Switch.

6.4. Seguridad de red de área local inalámbrica (WLAN). Redes Abiertas

6.4.1. Ataque Denegación de Servicio (DoS)

El objetivo de este ataque implementado en una red inalámbrica consiste en impedir una comunicación entre el terminal y un punto de acceso. Para lograr esto sólo hemos de hacernos pasar por el punto de acceso poniéndonos su dirección MAC (obtenida mediante un simple Sniffer) y negarle la comunicación al terminal o terminales elegidos mediante el envío continuado de notificaciones de desasociación (Panda software International, 2005).

6.4.2. Descubrir ESSID ocultos.

En casi todos los puntos de acceso podemos encontrar la opción de deshabilitar el envío del ESSID en los paquetes o desactivar BEASON FRAMES. Ante esta medida de seguridad, un presunto atacante tendría dos opciones: a) Esnifar la red durante un tiempo indeterminado a la espera de una nueva conexión a la red con el objetivo de conseguir el ESSID presente en las tramas PROVE REQUEST del

cliente (en ausencia de BEASON FRAMES) o en las tramas PROVE RESPONSE. b) Provocar la desconexión de un cliente mediante el mismo método que empleamos en el ataque DoS pero sin mantener al cliente desconectado (Panda software International, 2005).

6.4.3. Ataque Man in the middle

Mediante este ataque se hace creer al cliente victima que el atacante es el punto de acceso y, al mismo tiempo convencer al punto de acceso que el atacante es el cliente. Para llevar a cabo un ataque de este tipo es necesario conseguir mediante el uso de un Sniffers datos como el ESSID de la red, la dirección MAC del punto de acceso, la dirección MAC de la víctima (Panda software International, 2005).

Una vez obtenidas estos datos emplearíamos la misma metodología que en el ataque de tipo DoS para romper la conexión entre el cliente y el punto de acceso. Tras esta ruptura la tarjeta del cliente comenzará a buscar un nuevo punto de acceso en los diferentes canales, momento que aprovechará el atacante para suplantar al punto de acceso empleando su MAC y ESSID en un canal distinto. Para ello el atacante habrá de poner su propia tarjeta en modo máster. De forma paralela el atacante ha de suplantar la identidad el cliente con el punto de acceso real empleando para ello la dirección MAC del cliente, de esta forma el atacante logra colocarse entre ambos dispositivos de forma transparente (Panda software International, 2005).

6.4.5. WEP – Privacidad Equivalente al Cable.

Se fundamenta en el algoritmo de seguridad empleado para brindar protección a las redes inalámbricas incluido en la primera versión del estándar IEEE

802.11 y mantenido sin cambios en 802.11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes. Este sistema emplea el algoritmo RC4, proporcionado por RSA Security, para el cifrado de las llaves que pueden ser de 64 o 128 bits teóricos, puesto que en realidad son 40 o 104 y el resto (24 bits) se emplean para el vector de inicialización (Panda Software International, 2005).

La seguridad ofrecida por WEP tiene como pilar central una clave secreta compartida por todos los comunicadores y que se emplea para cifrar los datos enviados. Pese a no estar así establecido, en la actualidad todas las estaciones y punto de acceso comparten una misma clave, lo que reduce el nivel de seguridad que puede ofrecer este sistema (Panda software International, 2005).

6.4.6. WPA

En el estándar 802.11se definen unos mecanismos de seguridad que se han demostrado insuficientes e ineficientes: la confidencialidad se basa en el sistema denominado WEP (Wired Equivalent Privacy) que consiste en un sistema de cifrado simétrico RC4, utilizando una clave estática que comparten estaciones clientes y el punto de acceso. WEP usa vectores de inicialización para generar claves diferentes para cada trama. No obstante, WEP es un sistema muy débil ya que se puede conseguir la clave de cifrado monitorizando las tramas y procesándolas (Panda Software International, 2005).

Igualmente, la integridad se consigue utilizando técnicas de detección de errores (CRC) que no son eficientes para garantizar la integridad y la autenticación es inexistente ya que incluso permite hallar la clave usada por WEP de forma muy

sencilla. Algunos fabricantes proporcionan autenticación del equipo a partir de la dirección MAC de la estación, pero es un método muy poco flexible. Wi-Fi Alliance, como organización responsable de garantizar la interoperabilidad entre productos para redes inalámbricas de fabricantes diversos, ha definido una especificación de mercado basado en las directrices marcadas por el grupo de trabajo 802.11i denominada Wi-Fi Protected Access (WPA), junto con la correspondiente certificación de productos (Panda software International, 2005).

6.4.7. WPA2

Es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las vulnerabilidades detectadas en WPA, así mismo está basada en el nuevo estándar 802.11i. WPA, por ser una versión previa, que se podría considerar de "migración", no incluye todas las características del IEEE 802.11i, mientras que WPA2 se puede inferir que es la versión certificada del estándar 802.11i. El estándar 802.11i fue ratificado en junio de 2004. La alianza Wi-Fi llama a la versión de clave pre-compartida WPA-Personal y WPA2-Personal y a la versión con autenticación 802.1x/EAP como WPA- Enterprise y WPA2-Enterprise (Panda Software International, 2005).

Los fabricantes comenzaron a producir la nueva generación de puntos de accesos apoyados en el protocolo WPA2 que utiliza el algoritmo de cifrado AES (Advanced Encryption Standard). Con este algoritmo será posible cumplir con los requerimientos de seguridad del gobierno de USA - FIPS140-2. "WPA2 está idealmente pensado para empresas tanto del sector privado cómo del público. Los productos que son certificados para WPA2 le dan a los gerentes de TI la seguridad

que la tecnología cumple con estándares de interoperatividad" declaró Frank HazlikManaging Director de la WiFi Alliance. Si bien parte de las organizaciones estaban aguardando esta nueva generación de productos basados en AES es importante resaltar que los productos certificados para WPA siguen siendo seguros de acuerdo a lo establecido en el estándar 802.11i (Panda Software International 2005).

WPA2 (Wi-Fi Protected Access 2), es compatible con su antecesor WPA, proporciona a los administradores de red un alto nivel de fiabilidad que sólo los usuarios autorizados pueden acceder. Está basado en el estándar IEEE 802.11i ratificado, WPA2, proporciona seguridad a escala mediante la aplicación del Instituto Nacional de Estándares y Tecnología (NIST) FIPS 140-2 algoritmo de encriptación AES. WPA2 se puede activar en dos versiones: WPA2- Personal y WPA2- Enterprise. La primera protege el acceso no autorizado de la red mediante la utilización de una contraseña, y la segunda verifica los usuarios de la red a través de un servidor respectivamente (Panda Software International, 2005).

6.4.8. Privacidad e Integridad con TKIP

Temporal Key Integrity Protocol (TKIP) es el protocolo elegido con el objetivo de sustituir a WEP y solucionar los problemas de seguridad que éste plantea. Como características mejoradas destacar la ampliación (Panda Software International, 2005).

6.4.9. Autenticación mediante 802.1X/EAP

El cometido principal del estándar 802.11x es encapsular los protocolos de autenticación sobre los protocolos de la capa de enlace de datos y permite emplear

el protocolo de autenticación extensible (EAP) para autentificar al usuario de varias maneras. IEEE 802.1x define 3 entidades: El solicitante (suplicant),reside en la estación inalámbrica, el autenticador (authenticator), reside en el AP, el servidor de autenticación, reside en un servidor AAA (Authentication, Authorization, Accounting) como RADIUS.

A su vez, EAP comprende 4 tipos de mensajes: a) Petición: empleado para enviar mensajes desde el AP al cliente. b) Respuesta: empleado para enviar mensajes desde el cliente al AP. c) Éxito: emitido por el AP, significa que el acceso está permitido. d) Fallo: enviado por el AP cuando para indicarle al Suplicante que se deniega la conexión. Ahora bien, el proceso de Autenticación, tras la asociación descrito brevemente incluye: envio del el AP-Request/Identity desde el Autenticador al Suplicante. El suplicante responde con EAP-Response/Identity al Autenticador, el cual lo pasa al Servidor de Autenticación. Se tuneliza el Challenge/Response y si resulta acertado el Autenticador permite al Suplicante acceso a la red condicionando por las directrices del Servidor de Autenticación (Panda Software International, 2005).

El funcionamiento base del estándar 802.11x se centra en la denegación de cualquier tráfico que no sea hacia el servidor de autenticación hasta que el cliente no se haya autenticado correctamente. Para ellos el autenticador crea un puerto por cliente que define dos caminos, uno autorizado y otro no; manteniendo el primero cerrado hasta que el servidor de autenticación le comunique que el cliente tiene acceso al camino autorizado (Panda Software International, 2005).

El solicitante, cuando pasa a estar activo en el medio, selecciona y se asocia a un AP. El autenticador (situado en el AP) detecta la asociación del cliente y habilita un puerto para ese solicitante, permitiendo únicamente el tráfico 802.1x, el resto de tráfico se bloquea. El cliente envía un mensaje "EAP Stara". El autenticador responde con un mensaje "EAP Request Indetity" para obtener la identidad del cliente, la respuesta del solicitante "EAP Response" contiene su identificador y es retransmitido por el autenticador hacia el servidor de autenticación. A partir de ese momento el solicitante y el servidor de autenticación se comunicarán directamente, utilizando un cierto algoritmo de autenticación que pueden negociar. Si el servidor de autenticación acepta la autentificación, el autenticador pasa el puerto del cliente a un estado autorizado y el tráfico será permitido (Panda Software International, 2005).

6.4.10. Extensible Authentication Protocol - EAP. TLS.

Establece Carlson (2004), que el Extensible Authentication Protocol (EAP) es un framework de autenticación usado habitualmente en redes WLAN Point-to-Point Protocol. Aunque el protocolo EAP no está limitado a LAN inalámbricas y puede ser usado para autenticación en redes cableadas, es más frecuente su uso en las primeras.

Requiere de la posesión de certificados digitales por parte del cliente y el servidor de autenticación; el proceso de autenticación comienza con el envío de su identificación (nombre de usuario) por parte del solicitante hacia el servidor de autenticación, tras esto el servidor envía su certificado al solicitante que, tras validarlo, responde con el suyo propio. Si el certificado del solicitante es válido, el servidor responde con el nombre de usuario antes enviado y se comienza la

generación de la clave de cifrado, la cual es enviada al AP por el servidor de autenticación para que pueda comenzar la comunicación segura (Panda Software International 2005).

Indica igualmente el autor mencionado que, dentro de las vulnerabilidades existentes, puede afirmarse que en la fase de identificación el cliente manda el mensaje EAP – Identity sin cifrar, permitiendo a un atacante ver la identidad del cliente que está tratando de conectarse. Se infiere entonces que el mayor inconveniente que tiene el uso de EAP – TLS es que tanto el servidor de autenticación como los clientes han de poseer su propio certificado digital, y la distribución entre un gran número de ellos puede ser difícil y costosa.

Para corregir este defecto se crearon PEAP (Protected EAP) Y EAP - Tunneled TLS que únicamente requieren certificado en el servidor. La idea base de estos sistemas es que, empleando el certificado del servidor previamente validado, el cliente pueda enviar sus datos de autenticación cifrados a través de un túnel seguro. A partir de ese momento, y tras validar el servidor al solicitante, ambos pueden generar una clave de sesión (Panda Software International 2005).

6.4.11. Ataque WPA – PSK

El único ataque conocido contra WPA – PSK es del tipo fuerza bruta o diccionario; pese a la existencia de ese ataque la realidad es que el rendimiento del ataque es tan bajo y la longitud de la passphrase puede ser tan larga, que implementarlo de forma efectiva es prácticamente imposible. Los requisitos para llevar a cabo el ataque son: un archivo con la captura del establecimiento de conexión

entre el cliente y el AP, el nombre de ESSID y un archivo de diccionario. Se puede auditar la fortaleza de las contraseñas empleadas en un sistema realizando ataques de diccionario o de fuerza bruta, en este último caso empleando herramientas al uso para crear todas las combinaciones de caracteres posibles (Panda Software International, 2005).

6.4.12. Portales cautivos

Ibáñez (2011) define los portales cautivos como "un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal" (p. 1). El programa obstaculiza el tráfico HTTP hasta que el usuario se verifica. En este punto, el portal ejecuta acciones para hacer que la sesión expire transcurrido un periodo de tiempo establecido o controlar el ancho de banda usado por cada cliente. Este sistema fue creado para permitir la validación de usuarios en nodos Wireless, lo que actualmente se utiliza para generar conexión a usuarios en locales públicos como hoteles y aeropuertos, entre otros.

En un sistema con portal cautivo se definen dos partes diferenciadas: la zona pública y la privada. La zona pública se compone, normalmente, de nodos Wireless que posibilitan la conexión de cualquier Terminal; en cambio el acceso la zona privada, normalmente Internet, se encuentra regulado por un sistema de autenticación que impide la navegación hasta que el usuario se valida. El sistema de portales cautivos se compone en líneas generales, de una serie de APs conectados a un GATEWAY colocado antes de la zona privada, un servidor web donde colocar el portal y una base de datos donde almacenar los usuarios y el servicio de

autenticación.

En el momento de qué un usuario no autenticado decide conectarse a la zona privada el Gateway comprueba si dicho usuario está autenticado; para ello se basa en la posesión de tokens temporales gestionados por http. Si dicho usuario no posee un token válido, el Gateway re direcciona la conexión hacia el portal donde al usuario se le solicitará un usuario y contraseña válidos para asignarle un token, Una vez obtenido un token el Gateway permitirá la conexión hacia la zona privada.

Este sistema presenta vulnerabilidades asociadas con las características de la zona abierta de los sistemas que implantan este sistema de portales, se permite la asociación con el AP a cualquier cliente y el tráfico entre los clientes y el AP no va; por este motivo se puede capturar el tráfico de las conexiones con la zona privada. Por otra parte, es posible implementar ataques de tipo spoofing o hijacking mientras el token que emplea el usuario legítimo sea válido.

6.4.13. Rogue Access Point (AP)

Un Rogue AP (también conocidos como Fake AP) es un punto de acceso que tiene por objetivo que los usuarios se conecten a él para, una vez dentro, capturar su tráfico y con ello, sus credenciales. Se define como un Punto de acceso no autorizado. Este tipo de ataques consiste, a nivel básico en colocar un punto de acceso bajo nuestro control cerca de las instalaciones de la víctima de forma que los clientes asociados o por asociar a esa red se conecten a nuestro AP en lugar de uno legítimo de la víctima debido a la mayor señal que recibe del nuestro.

Una vez conseguida la asociación al Rogue AP, el atacante puede provocar ataques de tipo DoS, robar datos de los clientes como usuarios y contraseñas de diversos sitios Web o monitorizar las acciones del cliente. Este tipo de ataques se ha empleado tradicionalmente para crear puertas traseras corporativas y para espionaje industrial. El ROGUE AP puede consistir en un AP modificado o un portátil con el software adecuado instalado y configurado. Este software ha de consistir en: Servidor http, servidor DNS, servidor DHCP y un portal cautivo con sus correspondientes reglas para redirigir el tráfico al portal. Todo este proceso de instalación y configuración se puede simplificar bastante mediante Airsnarf, herramienta que automatiza el proceso de configuración y arranque de un Rogue AP.

Sin embargo, hace falta algo más para poder montar un Rogue AP, se requiere que la tarjeta Wireless sea compatible con HostAP, un driver específico que permite colocar la tarjeta en modo máster, necesario para que nuestro terminal pueda comportase como si fuese un AP. Si queremos montar un Rogue AP sobre un Windows deberemos encontrar una tarjeta compatible con SoftAP para poder cambiar el modo a máster, y emplear Airsnarf para configurar los distintos servicios.

El proceso de configuración que lleva a cabo Airsnarf consiste en colocar el portal cautivo y arrancar el servidor http, configurar el servidor DHCP para que proporciones IP, Gateway y DNS al cliente; evidentemente el Gateway y el servidor DNS será el terminal del atacante convertido en Rogue AP. Por último, se configura el servidor DNS para que resuelva todas las peticiones con la IP del atacante, de forma que se puedan redireccionar todas hacia el portal cautivo del Rogue AP.

Una vez el usuario introduce su usuario y contraseña en el portal cautivo, el atacante ya las tiene en su poder. Lo normal es cambiar la apariencia del portal cautivo para que sea igual a la del portal del sistema al que se está suplantando. Otra opción es dejar navegar al usuario normalmente, pero redirigir determinadas páginas a otras copias locales con el fin de obtener usuarios y contraseñas. Para ello se puede modificar el servidor DNS para resolver aquellas páginas que nos convengan a nuestra dirección local donde tendremos preparada una copia falsa de la página (Panda Software International, 2005).

Por otra parte, con el nombre de *Rogue RADIUS* se conocen aquellos montajes que, aparte del Rogue AP clásico, incorporan un servidor RADIUS en el terminal del atacante. Para este fin se emplea comúnmente un servidor Free RADIUS adecuadamente configurado para responder a las peticiones de los usuarios legítimos. Este tipo de montaje se emplea contra sistemas que cuentan con servidores de autenticación y redes securizadas mediante EAP de forma que el atacante pueda suplantar todos los dispositivos y servidores presentes en el sistema legítimo de forma convincente, autenticador y servidor de autenticación (Panda Software International, 2005).

En este escenario, EAP - TLS pretende mejorar la seguridad de EAP mediante la implantación de certificados digitales instalados en todos los clientes y servidores. De esta manera se añade la necesidad de poseer un certificado válido para completar la autenticación. Tras el intercambio de certificados entre el suplicante y el servidor de autenticación, estos negocian un secreto común que se emplea para cifrar el resto de las comunicaciones a partir de ese momento. EAP- TTLS (EAP-

Tunneled - TLS) añade a las características de seguridad de EAP- TLS el establecimiento de un canal de comunicación seguro para el intercambio de las credenciales de usuario. De esta forma se incrementa la seguridad frente a ataques de sniffing que pretendan hacerse con estos datos. Por otra parte, elimina la necesidad de contar con certificados en todos los clientes, que conlleva un proceso de distribución y mantenimiento engorroso y caro.

De esta forma, el proceso de autenticación pasa por una primera fase de asociación del suplicante con el autenticador y una segunda en la que el servidor de autenticación envía su certificado al suplicante que, una vez validado, emplea para crear un túnel de comunicación seguro por donde enviar las credenciales y finalizar la autenticación. Tras montar un Rogue AP con un Rogue RADIUS el atacante puede desasociar a un cliente y cuando este cliente se intenta conectar, se asociará al Rogue AP por ofrecer esta mayor intensidad de señal. Una vez asociado se repetirá el proceso de autenticación mediante EAP – TLS/ TTLS- PEAP pero contra el Rogue RADIUS bajo nuestro control. De esta forma se podría desasociar usuarios, recolectar usuarios y contraseñas, recolectar las credenciales de los usuarios y suplantar a otros usuarios en la red legítima.

Ahora bien, en la tarea de defender los sistemas frente a un ataque Rogue APs, deben tomarse en cuenta tanto el cliente, como la infraestructura. En el caso del *cliente*, el peligro al que se enfrenta el usuario de un terminal móvil es la asociación a un Rogue AP de forma voluntaria o no. Es de sobra conocida la habilidad de Windows XP para manejar las conexiones inalámbricas por sí mismo, y es precisamente esta característica la más apreciada por los atacantes pues el sistema

operativo se basa sólo en la intensidad de la señal y el SSID para asociarse a un AP u a otro. Es por ello que los terminales así configurados son presa fácil de los Rogue AP.

El grupo Shmoo, creador entre otros de AIRSNARF, ha desarrollado una herramienta que monitoriza la conexión Wireless del terminal donde está instalado para detectar ataques mediante Rogue APs. Para ello vigila autenticaciones/Desautenticaciones y operaciones masivas, Firma de Rogue APs conocidas y aumento repentino de la intensidad de la señal junto a un cambio de AP. Estas técnicas no son definitivas, pero aumentan sensiblemente la seguridad frente a este tipo de ataques.

6.5. Aplicación de NIST en la Gestión de Seguridades de Redes WIFI

6.5.1 NIST. Propósito

El propósito de la normativa es proporcionar recomendaciones para mejorar la configuración de seguridad y el monitoreo del IEEE 802.11, redes de área local inalámbrica (WLAN) y los dispositivos que se conectan a esas redes. Las recomendaciones del borrador SP 800-153 cubren temas como configuraciones de seguridad WLAN estandarizadas, dispositivos de cliente WLAN conectados doblemente, evaluaciones de seguridad y monitoreo continuo.

6.5.2. Aplicación de NIST en la Gestión de Seguridades de Redes WIFI

La red inalámbrica permite que los dispositivos informáticos con capacidades inalámbricas utilicen recursos informáticos sin estar físicamente conectados a una red. Los dispositivos simplemente necesitan estar dentro de una cierta distancia (conocida como el rango) de la infraestructura de red inalámbrica. Las redes de área local

inalámbrica (WLAN) y grupos de dispositivos de redes inalámbricas dentro de un área geográfica limitada, como un edificio, son capaces de intercambiar datos a través de comunicaciones por radio. Las WLAN se implementan generalmente como extensiones a las redes de área local (LAN) existentes para proporcionar una mayor movilidad de los usuarios y acceso. Las tecnologías WLAN más implementadas se basan en el estándar IEEE 802.11 y sus enmiendas. El término genérico "WLAN" se refiere a un IEEE 802.11 WLAN.

Los dos tipos fundamentales de componentes WLAN son los dispositivos cliente (como los portátiles y los teléfonos inteligentes) y puntos de acceso (APs), que conectan lógicamente dispositivos cliente con un sistema de distribución (DS), típicamente la infraestructura de la red cableada de la organización. El DS es el medio por el cual los dispositivos cliente pueden comunicarse con las redes LAN cableadas de la organización y redes externas como Internet. Las WLAN también utilizan conmutadores inalámbricos, que actúan como intermediarios entre los puntos de acceso y el DS (Ilustración 7).

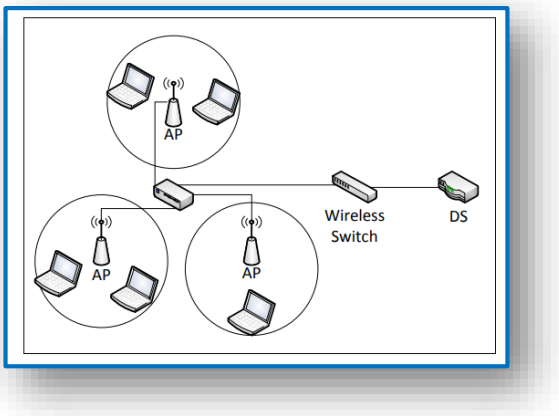


Ilustración 6. Vista simplificada de la arquitectura WLAN.
Fuente: TechNet (2017).

La seguridad de cada uno de los componentes WLAN, incluidos los dispositivos cliente, los AP y los conmutadores inalámbricos, depende en gran medida de su configuración de seguridad WLAN. La necesidad de estandarizar las configuraciones de seguridad de los componentes WLAN es importante para proporcionar recomendaciones para diseñar, implementar, evaluar y mantener esas configuraciones, particularmente para dispositivos cliente. WEP Y WPA, están diseñados para proteger el nivel de enlace de datos durante la transmisión inalámbrica entre clientes y APs. Los Estándares WLAN no pueden proporcionar seguridad de extremo a extremo porque sólo se utilizan para el enlace inalámbrico entre el AP y STA (Ilustración 8).

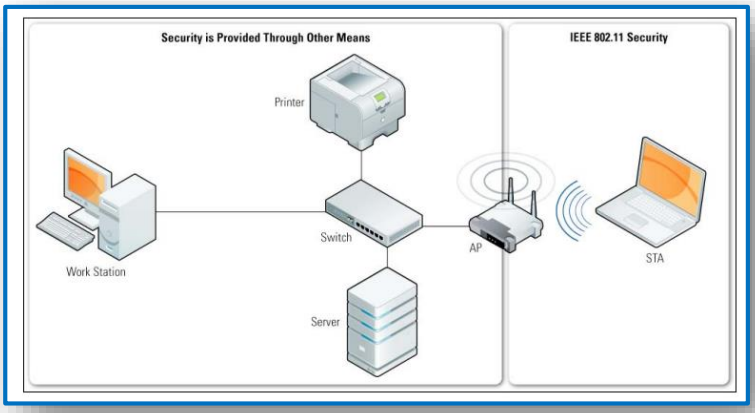


Ilustración 7. Falta de seguridad de extremo a extremo de funciones de seguridad WLAN WEP.

Fuente: Solís (2015).

Ahora se sabe que este sistema tiene una serie de vulnerabilidades de seguridad. Inicialmente fue diseñado por el IEEE para proporcionar los siguientes tres servicios básicos de seguridad: a) Autenticación: para verificar la identidad de las estaciones cliente que se comunican. Esto controla el acceso negando el paso a estaciones de cliente que no pueden autenticarse correctamente. b) Confidencialidad: utilizar el cifrado para proporcionar redes inalámbricas con la misma privacidad o

similar logrado mediante una red cableada sin cifrar. La intención era evitar el compromiso de información de escuchas ilegales. c) Integridad: para garantizar que los mensajes no fueron modificados en tránsito entre clientes inalámbricos y APs.

Las capacidades previstas de WEP para proporcionar autenticación y proteger la confidencialidad e integridad son descritas a continuación, junto con debilidades conocidas en esas capacidades. Es importante señalar que WEP no se ocupa de otros servicios de seguridad tales como auditoría, autorización, protección de repetición y gestión de claves. La falta de servicios clave de gestión es particularmente problemática, las organizaciones que implementan WLANs heredadas determinan cómo generar, distribuir, almacenar, cargar, archivar, auditar y destruir claves WEP. Muchas organizaciones optan por no cambiar claves WEP regularmente, Que proporciona a los atacantes la oportunidad de capturar suficientes datos para calcular la clave WEP y usarla para obtener acceso no autorizado a datos o realizar otros ataques.

Muchas organizaciones también eligen la misma clave para muchos dispositivos, lo que supone un riesgo significativo si un atacante obtiene acceso a uno de los dispositivos (por ejemplo, una computadora portátil que se pierde, es robada o está infectada con el malware de un atacante). Usando la misma tecla para muchos dispositivos también facilitan a un atacante realizar ataques analíticos para recuperar la clave. Además, sin las prácticas adecuadas de gestión de claves, las IEEE 802.11 WLAN heredadas pueden tener vulnerabilidades como el uso de claves no únicas, teclas predeterminadas de fábrica u otras claves débiles (por ceros, todos unos, y otros patrones fácilmente adivinados).

6.5.3. Autenticación.

En la especificación IEEE 802.11 heredada, la autenticación entre clientes y APs es sólo autenticando al cliente en el AP (Ilustración 9). El cliente debe confiar en que se está comunicando a una persona legítima. Existen dos métodos de autenticación: open-system y shared-key. El *Sistema abierto*, donde la autenticación es el único método de especificación IEEE 802.11 heredada requiere productos para apoyar. Sin embargo, la autenticación de sistema abierto no es verdadera autenticación; el AP acepta al cliente sin verificar su identidad, simplemente por el cliente que proporciona una dirección MAC al AP.

No hay ninguna validación de que esta dirección MAC no está falsificada o que el cliente está autorizado a tener acceso, por lo que la autenticación de sistema abierto es altamente vulnerable a ataques y prácticamente invita a acceso no autorizado. El otro método de autenticación en la especificación heredada, la *autenticación de clave compartida*, es un método criptográfico técnica de autenticación. Se trata de un simple esquema de "desafío-respuesta" basado en si un cliente tiene conocimiento de un secreto compartido: la clave WEP.

En este esquema, el desafío es generado por el AP y enviado al cliente en texto plano. El cliente genera una Pseudorandom serie de bytes conocido como el flujo de claves que es XORed8 con el desafío de texto claro del AP y enviado de vuelta al AP como una respuesta encriptada. El AP descifra el resultado calculado por el cliente y permite el acceso sólo si el valor descifrado es el mismo que el reto aleatorio transmitido.

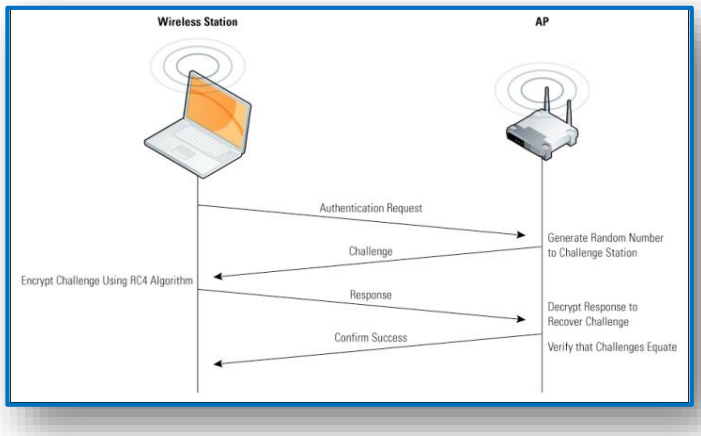


Ilustración 8. Autenticación de clave compartida.
Fuente*:* Gallinger (2011).

El algoritmo utilizado en el cálculo criptográfico y para la generación del texto de desafío de 128 bits es el RC4 cifrado de flujo, que no está aprobado por FIPS. En la autenticación de clave compartida, el intercambio inicial del desafío de texto claro desde el AP y la respuesta cifrada del cliente es una falla importante de diseño de seguridad. Un ataque de espionaje capturar tanto el desafío de texto claro del AP como la respuesta cifrada del cliente, proporcionando atacante con dos de los tres componentes necesarios para determinar el flujo de claves aleatorio.

6.5.4. Arquitectura de WLAN según estándar NIST.

Al planificar la seguridad WLAN, los diseñadores de configuración deben considerar la seguridad no WLAN, sino también cómo puede afectar a otras redes accesibles a través de ella, como redes cableadas accesibles desde la WLAN. Un principio importante de la seguridad WLAN es separar WLAN con diferentes perfiles de seguridad. Por ejemplo, debe haber WLANs separadas para (Invitado, etc.) y uso interno. Los dispositivos de la WLAN externa de una organización no deben poder

conectarse a través de esa WLAN a dispositivos en otra de las WLAN de la organización. Esto ayuda a proteger las otras redes y dispositivos de la organización de terminales y usuarios externos. Las organizaciones suelen establecer WLAN externas principalmente para proporcionar acceso a Internet a los visitantes. Tales redes inalámbricas deben ser directrices para la seguridad de las redes de área local inalámbrica.

Para las WLAN externas que necesitan acceso a la red interna, los dispositivos cliente WLAN deben tener acceso sólo a los hosts utilizando sólo los protocolos requeridos. Otro problema arquitectónico mencionado es la presencia de dispositivos de cliente conectados dobles. El término "dual conectado" se refiere generalmente a un dispositivo que está conectado tanto a una red cableada como a una WLAN al mismo tiempo. La principal preocupación con dos configuraciones conectadas es que un atacante puede ser capaz de obtener acceso inalámbrico no autorizado a dispositivo cliente y luego utilizarlo para atacar recursos en la red cableada.

Esencialmente esto permite a un atacante explotar una red de menor seguridad con el fin de obtener acceso a una red de mayor seguridad. Un posible atacante tunea el tráfico de la red de mayor seguridad a la red a través del dispositivo cliente en lugar de seguir la arquitectura de red prevista y, por tanto, evita controles de seguridad basados en red. Generalmente violan el principio de deshabilitar los servicios de red innecesarios para reducir el ataque superficie; Si el dispositivo ya está conectado a un acceso de red por cable, el acceso WLAN suele ser redundante.

Las organizaciones no sólo deben considerar la utilización simultánea de redes por cable y WLAN, sino también otras formas de conectividad dual que involucra sus dispositivos cliente WLAN. Con la creciente variedad y popularidad de tecnologías de redes inalámbricas, hoy en día es común que los dispositivos se conecten a redes simultáneamente. Por ejemplo, la mayoría de los teléfonos inteligentes pueden usar redes de telefonía celular, WLAN y Bluetooth simultáneamente, mientras que también están conectados a ordenadores portátiles / escritorios posiblemente sus redes cableadas a través de una conexión cableada (por ejemplo, USB).

Igualmente, las organizaciones deberían evaluar el riesgo de las posibles combinaciones de tecnologías de WLAN y determinar cómo se deben mitigar esos riesgos. Esto no significa que todas las formas de doble conexión deberían prohibirse automáticamente; Ejemplo de casos de uso incluye un teléfono inteligente que se conecta tanto a una WLAN como a un auricular de red Bluetooth simultáneamente, y un ordenador portátil que se conecta tanto a una WLAN como a un teclado y ratón en red Bluetooth en conjunto.

Sin embargo, la seguridad de tales casos de uso depende en gran medida de la seguridad de todas las redes. Si una o más de las redes no pueden reducir su riesgo a un nivel aceptable, las conexiones que involucren a esa red pueden suponer un riesgo excesivo para la organización. La principal cuestión relacionada con el riesgo a considerar es la probabilidad de que un atacante acceda y manipulando las comunicaciones legítimas y el impacto posible y típico de tal ataque.

Las organizaciones deben tener políticas que establezcan claramente qué formas de conexiones duales están permitidas o prohibidas para sus dispositivos cliente WLAN bajo diversas circunstancias. Las organizaciones deben hacer cumplir estas políticas a través de los controles de seguridad apropiados, incluyendo las siguientes acciones:

- Para todos sus dispositivos cliente WLAN: desactive todas las interfaces de red que no están autorizadas para uso (incluyendo planes de contingencia para la continuidad del negocio, recuperación de desastres, etc.), y configure el dispositivo para que el usuario no pueda habilitarlos o de otra manera evitar las restricciones.
- Para todos sus dispositivos cliente WLAN no autorizados para conexiones duales o Implementar los controles técnicos de seguridad apropiados.
- Las dos configuraciones conectadas están prohibidas. Los controles preventivos pueden necesitar aplicar políticas. Por ejemplo, una organización puede permitir sólo el uso de red por cable en su sede, pero podría permitir el acceso por cable o inalámbrico a redes externas. Los controles preventivos también pueden necesitar flexibilidad; Organizaciones a menudo permiten a los usuarios adjuntar los dispositivos cliente móvil de la organización a nuevas WLAN externas y, por lo tanto, los usuarios necesitan una cierta capacidad de administrar la configuración WLAN de sus dispositivos.

  Ahora bien, algunos ejemplos de controles preventivos incluyen:

a) Configurar el BIOS del dispositivo para que las conexiones WLAN se terminen automáticamente cuando se detecta una conexión por cable. La configuración del BIOS para esto se denomina conmutación LAN / WLAN.

b) Habilitar controles especializados basados en software que permitan acceso a la red WLAN o por cable, pero no ambos simultáneamente. Estos controles podrían ser incorporados en el sistema operativo (SO), proporcionado como parte del controlador WLAN o software de gestión, proporcionado por el dispositivo fabricante (por ejemplo, proveedor de portátiles), o adquiridos de terceros. Estos controles suelen favorecer a las LAN que a las WLAN debido a su relativa fiabilidad, rendimiento y seguridad.

c) Configurar herramientas de seguridad de red basadas en host (por ejemplo, firewalls basados en host, intrusión basada en host detección y prevención) para evitar que múltiples interfaces de red se utilicen en una hora.

d) Especificar y hacer cumplir perfiles de red autorizados y perfiles no autorizados a través de OS / dominio, software basado en políticas de terceros.

6.5.5. Implementación, evaluación y mantenimiento de la configuración WLAN

Después de diseñar una configuración de seguridad WLAN, una organización debe determinar cómo evaluará la efectividad de la implementación, desplegará la implementación a los dispositivos apropiados, y mantener la configuración y su implementación en todos los dispositivos. Las organizaciones deben asegurarse de que sus dispositivos cliente y APs WLAN tengan configuraciones en todo y que cumplan con las políticas WLAN de la organización. Las organizaciones deben normalizar, automatizar y centralizar tanto de su seguridad WLAN implementación y

mantenimiento de la configuración, en la práctica, especialmente para sus dispositivos cliente WLAN y puntos de acceso.

Esto permite a las organizaciones implementar una seguridad WLAN consistente para detectar y corregir cambios no autorizados en las configuraciones, y para reaccionar a las vulnerabilidades identificadas o los incidentes recientes indican la necesidad de cambiar la configuración de seguridad de la WLAN.

Existen soluciones que pueden manejar una amplia variedad de software. Tales soluciones pueden ser incorporadas en los dispositivos cliente y otros dispositivos WLAN. Además, el software de gestión de clientes WLAN a menudo tienen capacidades de gestión de configuración. Si la configuración existente no permite la implementación de soluciones y el mantenimiento, entonces la organización debería evaluar alternativas e implementar una solución de gestión de configuración que proporcione las capacidades que faltan. Igualmente, las organizaciones deben evaluar cuidadosamente todas las implementaciones de configuración de seguridad WLAN estandarizadas.

Antes de implementarlos en entornos de producción, incluso si la organización confía en que la configuración es sólida, debe evaluarse detenidamente para garantizar que sus requisitos específicos de seguridad y operacionales de la organización. Cada entorno operativo tiene características que deben tenerse en cuenta.

6.5.6. Monitoreo de ataques.

Las organizaciones deben monitorear continuamente sus WLANs, lo cual implica los mismos controles de seguridad que se utilizarían para cualquier conexión

de red en los sistemas de una organización. Los ataques específicos de WLAN pueden dividirse en dos tipos: pasivo y activo. Estas clases de ataque, que son significativos para fines de monitoreo, se describen a continuación.

Ataque pasivo: un ataque en el que una parte no autorizada sólo supervisa las comunicaciones WLAN; el atacante no genera, altera o interrumpe las comunicaciones WLAN. Hay dos tipos de ataques pasivos:

Escuchar a escondidas: el atacante supervisa las transmisiones de datos WLAN para el contenido del mensaje.

Análisis de tráfico (también conocido como análisis de flujo de tráfico). El atacante obtiene inteligencia del monitoreo de las transmisiones para patrones de comunicación. Una cantidad considerable de la información está contenida en el flujo de mensajes entre las partes que se comunican.

Ataque Activo: un ataque en el que una parte no autorizada genera, altera o interrumpe las comunicaciones WLAN. Los ataques activos pueden adoptar la forma de uno de los siguientes tipos: Enmascaramiento. El atacante se supone como un usuario autorizado que tiene acceso a ciertos privilegios no autorizados. Repetición. El atacante supervisa las transmisiones (ataque pasivo) y retransmite mensajes posando como el usuario legítimo. Modificación del mensaje. El atacante altera un mensaje legítimo eliminando, añadiendo, cambiando o reordenando el mensaje. Negación de servicio (DoS). Un DoS puede ocurrir inadvertidamente, como otros dispositivos electrónicos causando interferencia, o puede ocurrir intencionalmente, como un

atacante que envía grandes números de mensajes a una velocidad alta para inundar la WLAN. Malversación de fondos. El atacante roba o hace otro uso no autorizado de los servicios WLAN.

Una forma de ataque activo que es particularmente notable es el despliegue de dispositivos WLAN deshonestos. Por ejemplo, un atacante despliega un AP que ha sido configurado para aparecer como parte de la infraestructura de WLAN. Esto puede proporcionar una puerta trasera en la red cableada, eludiendo la seguridad perimetral mecanismos, como los firewalls. Además, si los dispositivos cliente se conectan inadvertidamente al AP atacante puede ver y manipular las comunicaciones de los dispositivos cliente (por ejemplo, ataques man-in-the-middle), así como potencialmente tener acceso a los propios dispositivos del cliente.

La supervisión de ataques específicos de WLAN se centra en ataques activos. Porque los ataques pasivos implican estrictamente interceptar las transmisiones de radio y no generar sus propias transmisiones, no hay nada en la organización a monitorear electrónicamente. Mitigar los ataques pasivos es principalmente una función de la seguridad. Sin embargo, todas las formas de ataque activo mencionadas anteriormente pueden ser detectadas a través del monitoreo.

7. RESULTADOS

El cuestionario utilizado en este estudio (Anexo 1) constó de noventa y dos (92) preguntas, divididas en seis (6) dimensiones, cinco (5) de ellas correspondientes al objetivo 2 y una correspondiente al objetivo 3. Las dimensiones del objetivo 2 incluyen: Parte Técnica (18 preguntas), Diseño Lógico de Red (14 preguntas), Configuración, Autenticación y Cifrado de Equipos Inalámbricos (22 preguntas), Administración de Recursos Humanos (24 preguntas). En el caso del Objetivo 3, se incluye la dimensión comparativa (14 preguntas).

A fin de facilitar la comprensión de los resultados obtenidos y el respectivo análisis de los mismos se procedió a agrupar las respuestas obtenidas para cada una de las dimensiones definidas. De esta forma (Tabla 2 y siguientes), se muestran las alternativas de respuesta (Si, No, N/A), el total de respuestas obtenidas para las preguntas (ítem) incluidas en cada dimensión, la frecuencia y el porcentaje. Tomando en consideración lo descrito, se exponen a continuación los resultados en esta etapa del estudio. El cuestionario se aplicó a las personas que administran la red de la institución de educación superior.

7.1. DESARROLLO LISTAS DE VERIFICACIÓN

Objetivo 2. Diagnosticar los mecanismos de seguridad de la red WIFI IESONAIR utilizados en la Institución de Educación Superior (IES) seleccionada como objeto de estudio.

Dimensión: Parte Técnica.

Tabla 2. Parte Técnica

Alternativas	Total Respuestas Ítem 1-18	
	Frecuencia	Porcentaje (%)
Si	47	87
No	2	4
N/A	5	9
Total	**54**	**100**

Fuente: El Investigador (2017).

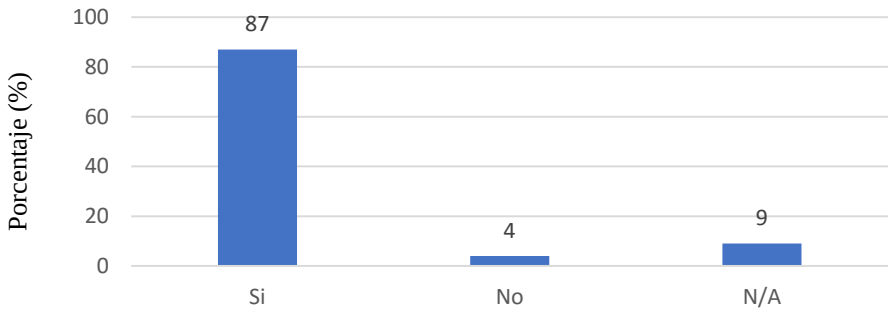


Grafico 1. Parte Técnica.
Fuente: El Investigador (2017)

Análisis: el ochenta y siete por ciento (87%) de los encuestados opina que en la IES se utilizan mecanismos de seguridad de la red WIFI IESONAIR como contraseñas LDAP, tiempo de inactividad en el uso de la plataforma y de conexión a la red, el refrescamiento de claves, asignación de ancho de banda por usuarios para controlar el tráfico, segmentación de la red por perfiles de usuarios, óptimos equipos de conexión (Servidor principal Controlador de dominio y DNS, Servidor secundario: Proxi, Firewall, Radius, Enrutamiento, Vlan, Programas monitoreo, aplicaciones de auditoria para la red, Router. Switch principal, Switch secundario, puntos de acceso, adaptador de red), segmentación de red por perfiles de usuarios y las estaciones de trabajo puertos y servicios trabajan sin problemas. Solo un cuatro por ciento (4%) opina que no y el restante nueve por ciento (9%) opina que esto no aplica. La inexistencia de puerto seguro para la conexión de equipos externos que no pertenecen

a la universidad y la eliminación eventual de usuarios en la cuenta de correo, se cuentan entre las debilidades encontradas.

Dimensión: Diseño Lógico de Red.

Tabla 3. Diseño Lógico de Red.

Alternativas	Total Respuestas Ítem 1-14	
	Frecuencia	Porcentaje (%)
Si	30	71
No	6	14
N/A	6	14
Total	**42**	**100**

Fuente: El Investigador (2017).

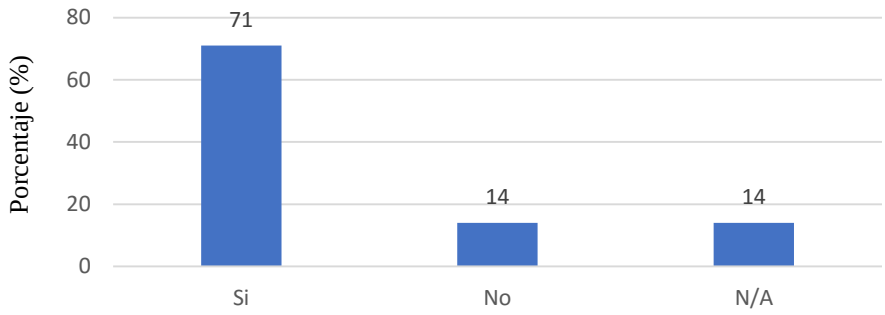


Grafico 2. Diseño Lógico de Red.

Fuente: El Investigador (2017).

Análisis: los resultados obtenidos indican que para el setenta y un por ciento (71%) de los encuestados en la IES evaluada si se toman en cuenta aspectos relacionados con el diseño lógico de red como la estandarización de los nombres de cuentas de usuario, las cuentas de usuarios personalizadas con políticas de restricciones, el monitoreo de los logs para revisar posibles intromisiones, la utilización de un modelo basado en dominios, actualización de los equipos de conexión de la WLAN según los requerimientos actuales de seguridad en las necesidades de la universidad, protocolo de red TCP/IP, registros de navegación de usuarios, ausencia de problemas por parte de los usuarios para reconocer la red inalámbrica y determinación de niveles de acceso

a los recursos compartidos. Un catorce por ciento (14%) indica que esto no ocurre y un porcentaje similar (14%), afirma que no aplica. Las pruebas periódicas de seguridad, así como las pruebas de salto por salto entre entidad origen y cada elemento intermedio, las restricciones para el uso de archivos en la WLAN, la revisión periódica de accesos asignados a las cuentas de usuario y el suministro de herramientas para implementar mecanismos de integridad como MDS, son elementos que no son tomados en cuenta de forma permanente en los protocolos de seguridad implementados.

Dimensión: Configuración, autenticación y cifrado de equipos inalámbricos.

Tabla 4. Configuración, autenticación y cifrado.

Alternativas	**Total Respuestas Ítem 1-22**	
	Frecuencia	**Porcentaje (%)**
Si	43	65
No	17	26
N/A	6	9
Total	**66**	**100**

Fuente: El Investigador (2017).

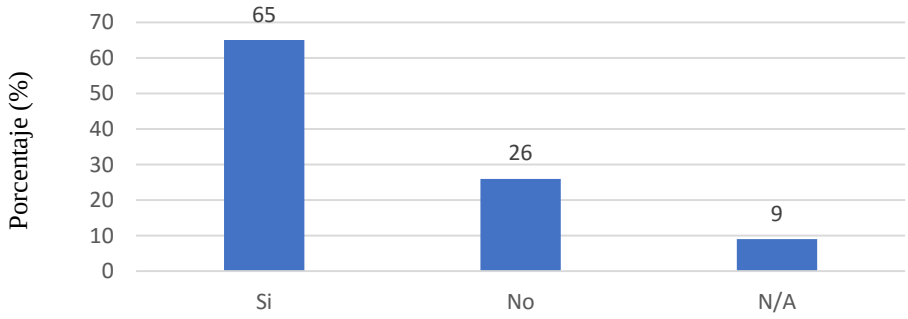


Grafico 3. Configuración, autenticación y cifrado.
Fuente: El Investigador (2017).

Análisis: el sesenta y cinco por ciento (65%) de los encuestados afirma que, si son tomados en cuenta elementos de configuración, autenticación y cifrado en los protocolos de seguridad utilizados, incluyendo la utilización del Nombre de Red o SSID por defecto del router inalámbrico, punto de acceso o puerta de enlace,

desactivación de los protocolos de gestión inseguros o innecesarios en los puntos de acceso, cambio de los parámetros por defecto en los puntos de acceso, los tamaños de clave cifrado son de por lo menos 128 bits, las claves por defecto son reemplazadas por claves únicas más seguras, el Firewall configurado funciona para los usuarios de red interna y externa, los usuarios se autentican (Radius local, Kerbeos) con nombres de usuarios y contraseña para la red WLAN, se utiliza el protocolo de autenticación 802.1x, el acceso se concede únicamente a las máquinas cliente con direcciones MAC registradas, todas las funciones de seguridad posible que se proporcionan en la arquitectura están en uso y se manejan blacklist en páginas para la navegación web. Por su parte, el veintiséis por ciento (26%) indica que esto no se realiza y un minoritario nueve por ciento (9%) responde que no aplica. Dentro de estos últimos elementos se cuentan: cambio en el servicio set identifier (SSID) por defecto del punto de acceso, la cadena de caracteres SSID es fácil de adivinar y refleja información sobre la empresa (nombre, ubicación, función), las claves se almacenan en texto plano, presencia de servidor de control de navegación tipo ISA SERVER, configuración de servidor para prevenir el uso de conexiones duales, utilización de IPSec en lugar del predeterminado WEP como el protocolo de seguridad, uso de un algoritmo de cifrado más seguro que el algoritmo RC4 por defecto (3DES o AES), obtención de autenticación del usuario a la WLAN a través de métodos más seguros (datos biométricos, tarjetas inteligentes, autenticación de dos factores, PKI, RSA), desactivación del DHCP en redes WLAN externas si no es totalmente necesario, instalación de firewall a clientes inalámbricos y en la red inalámbrica no pueden ser utilizados dispositivos como impresoras y servidor de archivo.

Dimensión: Administración de Recursos Humanos

Tabla 5. Administración de Recursos Humanos.

Alternativas	Total Respuestas Ítem 1-24	
	Frecuencia	Porcentaje (%)
Si	27	38
No	33	46
N/A	12	17
Total	**72**	**100**

Fuente: El Investigador (2017).

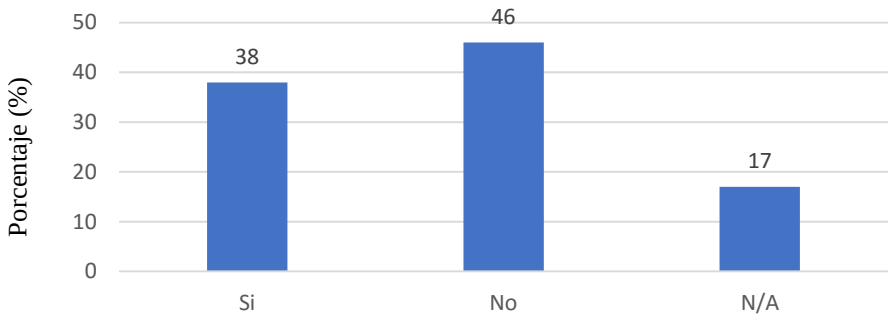


Grafico 4. Administración de Recursos Humanos.
Fuente: El Investigador (2017).

Análisis: los resultados obtenidos indican que para el cuarenta y seis por ciento (46%) y el diecisiete por ciento (17%) de los encuestados existen fallas en la administración de recursos humanos, relacionadas con ausencia de acuerdos y firma por parte de los empleados de los términos y condiciones en el contrato de trabajo, acuerdos de confidencialidad o no divulgación a aquellos que tendrán acceso a la red inalámbrica, verificación y solicitud a los empleados de aplicación de seguridad inalámbrica de acuerdo con las políticas y procedimientos de seguridad, responsabilidades del personal y de la organización en lo concerniente a la red inalámbrica interna, no existe la socialización y la capacitación regular del personal en concientización y actualización de políticas y procedimientos de seguridad inalámbricas relevantes para su función, capacitaciones al personal de modo que le permita conocer problemas e

incidentes en la red inalámbrica, seguimiento de proceso disciplinario formal para el personal que ha cometido una falta disciplinaria en la red inalámbrica, inicio del proceso disciplinario después de una previa verificación de que ha ocurrido una falta en la red inalámbrica, tratamiento correcto y justo para el personal sospechoso, retiro inmediato de sus derechos y obligaciones de personal sospechoso, acceso a los visitantes a la sala de telecomunicaciones sin aprobación escrita, claridad en la definición y asignación de las responsabilidades para llevar a cabo la finalización o cambio de empleo, devolución por parte del personal de todos los equipos inalámbricos de la organización que están a su cargo al finalizar su empleo, transferencia de la información a la institución en caso que el empleado compre o use su propio equipamiento, retiro, anulación o ajuste de los derechos de acceso a la red inalámbrica al finalizar el empleo, reducción o eliminación de los derechos de acceso a la red inalámbrica e instalaciones antes de terminar o cambiar de empleo, cambio de todas las contraseñas de cuentas que siguen activas a la finalización o cambio de empleo. Por el contrario, un minoritario treinta y ocho por ciento (38%), afirma que si son tomadas en cuenta estrategias de seguridad aplicadas al recurso humano relacionadas con definición de los roles y responsabilidades del personal sobre la red inalámbrica interna, conocimientos en los roles y responsabilidades del personal sobre la red inalámbrica, roles y responsabilidades del personal segmentados por departamentos de acuerdo a las necesidades de la organización, acceso restringido del equipo de limpieza a la sala de telecomunicaciones para evitar el sabotaje y si tienen acceso están acompañados por el personal de la misma área.

Objetivo 3. Comparar los mecanismos de seguridad de la red WIFI IESONAIR recomendados por el Instituto Nacional de Estándares y Tecnología (NIST), con el procedimiento cumplido en una Institución de Educación Superior (IES).

Dimensión: Comparativa.

Tabla 6. Comparación NIST.

Alternativas	Total Respuestas Ítem 1-14	
	Frecuencia	Porcentaje (%)
Si	36	85
No	4	10
N/A	2	5
Total	**42**	**100**

Fuente: El Investigador (2017).

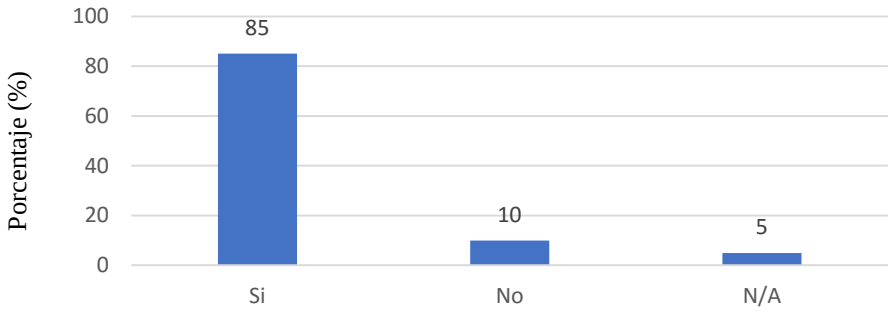


Grafico 5. Comparación NIST
Fuente: El Investigador (2017).

Análisis: el ochenta y cinco por ciento (85%) de la muestra afirma que el procedimiento cumplido en una Institución de Educación Superior (IES) si es comparable con los mecanismos de seguridad de la red WIFI IESONAIR recomendados por el Instituto Nacional de Estándares y Tecnología (NIST), cumpliéndose aspectos relacionados con presencia de un inventario de los equipos existentes para poder actualizarlos periódicamente, lista de las aplicaciones para el monitoreo de tráfico, información sobre nuevos tipos de ataque y vulnerabilidades para aplicar la seguridad a la WLAN, topología de red definida acorde a la seguridad

de la organización, estándar del cifrado en las claves criptográficas de seguridad fuerte es usado en la WLAN de la universidad, presencia de usuarios o grupos de usuarios autorizados y no autorizados a utilizar WLAN de la organización, restricción de derechos de los dispositivos o individuos a acceder a una red o recursos dentro de WLAN, monitoreo periódico de la seguridad en la WLAN, segmentación de la red por perfiles de usuarios (WLAN interna y WLAN externa) y presencia en las tecnologías WLAN de los últimos parches de seguridad y actualizaciones. Por otra parte, un diez por ciento (10%) indica que no es comparable, mientras que un minoritario cinco por ciento (5%), afirma que no aplican elementos como asegurar que la comunicación en la WLAN no pueda ser leída por personas no autorizadas, posibilidad de detectar cualquier cambio intencional o no intencional a los datos que ocurren en tráfico, asegurar que los dispositivos y las personas puedan acceder a una red y sus recursos cuando sea necesario y permitir el uso de conexiones duales en las estaciones.

Una vez analizados los resultados puede inferirse que, si bien un porcentaje significativo (85%) de los encuestados indica que los estándares recomendados por el Instituto Nacional de Estándares y Tecnología (NIST), relacionados con la seguridad de la red WIFI IESONAIR, son comparables con los existentes en la IES evaluada, existen algunas vulnerabilidades que deben ser corregidas a fin de optimizar el proceso. Por otra parte, el análisis realizado permitió igualmente definir limitantes en la administración del recurso humano que labora en la institución, particularmente en aspectos relevantes como la confidencialidad, concientización, capacitación sobre mecanismos de seguridad de la red y retiro inmediato de derechos y obligaciones de personal sospechoso, entre otros elementos, mismos que deben igualmente ser tomados en cuenta en futuras estrategias gerencial.

8. CONCLUSIONES Y RECOMENDACIONES.

8.1. CONCLUSIONES.

1. El Instituto Nacional de Estándares y Tecnología (NIST) proporciona recomendaciones orientadas a garantizar la seguridad de las redes WIRELESS, incluidas estas en el estándar IEEE 802.11, indicando en líneas generales que el protocolo de seguridad debe realizarse bajo el concepto de Red de Seguridad Robusta (RSN) y continuo monitoreo. Son lineamientos utilizados alrededor del mundo, los cuales pueden ser adoptados por las instituciones y organizaciones a fin de optimizar los protocolos de seguridad de sus redes inalámbricas. De acuerdo con la normativa, los mecanismos más utilizados para brindar seguridad a redes inalámbricas son: autenticación de usuario, claves de acceso a la red, listas de control de acceso en puntos de acceso y cifrado WEP o WPA para los paquetes de datos.

De acuerdo con la normativa, la seguridad de cada uno de los componentes WLAN, incluidos los dispositivos cliente, los AP y los conmutadores inalámbricos, depende en gran medida de su configuración, por lo cual resulta necesario la estandarización de la misma y la definición de recomendaciones para su diseño, implementación, evaluación y mantenimiento.

Por otra parte, el estándar NIST proporciona inicialmente tres servicios básicos de seguridad que son la autenticación, confidencialidad e Integridad. La autenticación permite verificar la identidad de las estaciones cliente que se comunican, lo cual controla el acceso y niega el paso a estaciones de cliente que

no pueden autenticarse correctamente. La confidencialidad a través del cifrado proporciona redes inalámbricas con la misma o similar privacidad, mediante una red cableada sin cifrar, evitando así el compromiso de información por escuchas ilegales. La integridad garantiza que los mensajes entre clientes inalámbricos y APs, no sean modificados en tránsito.

La normativa estudiada, adicionalmente proporciona lineamientos de seguridad relacionados con la arquitectura de WLAN, siendo un principio de seguridad considerado separar WLAN con diferentes perfiles de seguridad, como por ejemplo redes de uso interno y externo, elementos estos que no deben estar conectados. Igualmente considera las conexiones duales, los riesgos de seguridad inherentes y las estrategias de protección que deben ser implementadas.

Con respecto a las recomendaciones para el diseño, implementación, evaluación y mantenimiento de la red WLAN la norma NIST establece que las organizaciones deben en la práctica normalizar, automatizar y centralizar las estrategias de seguridad, así como la implementación y mantenimiento de la configuración, especialmente para sus dispositivos cliente WLAN y puntos de acceso, lo cual permite detectar y corregir cambios no autorizados en las configuraciones, y reaccionar a las vulnerabilidades identificadas o los incidentes recientes que indicarían la necesidad de cambiar la configuración de seguridad de la WLAN. Lo anterior puede realizarse mediante la utilización de gran variedad de software, convenientemente incorporados en los dispositivos cliente y otros dispositivos WLAN. Si esto no es posible, la organización debe necesariamente desarrollar estrategias que permitan la adecuada gestión de la configuración.

Igualmente debe monitorear continuamente los ataques activos o pasivos que pudieran presentarse.

2. Los mecanismos de seguridad de la red WIFI IESONAIR utilizados en la Institución de Educación Superior (IES) seleccionada como objeto de estudio, presentan vulnerabilidades evidentes relacionadas con la ausencia de encriptación en las contraseñas de acceso a la red utilizadas, no utilización de las contraseñas LDAP, e inexistencia de un tiempo de inactividad en el uso de la plataforma y de conexión a la red, refrescamiento de claves en la administración de usuarios de la red, eliminación de usuarios en la cuenta de correo ni puerto seguro para la conexión de equipos externos que no pertenecen a la universidad, entre otras limitantes.

Además, se evidencian fallas en el diseño lógico de red relacionadas con pruebas periódicas de seguridad, así como las pruebas de salto por salto entre entidad origen y cada elemento intermedio, las restricciones para el uso de archivos en la WLAN, la revisión periódica de accesos asignados a las cuentas de usuario y el suministro de herramientas para implementar mecanismos de integridad como MDS, siendo estos elementos que no son tomados en cuenta de forma permanente en los protocolos de seguridad implementados.

Igualmente, al evaluar la configuración, autenticación y cifrado de equipos inalámbricos, se resalta que no se aplican de forma constante elementos como el cambio en el servicio set identifier (SSID) por defecto del punto de acceso, la configuración de servidor para prevenir el uso de conexiones duales, utilización de IPSec en lugar del predeterminado WEP como el protocolo de seguridad,

presencia de servidor de control de navegación tipo ISA SERVER, uso de un algoritmo de cifrado más seguro que el algoritmo RC4 por defecto (3DES o AES), obtención de autenticación del usuario a la WLAN a través de métodos más seguros (datos biométricos, tarjetas inteligentes, autenticación de dos factores, PKI, RSA), desactivación del DHCP en redes WLAN externas si no es totalmente necesario, instalación de firewall a clientes inalámbricos. Adicionalmente, la cadena de caracteres SSID es fácil de adivinar y refleja información sobre la empresa (nombre, ubicación, función), las claves se almacenan en texto plano y en la red inalámbrica no pueden ser utilizados dispositivos como impresoras y servidor de archivo. La conjunción de los elementos citados pone en riesgo la seguridad de la red inalámbrica de la institución.

Por otra parte, puede concluirse que, aunque se cumplen algunos estándares recomendados para el adecuado manejo del recurso humano como definición y conocimiento de los roles y responsabilidades y acceso restringido de personal no autorizado, existen igualmente fallas que deben ser corregidas, encontrándose dentro de estas la ausencia de acuerdos en los términos, condiciones y confidencialidad en el contrato de trabajo, verificación y aplicación de normas de seguridad inalámbrica y escasa capacitación del personal en procedimientos, problemas e incidentes relacionados con la seguridad de la red inalámbrica.

Igualmente, existen limitantes en aspectos relevantes como verificación, tratamiento correcto y justo y seguimiento de proceso disciplinario formal para el personal que ha cometido una falta disciplinaria en la red inalámbrica, condiciones para finalización o cambio de empleo, devolución de equipos y transferencia de información a la IES en caso de finalización de la relación

laboral, retiro, anulación o ajuste de los derechos de acceso a la red inalámbrica al finalizar el empleo y cambio de todas las contraseñas de cuentas que siguen activas a la finalización o cambio de empleo.

3. Puede concluirse igualmente que los mecanismos de seguridad de la red WIFI IESONAIR recomendados por el Instituto Nacional de Estándares y Tecnología (NIST), difieren en aspectos puntuales del procedimiento cumplido en la Institución de Educación Superior (IES) evaluada, relacionados con seguridad de que la comunicación en la WLAN no pueda ser leída por personas no autorizadas, detección de cambio intencional o no intencional de los datos que ocurren en tráfico, acceso seguro de dispositivos y personas a una red y sus recursos cuando sea necesario y permiso de uso de conexiones duales en las estaciones.

Sin embargo, de acuerdo con los resultados, existen aspectos que si se cumplen de acuerdo con la normativa como inventario de equipos existentes, lista de las aplicaciones para el monitoreo de tráfico, información sobre nuevos tipos de ataque y vulnerabilidades para aplicar la seguridad a la WLAN, topología de red definida, estándar del cifrado en las claves criptográficas de seguridad fuerte y restricción de acceso a la red o recursos dentro de WLAN, entre otros. Aun así, se evidencian vulnerabilidades en la red evaluada que deben ser convenientemente corregidas.

4. Finalmente, se concluye que la adecuada adopción y posterior implementación de lineamientos basados en los estándares recomendados por Instituto Nacional de Estándares y Tecnología (NIST), permitiría optimizar la seguridad de la red WIFI IESONAIR de la Institución de Educación Superior (IES) estudiada. En

este sentido, la aplicación de medidas mínimas de seguridad, tales como cambiar la contraseña, utilizar una identificación no característica para la red, utilizar contraseñas difíciles de predecir, habilitar el encriptado WEP o WPA, desactivar el servidor DHCP o deshabilitar la red si no está en uso, entre otras estrategias, podría reducir el riesgo de que la red sea atacada.

8.2. RECOMENDACIONES.

1. Se recomienda a la IES realizar evaluaciones periódicas de seguridad al menos una vez al año para valorar la seguridad general de la WLAN. Además, se recomienda realizar evaluaciones periódicas al menos trimestralmente a menos que el monitoreo continuo de la seguridad WLAN ya esté recopilando toda la información sobre ataques WLAN y vulnerabilidades necesarias para propósitos de evaluación.

2. Se recomienda al planificar la frecuencia y amplitud de las evaluaciones periódicas, considerar la ubicación de la instalación que se está escaneando, porque la proximidad física de un edificio a un área pública (por ejemplo, calles y áreas comunes públicas) o su ubicación en un área metropolitana ocupada puede aumentar el riesgo de amenazas de WLAN. Igualmente, el nivel de seguridad de los datos a transmitir en la WLAN y la frecuencia con la que los dispositivos cliente WLAN se conectan y se desconectan del entorno y los niveles de tráfico típicos de estos dispositivos (por ejemplo, actividad ocasional o actividad constante).

3. Igualmente se recomienda implementar los lineamientos de seguridad de las redes inalámbricas, según lo establecido por la NIST, ajustando los mismos a las

condiciones y características propias de cada empresa y/o institución, con la finalidad de optimizar el funcionamiento y seguridad de la red, encontrar vulnerabilidades y así lograr prevenirlas (Anexos 1 y 2).

4. Se recomienda establecer charlas por lo menos anuales donde se socialice las políticas y mecanismos de seguridad establecidos por las autoridades de la IES al personal docente, administrativo y a los estudiantes para prevenir los riesgos de posibles ataques.

5. Se recomienda revisar la cobertura de la señal de los AP para evitar que la Wireless no sobrepase los límites externos de la institución, pudiendo tener acceso a la infraestrctura por personas no autorizados sin necesidad de ingresar a la IES.

9. GLOSARIO DE TÉRMINOS

Parafraseando lo establecido por Hernández *et al.* (2010), puede afirmarse que un glosario de términos en una investigación representa la definición de un listado de conceptos ordenados alfabéticamente, relevantes para el tema tratado. Los mismos permiten al lector mejorar la comprensión de los elementos citados previamente en el texto. Tomando en consideración lo descrito previamente, y con base en lo establecido por Gamma Internet Consultoría (2003), Escudero (2007), Gallager (2011), Kodak (2015), Intel (2017b), TechNet (2017), se expone a continuación el glosario de términos significativos para este estudio.

Ancho de Banda: Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información

Bluetooth: Especificación que proporciona un método para que los dispositivos, tales como teléfonos portátiles, equipos portátiles, equipos e impresoras, se conecten y compartan información entre sí a través de una frecuencia de radio de corto alcance**.**

Base de datos: Conjunto de datos que pertenecen al mismo contexto almacenados sistemáticamente. En una base de datos, la información se organiza en campos y registros. Los datos pueden aparecer en forma de texto, números, gráficos, sonido o vídeo.

Buffered memory (Memoria en búfer): Tipo de módulo de memoria que tiene un registro entre los módulos de memoria DRAM y la controladora de memoria del sistema. La memoria en búfer también se denomina memoria registrada y es más estable la memoria sin búfer, pero también tiene un mayor costo. La memoria en búfer se utiliza principalmente en servidores y estaciones de trabajo.

Byte: Unidad de almacenamiento de memoria que equivale a 8 bits.

Clave de codificación: serie de letras y números que permite codificar datos y después decodificarlos de forma que se puedan compartir de manera segura entre los miembros de una red. Los usuarios de WEP utilizan una clave de codificación que codifica automáticamente los datos salientes. Esta misma clave le permite al ordenador receptor decodificar automáticamente la información para que se la pueda leer.

Cliente, o dispositivo cliente: Cualquier equipo conectado a una red y que solicita servicios (ficheros, impresión) de otro miembro de la red. En el caso de las WLAN, se suele emplear para referirse a los adaptadores que proporcionan conectividad a través de la red inalámbrica, como tarjetas PCMCIA, PCI o USB, que permiten al equipo acceder a la red.

CPU: (Central Processing Unit - Unidad de procesamiento central) Otro nombre que se le da al procesador.

Driver (Controlador): Software escrito para un sistema operativo en particular y que es utilizado por el sistema operativo para comunicarse con un dispositivo de hardware determinado.

EAP. El Protocolo de autenticación extensible (EAP): estándar 802.1X que permite a los programadores transferir datos de autenticación entre los servidores RADIUS y los puntos de acceso inalámbrico. EAP dispone de una serie de variantes, entre las que se incluyen las siguientes: EAP MD5, EAP-TLS, EAP-TTLS, LEAP y PEAP.

EAP-TLS: Microsoft desarrolló EAP-Seguridad de la capa de transporte (EAP-TLS) sobre la base del estándar 802.1X para utilizar certificados digitales en el proceso de autenticación. Actualmente, constituye el estándar del sector para la autenticación 802.11i.

Gateway (Puerta de enlace): tipo particular de punto de acceso que permite que los clientes de la red inalámbrica compartan una conexión a Internet (módem DSL o de cable). Las puertas de enlace inalámbricas incluyen características tales como compatibilidad con NAT y VPN, que podrían no encontrarse en puntos de acceso sencillos.

GB: (Gigabyte) Unidad de almacenamiento de memoria que equivale a 1.024 megabytes (o 1.073.741.824 bytes).

GHz: (Gigahercio) Unidad de frecuencia que equivale a 1.000.000.000 de ciclos por segundo.

Router (Enrutador): Dispositivo que enruta datos entre distintas redes.

Server (Servidor): Computadora que brinda un servicio a uno o más equipos o aplicaciones (lo que se conoce como los clientes).

SSD: (Solid State Drive - Unidad de estado sólido).

SSID - (Service Set Identification: Identificación de conjunto de servicios) También conocido como nombre de la red e identifica la red. Se trata de un nombre único y controla el acceso a una red determinada. SSID puede tener hasta 32 caracteres y hace distinción de mayúsculas y minúsculas.

TKIP: El Protocolo de integridad de clave temporal (TKIP) forma parte del estándar de cifrado WPA para redes inalámbricas. TKIP es la siguiente generación de WEP, que proporciona una combinación de claves por paquete para solucionar las imperfecciones detectadas en el estándar WEP.

USB: (Universal Serial Bus - Bus serie universal) Especificación de conectividad que permite que los dispositivos periféricos como son los escáneres, las impresoras y los sticks de memoria se enchufen en la computadora y se configuren automáticamente.

WEP: (Wired Equivalent Privacy - Privacidad equivalente a cable) Función IEEE 802.11 opcional que se utiliza para proporcionar seguridad de datos y que es equivalente a la de la red local cableada típica. Cuando se activa WEP, se requiere que todas las estaciones (clientes y puntos de acceso) tengan la misma clave WEP. Se niega el acceso a la red a cualquier persona que no cuente con la clave correcta.

Wireless Client (Cliente inalámbrico): Software que controla un adaptador inalámbrico.

WLAN: (Wireless Local Area Network - Red local inalámbrica) Dos o más equipos que están enlazados juntos sin cables.

WPA -   (Wi-Fi Protected Access - Acceso Wi-Fi protegido) Función IEEE 802.11 opcional que se utiliza para proporcionar seguridad de datos y que es equivalente a la de la red local cableada típica. Ofrece mayor seguridad que WEP mediante la codificación y autentificación de usuario.

BIBLIOGRAFÍA

Alonso, J. I. (2004). **La situación de las Tecnologías WLAN basadas en el estándar IEEE 802.11 y sus variantes ("Wi-Fi").** Colegio Oficial de Ingenieros de Telecomunicación Grupo de Nuevas Actividades Profesionales. Madrid, España. Disponible: http://www.minetad.gob.es/telecomunicaciones/Espectro/NivelesExposicion/Informacin/coitInforme_wifi_2004.pdf. [Consulta: 25 de julio 2017].

Arias, F. (2012). **El Proyecto de Investigación. Introducción a la Metodología Científica.** 6ta Ed. Editorial Episteme. Caracas, Venezuela. 143 pp.

Avendaño, L. (2013). **Hardware de una computadora personal**. Cisco Networking Academy. Disponible: https://jmc-laurapa23.jimdo.com/telecomunicaciones-11-ccna-discovery-2013/1-periodo/capitulo-1/. [Consulta: 24 de julio 2017].

Camargo, J.L. (2011). **Redes Inalámbricas de Área Local (WLAN).** Capítulo 3. Disponible:http://bibing.us.es/proyectos/abreproy/11761/direccion/Volumen1%252F. [Consulta: 25 de julio 2017].

Carlson, J. (2004). **Extensible Authentication Protocol (EAP).** Vollbrecht Consulting LLC. Disponible: https://tools.ietf.org/html/rfc3748. [Consulta: 25 de julio 2017].

Claros, I. (2010). **MODELO OSI**. Disponible: http://belarmino.galeon.com/. [Consulta: 25 de julio 2017].

Claver, A. (2015). **Elementos comunes de hardware de una red inalámbrica de área local**. Disponible: https://antonioclaver.wordpress.com/2015/04/13/elementos-comunes-de-hardware-de-una-red-inalambrica/. [Consulta: 27 de julio 2017].

Corral, Y., Fuentes, N., Maldonado, C. y Brito, N. (2012). **Algunos Tópicos y Normas Generales aplicables a la elaboración de Proyectos y Trabajos de Grado y Ascenso**. Segunda Ed. Fondo Editorial de la Universidad Pedagógica Experimental Libertador (FEDUPEL). 224 pp.

Daza, F. (2010). **Ataques Pasivos y Ataques Activos**. Disponible: http://feladazarodriguez.blogspot.com/2010/09/ataques-pasivos-y-ataques-activos.html. [Consulta: 24 de julio 2017].

De Anda, M. (2009). **Ruteadores.** Disponible: http://deandatovarmiriam.blogspot.com/2009/04/ruteadores.html. [Consulta: 24 de julio 2017].

Diaz, Y. (2007). **Estándares y Organizaciones de las LAN Inalámbricas**. Tutorial sobre Redes de Computadoras de Área Local. Disponible: http://www.ciberesquina.una.edu.ve/342_Redes/Temas/Tema03/Apartado03/a3pag1.htm. [Consulta: 27 de julio de 2017].

Escudero, A. (2007). **Unidad 02: Estándares en Tecnologías Inalámbricas.** Disponible:http://www.itrainonline.org/itrainonline/mmtk/wireless_es/files/02_es_estandares-inalambricos_guia_v02.pdf. [Consulta: 27 de julio de 2017].

Fata, O. (2011). **Redes de Sensores**. Trabajo de Grado de Redes de Sensores. Facultad de Informática. Universidad Nacional de la Plata. Argentina. Disponible: http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Fata_Omar_Americo.pdf. [Consulta: 25 de julio de 2017].

Gallinger, A. (2011). **WPA - Protocolo de seguridad Wi-Fi.** Disponible: http://argentows.blogspot.com/2011/05/wpa-protocolo-de-seguridad-wi-fi.html. [Consulta: 16 octubre 2017].

Gamma Internet Consultoría. (2003)

Garijo, S. (2014). **La importancia de los recursos humanos en la eficacia de la empresa. Trabajo de grado en Administración y Dirección de Empresas.** Universidad de Valladolid, España. Disponible: https://uvadoc.uva.es/bitstream/10324/5981/1/TFG-O%20180.pdf. Consulta: 25 de julio de 2017].

Hernández, R., Fernández, C. y Batista, P. (2010). **Metodología de la Investigación.** (Quinta Ed.) Editorial McGraw-Hill. Lima, Perú. 613 pp.

Huidobro, J.M. (2000). **Sistemas telemáticos**. Seg. Ed. Edit. Paraninfo. Madrid, España. 212 p. Disponible: https://books.google.co.ve/books?id=mN5wszBGZEsC&pg=PA244&lpg=PA244&dq=huidobro+sistemas+telematicos&source=bl&ots=uke4Ka5fPu&sig=imuDJ9d12leaDBuDlD1WOKX_iDI&hl=es&sa=X&ved=0ahUKEwjX6_DqsYzWAhVILSYKHUNrBRoQ6AEIXDAN#v=onepage&q=huidobro%20sistemas%20telematicos&f=false. [Consulta: 27 de julio de 2017].

Hurtado de B., J. (2012). **El Proyecto de Investigación. Comprensión Holística de la Metodología de Investigación.** (Septima Ed.). Ediciones Quirón. SYPAL. Caracas, Venezuela. pp.191.

Ibáñez, A. (2011). **Cómo crear tu Portal Cautivo con Easy Hotspot**. Disponible:http://recursostic.educacion.es/observatorio/web/es/equipamiento-tecnologico/redes/1005-como-crear-tu-portal-cautivo-con-easy-hotspot. [Consulta: 27 de julio de 2017].

Intel. (2013). **Zotac Launches New Ivy Bridge-Powered ZBOX Nano SFF PCs.** Disponible: https://www.pcper.com/category/tags/ivy-bridge. [Consulta: 16 octubre 2017].

Intel. (2017). **Comprensión IEEE * 802.11 autenticación y la asociación**. Disponible: https://www.intel.la/content/www/xl/es/support/network-and-io/wireless-networking/000006508.html. [Consulta: 26 de julio de 2017].

Intel (2017b). **Glosario de Términos**. Disponible: https://www.intel.com/support/sp/glossary.htm. [Consulta: 16 octubre 2017].

Kodak. (2015). **Glosario de términos básicos en tecnología inalámbrica**. Disponible:http://resources.kodak.com/support/shtml/es/manuals/urg00336/urg00336c6s7.shtml. [Consulta: 16 octubre 2017].

López, F. (2002**). El estándar IEEE 802.11. Wireless LAN**. Temas Avanzados de Redes de Ordenadores. Cursos Doctorado. Dpto. de Ingeniería de Sistemas Telemáticos. E.T.S.I. Telecomunicación - Universidad Politécnica de Madrid. Madrid, España. Disponible: http://www.dit.upm.es//~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf. [Consulta: 25 de julio 2017].

Lombas, O. (2013). **Medios inalámbricos**. En: Medios de Networking. Módulo 3. Disponible: https://es.slideshare.net/elwood_bluesman/redesccnatema5-33-medios-inalmbricos. [Consulta: 27 de julio 2017].

Manaure, J. (2013). **Equipos de una red.** Disponible: https://cursobasicodeadministracionderedes.wordpress.com/unidad-3/equipos-de-una-red/. [Consulta: 25 de julio 2017].

Martínez, M. (2016). **Redes Inalámbricas**. Disponible: http://proyectodegrado43.blogspot.com/2016/. [Consulta: 26 de julio 2017].

Madrid, J. M. (2004). **Seguridad en redes inalámbricas 802.11.** Sistemas y Telemática. N.3: 13-28. Disponible: http://www.icesi.edu.co/contenido/pdfs/sist_telema3.pdf. [Consulta: 26 de julio 2017].

Méndez, C. (2008). **Metodología de la Investigación**. México: Editorial Mc Graw Hill, C.A.

Miranda, H.G. (2010). **Estudio e Implementación de Mecanismos de Seguridad WPA2 para un Sistema de Distribución Inalámbrico para dar cobertura a tráfico de voz sobre IP.** Trabajo de Grado de Ingeniero en Electrónica y Computación. Escuela Superior Politécnica de Chimborazo. Cochabamba, Ecuador.Disponible:http://dspace.espoch.edu.ec/bitstream/123456789/641/1/38T00258.pdf. [Consulta: 16 de septiembre 2017].

Palella, S., y Martins, P., F. (2010). **Metodología de la Investigación Cualitativa.** (Tercera Ed.). Fondo Editorial de la Universidad Pedagógica Experimental Libertador. FEDUPEL. Caracas. Venezuela. 285 pp.

Panda Software International. (2005). **Seguridad en Redes Inalámbricas.** Disponible:http://ocw.upm.es/teoria-de-la-senal-y-comunicaciones-1/comunicaciones-moviles-digitales/contenidos/Documentos/WP_wifi_PSE.pdf. [Consulta: 28 de julio 2017].

Quispe, M. (2010). **Implementación de un Sistema Red Inalámbrico para compartir recursos Informáticos en el Instituto Superior Tecnológico Publico Huaycan**. Trabajo de Grado de Técnico en Computación e Informática. Instituto Superior Tecnológico Publico Huaycan. Lima, Perú. Disponible: https://es.scribd.com/doc/50666727/IMPLEMENTACION-DE-UN-SISTEMA-RED-INALAMBRICO-PARA-COMPARTIR-RECURSOS-INFORMATICOS-EN-EL-INSTITUTO-SUPERIOR-TECNOLOGICO-PUBLICO-HUAYCAN/ [Consulta: 26 de julio 2017].

Ramos, A. (2013). **Montando un Rogue AP con Kali**. Disponible: http://www.securitybydefault.com/2013/11/montando-un-rogue-ap-con-kali.html. [Consulta: 28 de julio 2017].

Rocha, M. (2009). **Telecomunicaciones: Comunicación de Datos. Elementos de un Sistema Informático**. Asoc.Coop. de la FCE/UNC, 2000. Disponible: https://ti-1.wikispaces.com/4.1+Telecomunicaciones. [Consulta: 26 de julio 2017].

Rojas, J. y González, S. (2007). **Las Tecnologías aplicadas a las Redes de Computadoras.** Trabajo de Grado de Ingeniero en Comunicaciones y Electrónica. Disponible: https://es.scribd.com/document/276409626/Tesis-Seguridad-a-Nivel-WLAN. [Consulta: 23 de julio 2017].

Sabino, C. (2009). **¿Cómo Hacer una Tesis? y elaborar todo tipo de Escrito**. Editorial PANAPO C.A. Impreso en Venezuela por Editorial MELVIN C.A. pp. 141.

Sepúlveda, F. (2011). **Routers "vecinos" en EIGRP**. Disponible: http://www.franciscosepulveda.eu/2011/12/28/routers-vecinos-en-eigrp/. [Consulta: 16 octubre 2017].

Silva, J. (2011). **Principales Estándares 802.11.** Disponible: http://ieeestandards.galeon.com/aficiones1573579.html. [Consulta: 27 de julio 2017].

Solís, E. (2015). **Redes inalámbricas. Introducción a las redes Wireless**. Disponible: http://ecovi.uagro.mx/wireless.html. [Consulta: 16 octubre de 2017].

Special Publication 800-97. **(**2007). **Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.** Disponible: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.pdf. [Consulta: 29 de julio 2017].

Special Publication 800-153. (2012). **Guidelines for Securing Wireless Local Area Networks (WLANs).** Disponible: http://csrc.nist.gov/publications/drafts/800-153/Draft-SP800-153.pdf. [Consulta: 29 de julio 2017].

Special Publication 800-48. (2008). **Guide to Securing Legacy IEEE 802.11 Wireless Networks.** Disponible: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-48r1.pdf. [Consulta: 29 de julio 2017].

Tamayo y Tamayo, F. (2003). **El Proceso de la Investigación Científica.** 3era Edición. Editorial Limusa, S.A de CV. México. pp. 231.

TechNet. (2017). **Configuración de puntos de acceso inalámbrico seguros**. Disponible: https://technet.microsoft.com/es-es/library/cc875845.aspx. [Consulta: 16 octubre 2017].

34Telecom SL. (2016). **Introducción a la norma de redes 802.X**. Disponible: http://www.34t.com/box-docs.asp?doc=639. [Consulta: 29 de julio 2017].

Zyxel. (2017). **Switches**. Disponible: https://www.zyxel.com/co/es/products_services/smb-switches.shtml?t=c. [Consulta: 16 octubre 2017].

ANEXOS

ANEXO 1

DESARROLLO LISTA DE VERIFICACIÓN

Objetivo 2. Diagnosticar los mecanismos de seguridad de la red WIFI IESONAIR utilizados en la Institución de Educación Superior (IES) Universidad Tecnológica Equinoccial, seleccionada como objeto de estudio.

Interrogante			**SI**	**NO**	**N/A**
1	¿Se utilizan las contraseñas LDAP definidas para cada uno de los usuarios				
2	¿Existe un tiempo de inactividad en el uso de la plataforma y de conexión a la red?				
3	¿Existe un refrescamiento de claves en la administración de usuarios de la red?				
4	¿Se eliminan usuarios en la cuenta de correo no están en el dominio de la institución?				
5	ni existe el puerto seguro para la conexión de equipos externos que no pertenecen a la universidad				
6	¿La WLAN les asigna ancho de banda por usuarios para controlar el tráfico?				
7	¿Segmentan la red por perfiles de usuarios (WLAN interna y WLAN externa?				
8	¿Los equipos de conexión son los óptimos, tales como:	Servidor principal: Controlador de dominio y DNS?			
9		Servidor secundario: Proxi, Firewall, Radius, Enrutamiento, Vlan?			
10		Programas monitoreo?			
11		Aplicaciones de auditoria para la red?			
12		Router?			
13		Switch principal?			
14		Switch secundario?			
15		Puntos de acceso?			
16		Adaptador de red?			
17	¿Los componentes de red que más solicitudes hacen y atienden están trabajando sin problemas, como estaciones de trabajo, puertos y servicios?				
18	¿Segmentan la red por perfiles de usuarios (red interna y red externa?				

Diseño lógico de la red		**SI**	**NO**	**N/A**
1	¿Los nombres de cuentas de usuario de dominio están estandarizados?			
2	¿Tienen cuenta de usuarios personalizados con políticas de restricciones?			
3	¿Se realizan pruebas de seguridad periódicamente?			
4	¿Se realizan pruebas de salto por salto entre entidad origen y cada elemento intermedio?			
5	¿Monitorean los logs para revisar posibles intromisiones?			

6	¿Los usuarios presentan restricciones para el uso de archivos en la WLAN?			
7	¿Los usuarios presentan problemas para reconocer la red inalámbrica?			
8	¿La Universidad cuenta o utiliza un modelo basado en dominios?			
9	¿Los equipos de conexión de la WLAN están actualizados para los requerimientos actuales de seguridad en las necesidades de la universidad?			
10	¿Se determinó como protocolo de red TCP/IP?			
11	¿Se revisan periódicamente el acceso asignados a las cuentas de usuario?			
12	¿Se registra la actividad de los usuarios en la navegación de páginas web?			
13	¿Se determinó los niveles de acceso a los recursos compartidos?			
14	¿Se suministraron herramientas necesarias para poder implementar mecanismos de integridad como MD5, entre otras?			
Configuración, autenticación y cifrado de equipos inalámbricos				
1	¿El servicio set identifier (SSID) por defecto del punto de acceso ha sido cambiado?			
2	¿La cadena de caracteres SSID es fácil de adivinar y refleja información sobre la empresa (nombre, ubicación, función)?			
3	¿El router inalámbrico, punto de acceso o puerta de enlace utiliza el Nombre de Red o SSID por defecto?			
4	¿Las claves se almacenan en texto plano?			
5	¿Los protocolos de gestión inseguros o innecesarios en los puntos de acceso han sido desactivados?			
6	¿Los parámetros por defecto han sido cambiados en los puntos de acceso?			
7	¿Los tamaños de clave cifrado son de por lo menos 128 bits o lo más grande posible?			
8	¿Las claves por defecto son reemplazadas por claves únicas más seguras?			
9	¿El Firewall configurado funciona para los usuarios de red interna y externa?			
10	¿Poseen servidor de control de navegación tipo ISA SERVER?			
11	¿Hay dispositivos en la red inalámbrica pueden usar dispositivos como impresoras, servidor de archivo?			
12	¿Los usuarios se autentican (Radius local, Kerbeos) con nombres de usuarios y contraseña para la red WLAN?			
13	¿Los equipos están configurados para prevenir el uso de conexiones duales?			
14	¿Se utiliza IPSec en lugar del predeterminado WEP como el protocolo de seguridad?			
15	¿Se utiliza el protocolo de autenticación 802.1x?			
16	¿Un algoritmo de cifrado más seguro que el algoritmo RC4 por defecto está en uso (3DES o AES)?			
17	¿La autenticación del usuario a la WLAN es obtenida a través de métodos más seguros (datos biométricos, tarjetas inteligentes, autenticación de dos factores, PKI, RSA)?			
18	¿Si no es totalmente necesario el DHCP en redes WLAN externas, está desactivado?			

19	¿El acceso se concede únicamente a las máquinas cliente con direcciones MAC registradas?			
20	¿Todas las funciones de seguridad posible que se proporcionan en la arquitectura están en uso?			
21	¿Manejan blacklist en páginas para la navegación web?			
22	¿Todos los clientes inalámbricos tienen firewall instalado?			

Administración de recursos humanos		**SI**	**NO**	**N/A**
Roles y responsabilidades				
1	¿Son definidos los roles y responsabilidades del personal sobre la red inalámbrica interna?			
2	¿Poseen conocimientos en los roles y responsabilidades del personal sobre la red inalámbrica?			
3	¿Estos roles y responsabilidades del personal están segmentados por departamentos de acuerdo a las necesidades de la organización?			
Términos y condiciones de empleo				
4	¿Los empleados acuerdan y firman los términos y condiciones del contrato de empleo?			
5	¿El contrato de empleo establece responsabilidades del personal y de la organización concerniente a la red inalámbrica interna?			
6	¿Se aclara, establece y firman acuerdos de confidencialidad o no divulgación a aquellos que tendrán acceso a la red inalámbrica?			
Durante el empleo				
7	¿Se verifica y solicita que los empleados apliquen seguridad inalámbrica de acuerdo con las políticas y procedimientos de seguridad?			
8	¿Todo el personal es capacitado para el desempeño de sus funciones sobre la WLAN interna y externa?			
9	¿Se monitorea al personal para cumplir con políticas de seguridad inalámbrica?			
Toma de conciencia, educación y entrenamiento sobre seguridad WLAN				
10	¿Todo el personal es capacitado regularmente en concientización y actualización de políticas y procedimientos de seguridad inalámbricas relevantes para su función?			
11	¿Se realizan capacitaciones al personal de modo que le permita conocer problemas e incidentes en la red inalámbrica?			
Proceso disciplinario				
12	¿Se sigue un proceso disciplinario formal para el personal que ha cometido una falta disciplinaria en la red inalámbrica?			
13	¿Se inicia el proceso disciplinario después de una previa verificación de que ha ocurrido una falta en la red inalámbrica?			
14	¿El proceso disciplinario asegura un tratamiento correcto y justo para el personal sospechoso?			
15	¿En casos de mala conducta los procesos permiten el retiro inmediato de sus derechos y obligaciones?			
Personal de limpieza				
16	¿El equipo de limpieza es restringido a la sala de telecomunicaciones para evitar el sabotaje?			
17	¿Si el personal de limpieza debe tener acceso a la sala de telecomunicaciones es acompañado por el personal de la misma área?			

18	¿Se permite el acceso a los visitantes a la sala de telecomunicaciones sin aprobación escrita?			
Finalización o cambio de empleado				
Finalización de responsabilidades				
19	¿Están claramente definidas y asignadas las responsabilidades para llevar a cabo la finalización o cambio de empleo?			
Retorno de recursos				
20	¿Todo el personal devuelve todos los equipos inalámbricos de la organización que están a su cargo al finalizar su empleo?			
21	¿En caso de que el empleado compra o usa su propio equipamiento se asegura que la información es transferida a la organización?			
Eliminación de los derechos de acceso				
22	¿Los derechos de acceso a la red inalámbrica son retirados, anulados o se ajustan al finalizar el empleo?			
23	¿Los derechos de acceso a la red inalámbrica e instalaciones son reducidos o eliminados antes de terminar o cambiar de empleo?			
24	¿Se cambian todas las contraseñas de cuentas que siguen activas a la finalización o cambio de empleo?			

Objetivo 3. Comparar los mecanismos de seguridad de la red WIFI IESONAIR recomendados por el Instituto Nacional de Estándares y Tecnología (NIST), con el procedimiento cumplido en una Institución de Educación Superior (IES).

Interrogante		**SI**	**NO**	**N/A**
1	¿Cuentan con un inventario de los equipos existentes para poder actualizarlo periódicamente?			
2	¿Cuentan con una lista de las aplicaciones para el monitoreo de tráfico?			
3	¿Se informan sobre nuevos tipos de ataque y vulnerabilidades para aplicar la seguridad a la WLAN?			
4	¿La topología de red definida es acorde a la seguridad de la organización?			
5	¿El estándar del cifrado en las claves criptográficas de seguridad fuerte es usado en la WLAN universidad?			
6	¿Puede asegurar que la comunicación en la WLAN no pueda ser leída por personas no autorizadas?			
7	¿Puede detectar cualquier cambio intencional o no intencional a los datos que ocurren en tráfico?			
8	¿Asegura que los dispositivos y las personas puedan acceder a una red y sus recursos cuando sea necesario?			
9	¿Tienen usuarios o grupos de usuarios que estén autorizados y no estén autorizados a utilizar WLAN de la organización?			
10	¿Restringe los derechos de los dispositivos o individuos a acceder a una red o recursos dentro de WLAN?			
11	¿Monitorean periódicamente la seguridad en la wlan?			
12	¿Permiten el uso de conexiones duales en las estaciones?			
13	¿Segmentan la red por perfiles de usuarios (WLAN interna y WLAN externa?			
14	¿Las tecnologías WLAN tienen los últimos parches de seguridad y actualizaciones?			