Universidad Autónoma del Estado de México

Centro Universitario UAEM Zumpango

Ingeniería en Computación

Mecanismos y estrategias de seguridad en redes Wi-Fi

TESINA MONOGRÁFICA

que para obtener el título de

Ingeniero en Computación

presenta:

Emanuel Meneses Angón

Asesora:

Dra. María de Lourdes López García

Zumpango, Estado de México Enero, 2014

Dedicatoria

Para mis padres Alicia y Leobardo, por su comprensión, apoyo, confianza, amor y ayuda incondicional en los buenos y no tan buenos momentos, gracias a sus consejos y palabras de aliento crecí como persona. Me han enseñado a enfrentar las adversidades sin perder nunca la dignidad ni desfallecer en el intento. Hoy día puedo decir que me han dado todo lo que soy como persona, mis valores mis principios, mi perseverancia y mi empeño.

Gracias a mi madre por los ejemplos de perseverancia y constancia que la caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y sobre todo por siempre estar al pendiente de mis acciones, exigirme y mostrarme que cada día puedo dar un poco más de mi.

A mi abuelita Natividad por todo su cariño amor, a pesar de no estar de cuerpo presente, me ha dejado muchas enseñanzas, por todos sus consejos, siempre vivirá en mi mente y sobre todo en mi corazón.

Agradecimientos

Primero y como más importante, me gustaría agradecer sinceramente al CU Zumpango de la Universidad Autónoma del Estado de México, que me dio todo y abrió sus puertas del conocimiento para mí. A mi maravillosa carrera Ingeniería en Computación nido de muchos que como yo eligieron esta extraordinaria carrera y que con mucho orgullo, amor, pasión y respeto representaré.

Me gustaría agradecer sinceramente a mi asesora y tutora de este trabajo, Dra. María de Lourdes López García, por su esfuerzo y dedicación. Sus conocimientos, su orientación, su manera de trabajar, su persistencia, su paciencia y su motivación han sido fundamentales para ver cumplido el objetivo. Ella ha inculcado en mí atributos como la responsabilidad y rigor académico, además de haberme enseñado un sentido de seriedad al trabajar en esta investigación. A su manera, ha sido capaz de ganarse mi lealtad y admiración, así como sentirme en deuda con ella por todo lo recibido durante el periodo de tiempo que ha durado este trabajo.

De igual manera me gustaría agradecer los consejos y enseñanzas recibidas a lo largo de estos últimos años por los profesores de Ingeniería en Computación del Centro Universitario UEAEM Zumpango, ya que de una u otra manera aportaron sus conocimientos para mi formación como profesional.

A mis hermanos, por su compañía y el apoyo que me brindan. Sé que cuento con ustedes siempre. Y sobre todo a mis sobrinas Evolet y Cristal que son una motivación para seguir superándome y ser cada día mejor.

Y por último, pero no menos importante a mis revisores Arturo Redondo y Rafael Rojas, por sus consejos y observaciones, que estoy seguro me servirán para mi vida como profesionista.

Resumen

La flexibilidad y movilidad que proporcionan las redes inalámbricas han hecho que la implementación y utilización de las mismas se haya disparado en los últimos años. Este tipo de redes se caracteriza por su fácil implementación, comodidad de transmisión, facilidad de operación y bajo costo de instalación. De tal manera que, se han convertido en una excelente alternativa para ofrecer conectividad en lugares donde resulta complicado o imposible brindar servicio con una red cableada.

En los últimos años, la utilización de las redes inalámbricas ha crecido de manera exponencial, principalmente, en lugares donde se opta por esta tecnología tanto para la transmisión de datos entre dispositivos inalámbricos, como para el acceso de estos al resto de la red o a Internet a través de protocolos como Bluetooth o Wi-Fi (*Wireless Fidelity*), por mencionar algunos.

No obstante, cualquier tipo de red inalámbrica presenta riesgos ante un medio de transmisión tan observable como lo son las ondas de radio, lo que implica que la información viaje a través del aire de manera que cualquier individuo equipado con los dispositivos y conocimientos necesarios pueda interceptar la señal y analizarla. Sin embargo, obtener la señal no significa que pueda extraer la información, esto siempre y cuando se tomen las medidas necesarias para garantizar la seguridad de la información transmitida.

Así, en este documento estamos interesados en la seguridad de las WLAN, por lo que, presentamos una descripción completa de los protocolos de seguridad para este tipo de redes, sus vulnerabilidades y estrategias para disminuir el porcentaje efectivo de ataques. Desde estrategias muy básicas y sencillas de implementar, hasta mecanismos más robustos y con un grado mayor de complejidad en su configuración e implementación. Finalmente, con base en lo anterior el usuario final sea capaz de determinar la mejor opción para brindar el grado de seguridad de la información requerido, para este tipo de redes.

Abstract

The flexibility and mobility that the wireless networks provide have done that the implementation and utilization of the same ones has gone growing in the last years. This type of networks is characterized by his easy implementation, comfort of transmission, facility of operation and under cost of installation. In such a way that, they have turned into an excellent alternative to offer connectivity in places where it turns out to be complicated or impossible to offer service with a wired up network.

In the last years, the utilization of the wireless networks has grown in an exponential way, principally in places where it is chosen this technology so much for the transmission of information between wireless devices, as for the access of these to the rest of the network or to Internet across protocols as such as Bluetooth or Wi-Fi (Wireless Fidelity), to name a few.

Nevertheless, any type of wireless network presents risks before a medium so observable as they it are the waves of radio, which implies that the information travels across the air so that any individual equipped with the devices and necessary knowledge could intercept the sign and to analyze it. Nevertheless, the fact of obtaining the sign does not mean that it could extract the information, this always and when the necessary measurements are taken to guarantee the safety of the transmitted information.

This way, in this document we are interested in the safety of the networks Wi-Fi, for what, we submit a complete description of the safety protocols for this type of networks, his vulnerabilities and strategies to diminish the effective percentage of attacks. From very basic and simple strategies up to more robust mechanisms and with a major degree of complexity in his configuration and implementation. Finally, with base in the previous thing, the end user is able to determine the best option to provide the degree of security required for this type of information networks.

Contenido

Dedicatoria **III**

Agradecimientos **V**

Resumen **VII**

Abstract **IX**

Contenido **XI**

Lista de figuras **XV**

Lista de tablas **XVII**

1. Introducción **1**

1.1 Planteamiento del problema 1

1.2 Justificación 2

1.3 Objetivos 2

Objetivo General 2

Objetivos específicos 2

1.4 Alcance del proyecto 3

1.5 Organización del documento 3

2. Redes inalámbricas **5**

2.1 Definición de red inalámbrica 5

2.2 Tipos de redes inalámbricas 6

2.3 Componentes de una WLAN 8

2.4 Cobertura de una WLAN 11

2.5 Topologías de las WLAN 13

2.6 Estándar IEEE 802.11 15

2.6.1 Modelo de capas del Estándar IEEE 802.11 20

2.7 Ventajas y Desventajas de las WLAN 22

3. Wi-Fi (*Wireless Fidelity*) 27

3.1 Historia 27

3.2 Seguridad 28

3.3 Herramientas criptográficas 35

4. Protocolos de seguridad en las WLAN 41

4.1 Estándar IEEE 802.1X 41

4.2 EAP (*Extensible Authentication Protocol*) 43

4.2.1 Ventajas y desventajas 45

4.3 Protocolo WEP (*Wired Equivalent Privacy*) 46

4.3.1 Funcionalidad 48

4.3.2 Variantes de WEP 54

4.3.3 Ventajas y desventajas 55

4.4 Protocolo WPA (*Wi-Fi Protected Access*) 57

4.4.1 Funcionalidad 57

4.4.2 Ventajas y desventajas 59

4.5 Protocolo WPA2 60

4.5.1 Funcionalidad 60

4.5.2 Ventajas y desventajas 69

5. Mecanismos y estrategias de seguridad en redes Wi-Fi 73

5.1 Estrategias básicas de seguridad 73

5.1.1 No implementar tecnología WLAN 73

5.1.2 Cambiar el ESSID por defecto 74

5.1.3 Cambiar la contraseña por defecto 75

5.1.4 Desconectar el PA cuando no se encuentre en uso 75

5.1.5 Desactivar el broadcasting ESSID 75

5.1.6 Establecer el número máximo de dispositivos que pueden conectarse 75

5.1.7 Cambiar las llaves WEP regularmente 76

5.1.8 Desactivar DHCP 76

5.1.9 Activar el filtrado de direcciones MAC 76

5.2 Mecanismos de seguridad a nivel capa de encale de datos 78

5.2.1 Hacer uso de protocolos de cifrado de datos 78

5.2.3 Utilizar cifrado de datos y autenticación IEEE 802.1X-EAP 78

5.3 Mecanismos de seguridad a nivel capa de red 79

5.3.1 Utilizar una red privada virtual (VPN) 79

5.3.2 Utilizar IPSec para proteger el tráfico de la WLAN 80

5.4 Comparativa entre protocolos de cifrado WEP, WPA y WPA2 83

5.5 Comparativa entre soluciones de seguridad a nivel capa enlace de datos y a nivel capa de red 85

6. Proceso de la toma de decisiones para una red Wi-Fi segura 87

7. Conclusiones y Trabajo futuro 91

7.1 Trabajo futuro 93

Referencias 95

Lista de figuras

Figura 2.1. Ejemplo de una red inalámbrica de área local (WLAN) 8

Figura 2.2. Diagrama de estados para la conexión a una WLAN 9

Figura 2.3. Ejemplo de IBSS 12

Figura 2.4. Ejemplo de BSS extendido y DS 13

Figura 2.5. Rango típico de cobertura de una WLAN 13

Figura 2.6. Topología en modo AD HOC 14

Figura 2.7. Topología en modo infraestructura 15

Figura 2.8. Representación de los tiempos que intervienen en el mecanismo de acceso CSMA/CA 17

Figura 2.9. Diagrama de flujo del funcionamiento del CSMA/CA 18

Figura 2.10. Modelo de Capas IEEE 802.11 21

Figura 3.1. Método de Autenticación de Sistema Abierto 30

Figura 3.2. Mecanismo de autenticación de llave compartida 31

Figura 3.3. Acceso no autorizado a la red inalámbrica 32

Figura 3.4. Warchalking y su simbología 34

Figura 3.5. Wardriving y sus requisitos 34

Figura 4.1. Diagrama general de autenticación IEEE 802.1X 42

Figura 4.2. Diálogo EAP-RADIUS 43

Figura 4.3. Arquitectura de seguridad con WEP red corporativa 49

Figura 4.4. Canal de datos confidencial 49

Figura 4.5. Funcionamiento del algoritmo WEP en modalidad de cifrado 50

Figura 4.6. Funcionamiento del algoritmo WEP en modalidad de descifrado 51

Figura 4.7. Arquitectura de seguridad con WPA 59

Figura 4.8. Fases operacionales de WPA2 Guillaume Lehembre 63

Figura 4.9. Fase 1 acuerdo sobre política de seguridad 64

Figura 4.10. Fase 2 autenticación mediante IEEE 802.1X 65

Figura 4.11. Fase 3 derivación y distribución de llaves 66

Figura 4.12. Fase 3 jerarquía de llave por parejas 67

Figura 4.13. Fase 4 esquema y Cifrado de TKIP *Key Mixing* 68

Figura 4.14. Cifrado CCPM 69

Figura 5.1. Funcionamiento básico de VPN 80

Figura 6.1. Diagrama de flujo para la toma de decisiones para una WLAN 89

Lista de tablas

Tabla 2.1. Comparativa entre versiones del estándar IEEE 802.11 20

Tabla 3.1. Principales amenazas físicas para WLAN 37

Tabla 4.1. Amenazas y soluciones del estándar IEEE 802.1X 41

Tabla 4.2. Cronología de las vulnerabilidades en el protocolo WEP 48

Tabla 4.3. Transmisión y recepción del mensaje 53

Tabla 4.4. Operación XOR 53

Tabla 4.5. Diferentes modos de WPA 58

Tabla 4.6. Diferentes modos de WPA2 61

Tabla 5.1. Mecanismos y Estrategias de seguridad 74

Tabla 5.2. Comparativa de los enfoques de seguridad; autenticación y cifrado 84

Tabla 5.3. Comparativa de los enfoques de seguridad para las redes WLAN 85

Capítulo 1
Introducción

Con el paso de los años, nuestra sociedad ha experimentado una evolución en los medios de comunicación, dando origen a nuevas técnicas para transmitir información, un ejemplo de ello es la tecnología de comunicación inalámbrica. Dicha tecnología provee al usuario ciertas comodidades o ventajas de tal manera que su implementación y utilización fue incrementándose considerablemente en los últimos años [20].

1.1 Planteamiento del problema

Existen diversos tipos de redes inalámbricas de entre las cuales se pueden mencionar las redes de visión directa y las de visión no directa. Las primeras pueden ser a través de señales infrarrojas como la tecnología IrDa (*Infrared Data Association*), mientras que en las segundas se encuentran las redes Bluetooth, HomeRF y Wi-Fi, entre otras [2,13].

En este documento, estamos interesados en las redes inalámbricas Wi-Fi que se encuentran regidas por el estándar IEEE 802.11, ya que son las más utilizadas en la comunicación inalámbrica [13].

En la actualidad es un hecho que la tecnología Wi-Fi es una de las más poderosas en comunicación inalámbrica. Conforme pasa el tiempo, se implementa de manera más frecuente en diversos dispositivos electrónicos, principalmente en los dispositivos móviles, por lo cual surge la necesidad de considerar de manera más detallada el aspecto de la seguridad de la información [13].

Las WLAN al igual que cualquier tipo de red inalámbrica es considerada como insegura, debido a que emplea el aire como medio para transmitir la información, lo que implica que las señales viajen libres. Dicha característica la convierte en un blanco fácil para posibles ataques, por esta y más razones, las WLAN necesitan mecanismos de seguridad para garantizar la protección de la información a un nivel adecuado [13].

Es importante mencionar que la seguridad de la información transmitida a través del aire, en muchas ocasiones, pasa desapercibida. Los usuarios envían información privada o personal que

cualquier atacante puede monitorear y obtener para ser utilizada a su beneficio.

1.2 Justificación

Dado el problema de la vulnerabilidad de las redes inalámbricas, surge la necesidad de informar e instruir a los usuarios, los ataques y los mecanismos de seguridad que se encuentran a su alcance para que éstos sean utilizados de una forma precisa, de tal manera que la transmisión se realice sin que los atacantes puedan obtener y hacer uso inapropiado de la información.

En este documento, nos enfocamos en las soluciones que se han propuesto para mantener la comunicación segura de las redes inalámbricas, desde soluciones básicas de seguridad hasta soluciones robustas que normalmente son requeridas en entornos empresariales donde la confidencialidad e integridad de la información es un aspecto fundamental.

1.3 Objetivos

Objetivo General

Describir los principales mecanismos de seguridad para WLAN, para la reducción de riesgos en las posibles vulnerabilidades en el acceso externo no autorizado a la información de este tipo de redes.

Objetivos específicos

- Investigar las formas de comunicación inalámbrica.
- Describir las deficiencias en la seguridad de redes las WLAN.
- Detallar la tecnología y la funcionalidad de las WLAN.
- Analizar los esquemas de seguridad implementados en las WLAN.
- Describir las vulnerabilidades de los esquemas de seguridad de las WLAN.
- Investigar las soluciones propuestas a las vulnerabilidades de las WLAN.
- Realizar comparativas de diversos mecanismos de seguridad, así como el análisis de sus ventajas y desventajas.

1.4 Alcance del proyecto

El alcance de este proyecto de investigación consiste en una descripción a detalle de los principales mecanismos de seguridad utilizados en la tecnología de comunicación inalámbrica Wi-Fi.

Al terminar esta investigación, se obtendrá un documento guía o manual que servirá de base para poder realizar la implementación de un mecanismo de seguridad confiable, ya sea en el diseño e instalación de una nueva red o en una previamente instalada.

Todo lo anterior con la finalidad de proveer al lector los conocimientos básicos e intermedios de los ataques y los mecanismos de seguridad implementados en las WLAN.

1.5 Organización del documento

La organización del resto del documento se estructura de la siguiente manera. En el Capítulo 2, se presentan las bases para poseer un mejor entendimiento de las redes, enfocados principalmente en las redes de área local inalámbrica (WLAN). Se presentan los componentes necesarios, su cobertura o alcance, las principales topologías en las cuales se rigen, además de los estándares existentes que normalizan este tipo de redes y finalmente un balance entre ventajas y desventajas ofrecidas por las mismas.

En el Capítulo 3, se presenta un análisis basado en la tecnología Wi-Fi desde sus inicios, pasando por aspectos de mayor importancia como son la seguridad, describiendo los servicios de seguridad ofrecidos, los principales mecanismos de autenticación y algunos ataques a los que se encuentra expuesta. Además de la descripción general de las principales herramientas criptográficas que son utilizadas por esta tecnología.

El Capítulo 4 presenta una descripción sobre los principales protocolos de seguridad utilizados en las redes regidas por el estándar IEEE 802.11, es decir desde WEP (*Wired Equivalent Privacy*), WPA (*Wireless Protected Access*) y WPA2.

En el Capítulo 5, se realiza una descripción de los principales mecanismos y estrategias de seguridad existentes para la protección de las WLAN, las cuales se adecuan de acuerdo al nivel de seguridad requerido por el usuario final, es decir desde estrategias muy básicas, hasta mecanismos más robustos y por consecuencia más seguros.

El Capítulo 6, con la información proporcionada en los capítulos anteriores, se presenta la posibilidad de tomar decisiones justificadas sobre cómo aplicar cada opción de seguridad ya sea a entornos personales o empresariales, según sea el caso.

Finalmente, en el Capítulo 7 se presentan las conclusiones y trabajo futuro de ésta investigación.

Capítulo 2
Redes inalámbricas

En este capítulo se presentan los conceptos básicos, características, funcionalidad, ventajas y desventajas de las redes inalámbricas, necesarios para el correcto entendimiento de los mecanismos de seguridad mencionados en los siguientes capítulos de este documento.

2.1 Definición de red inalámbrica

Una red inalámbrica es un sistema de comunicación de datos que proporciona conexión inalámbrica entre dispositivos situados dentro de la misma área (interior o exterior) de cobertura. En lugar de utilizar cables como el par trenzado, el cable coaxial o la fibra óptica utilizados en las redes de área local (LAN) convencionales. Las redes inalámbricas transmiten y reciben datos a través de ondas electromagnéticas usando el aire como medio de transmisión. Así, una red inalámbrica permite a sus usuarios conectarse a una red o a Internet, sin la necesidad de usar cables. Existen básicamente tres categorías generales de las redes inalámbricas [24, 31]:

1. **Larga distancia:** utilizadas para transmitir la información en distancias que pueden variar desde una misma ciudad o hasta varios países aledaños; sus velocidades de transmisión son relativamente bajas, de 4.8 a 19.2 Kbps aproximadamente y poseen la capacidad de cubrir distancias desde unos 100 a 1000 km.

2. **Media distancia:** utilizadas para distancias cortas a medianas como en municipios o conjuntos residenciales por mencionar algunos, gracias a su movilidad el ancho de banda que proporcionan es reducido entre 1 Mbps a 3 Mbps. En la mayoría de las ocasiones este tipo de redes hace uso de antenas direccionales, las cuales son capaces de superar 1 km de distancia, para poder establecer una comunicación exitosa.

3. **Corta distancia:** utilizadas principalmente en redes corporativas cuyas oficinas se encuentran en uno o varios edificios relativamente cercanos, es decir, su cobertura no supera los 100 metros de distancia además de que alcanzan velocidades del orden de 280 Kbps hasta los 2 Mbps.

En resumen una red de tipo inalámbrica funciona de la misma manera que cualquier otro tipo de redes de comunicación entre dispositivos, consiste básicamente en conectar dispositivos móviles

formando redes con una infraestructura libre de cables, lo que es una ventaja apreciable ya que proporciona a los usuarios mayor movilidad sin perder la conexión a la red de datos que pueden provenir de otros dispositivos, Servidores, bases de datos, Internet, por mencionar algunos [22, 26].

2.2 Tipos de redes inalámbricas

Las redes inalámbricas se clasifican en dos principales tipos [26]:

1. Las redes inalámbricas que **necesitan una línea de visión directa y sin elementos que bloqueen la señal**, por ejemplo las señales de infrarrojos (IR), las cuales se rigen bajo la tecnología IrDa, estándar utilizado por los dispositivos de señales infrarrojas (IR). Típicamente este tipo de redes necesitan de un funcionamiento próximo entre los dispositivos que la conforman, para poder establecer una comunicación exitosa. El hecho de que sean consideradas como las iniciadoras de las redes inalámbricas deriva una serie de ventajas y desventajas, dentro de las primeras se encuentran ejemplos como emisores/receptores simples y baratos, además de que no interfieren con otros dispositivos de radio frecuencia (FR). En las segundas se encuentra la limitación del ancho de banda y la necesidad de comunicación visual , ésta es una desventaja importante, ya que no es posible comunicar dos dispositivos que se encuentren situados en salas diferentes, por otro lado, habitualmente las comunicaciones sólo son entre dos dispositivos [5, 26].

   Este tipo de redes son normalmente llamadas WPAN *(Wireless Personal Area Network)*, están pensadas para cubrir un área del tamaño de una habitación en el mejor de los casos y están basadas en infrarrojos que permiten la comunicación entre dos elementos (computadoras portátiles, PDAs, etc.,) a baja velocidad y a una distancia cercana.

2. Las redes inalámbricas que **NO necesitan una línea de visión directa**, como son las señales de radiofrecuencia para la transmisión de información, son capaces de traspasar objetos sólidos, además de poseer una mayor cobertura o alcance para establecer una comunicación entre sus dispositivos. Las señales de radio, los rayos X o las RF son capaces de traspasar objetos sólidos mientras que otras, como las señales infrarrojas, no poseen dicha capacidad. Existen diversos tipos de redes inalámbricas que se clasifican en función del rango de frecuencias utilizado por cada una y en función de su rango de cobertura [24, 26]:

2.1 **WLAN (*Wireless Local Área Network*):** es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas. Utiliza tecnologías de radiofrecuencia para transmitir y recibir datos a través de ondas electromagnéticas. Permite mayor movilidad a los usuarios al minimizar las conexiones cableadas, estableciendo conexión a los usuarios situados dentro de la misma zona de cobertura, tales como oficinas, campus, hogares, edificios o espacios públicos. En este tipo de redes se puede encontrar tecnologías inalámbricas basadas en *HiperLAN* un estándar del grupo ETSI (*European Telecommunications Standards Institute*), o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes. Ejemplos prácticos de este tipo de redes son las tecnologías Bluetooth, HomeRF (*Home Radio Frequency*) y WECA (*Wireless Ethernet Compatibility Alliance*).

2.2 **WMAN (*Wireless Metropolitan Area Network*):** es un sistema de comunicación para redes de área metropolitana basado en el estándar de comunicación inalámbrica IEEE 802.16 conocido también como WiMAX (*Worldwide Interoperability for Microwave Access*), estándar orientado a sistemas de acceso radio de banda ancha.

2.3 **WWAN (*Wireless Wide Area Network*):** son redes cuyo ámbito cubre áreas más amplias. Por su gran tamaño, estas redes son explotadas por las empresas de telefonía móvil o ISPs (*Internet Service Providers*) con el UMTS (*Universal Mobile Telecommunications System*), utilizado en los teléfonos móviles de tercera generación (3G) y en la tecnología digital para móviles GPRS (*General Packet Radio Service*).

Dentro del grupo de las redes inalámbricas que **NO necesitan una línea de visión directa** y las WLAN se encuentran las redes que nos competen, es decir, las redes definidas por el estándar IEEE 802.11**,** las cuales son requeridas por todas aquellas aplicaciones en donde existan limitaciones para la instalación de infraestructura de cableado, dichas limitaciones pueden deberse a situaciones como la necesidad de un rápido despliegue en edificios sin cableado, por ejemplo una compañía que se muda a un nuevo edificio, se pueden también presentar dificultades para instalar cableado por razones de acceso, estética o asepsia, etc., un quirófano sería un caso de esta última, en muchas ocasiones surge la necesidad de movilidad de los usuarios finales, o existe una gran dispersión de usuarios con distancias mayores a los 100 metros, dicha distancia es considerada como máxima normalizada por IEEE 802.3 para Ethernet [7].

2.3 Componentes de una WLAN

Las WLAN no necesitan un medio físico guiado, ya que como se mencionó anteriormente, utilizan ondas de radio para llevar la información de un punto a otro. Para que una WLAN establezca una comunicación exitosa, son necesarios diversos elementos ya sean físicos (dispositivos electrónicos) o no (medio de transmisión; el aire). Estas redes normalmente utilizan las bandas ISM (*Industrial Scientific and Medical*) es una banda libre que incluye lo rangos ubicados en 900 MHz, 2.4 GHz y 5.7 GHz. Estas bandas son de uso común y no requieren de licencia para utilizarlas. Uso común implica que no están protegidas frente a interferencias y que no pueden interferir en aplicaciones con licencia. En la **Figura 2.1** se muestra una configuración de una red WLAN, que se enlaza a una red LAN fija. Se puede apreciar tanto a las estaciones de trabajo inalámbricas (WSTA) como los Puntos de Acceso (PA), ambos descritos a continuación [24, 25, 27].

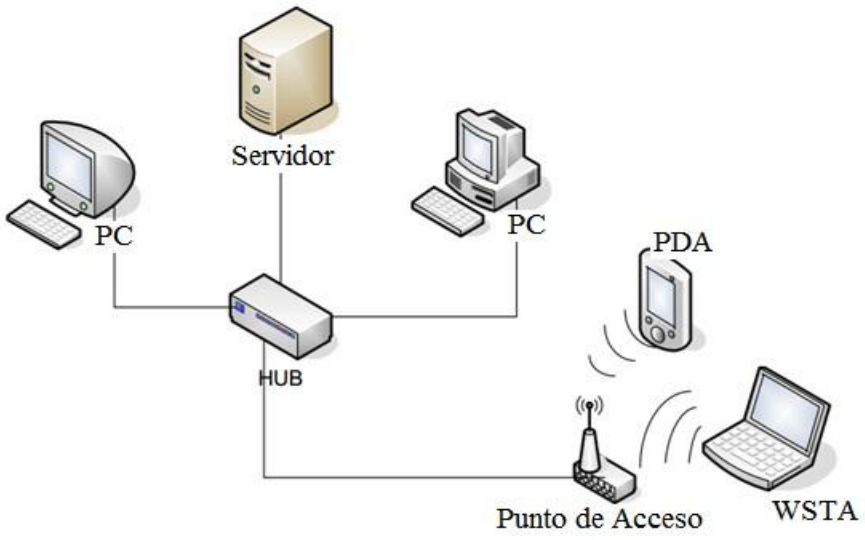

Figura 2.1: ejemplo de una red inalámbrica de área local (WLAN)

PA: un punto de acceso es un nodo (nodo refiere a las terminales conectadas a una red,) capaz de transmitir y recibir señales que viajan por la red, dicho dispositivo se comunica con los demás nodos de la red, siempre y cuando estos estén equipados con un adaptador o bien una tarjeta de red inalámbrica, además de una correcta configuración de las mismas. Por defecto, transmite señales de gestión periódicas, la WSTA recibe dichas señales e inicia la autenticación mediante el envió de una trama de autenticación, una vez realizada esta tarea, la WSTA envía una trama asociada y el PA responde con otra, cabe mencionar que los PA pueden conectarse a redes cableadas, pero de igual manera pueden funcionar de manera independiente, esto para poder ampliar el rango de transmisión de una red de tipo inalámbrica [25, 27].

Estaciones de trabajo inalámbricas (WSTA): por otro lado se encuentran las estaciones cliente de tipo inalámbricas, las cuales son los dispositivos que utilizan las personas que se conectan a las WLAN a través de los PA. Dichas estaciones deben de estar regidas bajo el estándar IEEE 802.11, por lo cual deben poseer tarjetas de red inalámbricas que pueden ser de varios tipos tales como PCMCIA, PCI o USB. En el estándar IEEE 802.11 se definen básicamente cuatro servicios que debe ofrecer una WSTA para que pueda conectarse exitosamente a la red, en el caso de la autenticación sirve para controlar el acceso a la red y así mejorar la seguridad, la des autenticación para eliminar a un usuario de la red y así evitar que pueda utilizar los recursos de la red, privacidad sirve para proteger los datos transmitidos a través de la red y por último el transporte de unidad de servicios de la capa MAC (*Media Access Control*), éste último es un servicio que asegura la transmisión y recepción de información de una manera confiable [31].

En la **Figura 2.2** se muestra el diagrama de estados que contiene los pasos que debe realizar una WSTA para asociarse a un PA [20]:

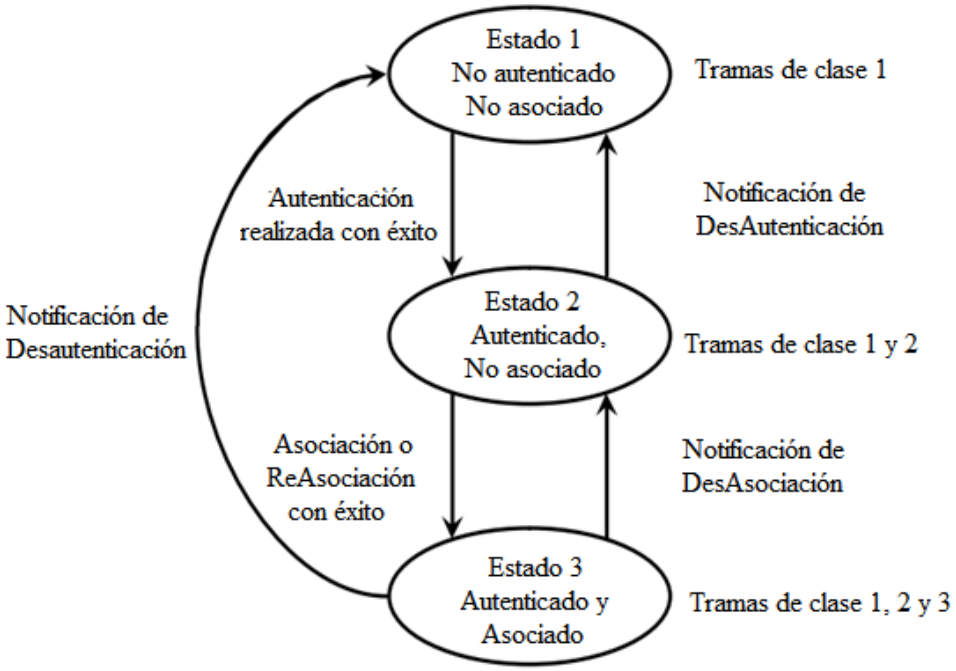

Figura 2.2: diagrama de estados para la conexión a una WLAN [20]

La autenticación en una WLAN se lleva a cabo en la capa 2 del modelo OSI (*Open System Interconnection*), dicha acción es el proceso de autenticar el dispositivo y no al usuario, es por eso que este punto es considerado como fundamental para poder garantizar la seguridad, en la detección de fallos y administración general de una WLAN. Antes de que una WSTA pueda asociarse a la red, debe establecer su identidad, para ello debe superar una serie de pruebas o desafíos que permitan saber quién se quiere conectar es quien dice ser. El proceso se inicia

cuando la WSTA envía una trama de petición de autenticación al PA y éste acepta o rechaza la trama, la WSTA recibe una respuesta por medio de una trama de respuesta de autenticación. También puede configurarse el PA para derivar la tarea de autenticación a un Servidor de autenticación, que realizaría un proceso de credencial más exhaustivo. Es importante mencionar que la autenticación en este tipo de redes puede ser abierta o de llave compartida, aspectos que se abordaran más a detalle posteriormente.

La asociación que se realiza después de la autenticación, es el estado que permite que una WSTA use los servicios del PA para transferir datos. Para que un dispositivo se pueda asociar a un PA debe realizar dos pasos, los cuales poseen 3 estados o tipos de autenticación y asociación [20]:

- *Sin autenticación y desasociado:* el nodo no ha sido autenticado en la red y no está asociado al PA.
- *Con autenticación y desasociado:* el nodo ha sido autenticado en la red, pero todavía no ha sido asociado al PA.
- *Con autenticación y asociado:* el nodo está conectado a la red y puede transmitir y recibir datos a través del PA.

En la transición por los diferentes estados, ambas partes como la WSTA y el PA, intercambian mensajes llamados *management frames*. El proceso que realiza una WSTA para encontrar y asociarse con un PA es el siguiente [20]:

1. Los PA transmiten *BEACON FRAMES* cada cierto intervalo de tiempo fijo. Para asociarse con un PA y por consiguiente a una red en modo infraestructura, la WSTA escucha en busca de *BEACON FRAMES* para identificar PA. La estación también puede enviar una trama *PROVE REQUEST* que contenga un ESSID (*Extended Service Set ID*) determinado para ver si le responde un PA que tenga el mismo ESSID.

2. Después de identificar al PA, la WSTA y el PA realizan autenticación mutua intercambiando varios *MANAGEMENT FRAMES* como parte del proceso.

3. Posteriormente de una autenticación realizada con éxito, la WSTA pasa al segundo estado de la **Figura 2.2**.

4. Para llegar al tercer estado, la WSTA debe mandar una trama *ASSOCIATION REQUEST* y el PA debe contestar con una trama *ASSOCIATION RESPONSE*, entonces la estación se convierte en un nodo más de la WLAN y ya está listo para enviar y recibir datos.

La antena del dispositivo emisor PA: tiene la finalidad de expandir la señal de manera abierta, los enrutadores utilizan prácticamente una antena omnidireccional, la cual consiste en transmitir una onda de forma circular que se abre en radio con centro en la posición de la antena, es decir, la onda se despliega apuntando a cualquier dirección dentro de su cobertura. Dado que los dispositivos van a ser usados por el usuario en una casa o estancia, cuyo objetivo no es alcanzar cobertura mayor, la antena omnidireccional debe estar a la altura del techo o en el punto más alto, esto producirá una mejor cobertura que si la antena estuviese a la altura de los dispositivos a interconectar [12,13].

La antena del dispositivo receptor WSTA: es la tarjeta de red inalámbrica que contienen las WSTA, se dice que dicha antena es más compleja en comparación con la del dispositivo repetidor o PA, aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente [12].

2.4 Cobertura de una WLAN

La celda es considerada como el elemento fundamental de la arquitectura de las WLAN, dicha celda define el área geográfica en la cual los dispositivos se interconectan inalámbricamente. Suele ser de tamaño reducido, aunque mediante la implementación de diversas fuentes de emisión es posible combinar las celdas para cubrir de forma casi total un área más extensa. En general, la celda está compuesta por un único PA y las WSTA que son consideradas como adaptadores que permiten la conversión de información, normalmente encapsulada bajo el protocolo Ethernet (IEEE 802.3), lo cual permite el envío y recepción de información dentro de la celda. El PA tiene la capacidad de gestionar todo el tráfico de las WSTA y puede comunicarse tanto a su celda de cobertura, como a otras redes a las cuales estuviese conectado, a esta configuración se le denomina BSS (*Basic Service Set*). Una WSTA puede tener vinculación con otro BSS a través del PA mediante un sistema de distribución DS (*Distribution System*) encargado de comunicar el BSS con una red externa, del cual se derivan otras clasificaciones como las siguientes [10,24]:

BSS Independiente (IBSS): un BSS es independiente cuando en una celda inalámbrica no existe un sistema de distribución, por lo tanto, no tiene conexión con otras redes, es por eso que es utilizada en las redes inalámbricas sin salida a otras redes (**Figura 2.3**).

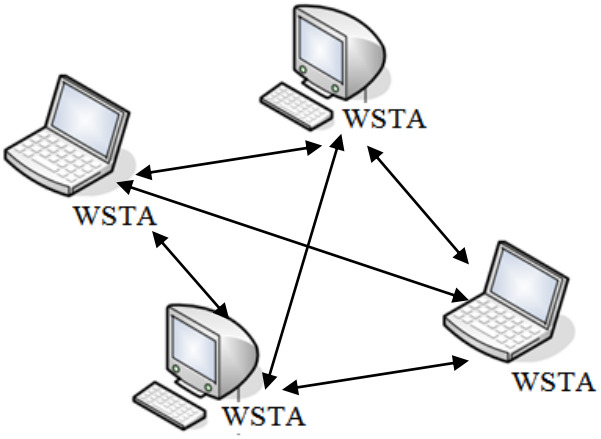

Figura 2.3: ejemplo de IBSS (Conjunto de servicios básicos independientes)

BSS Extendido (ESS): se representa por un conjunto de BSS asociados mediante un sistema de distribución, esto permite que una serie de prestaciones avanzadas opcionales como el roaming (itinerancia; capacidad de un dispositivo para moverse de una zona de cobertura a otra) entre celdas se presenten como una LAN simple para el nivel LLC (*Logical Link Control*) es decir la capa de control de enlace, sin notar que forman diferentes puntos de la red (**Figura 2.4**).

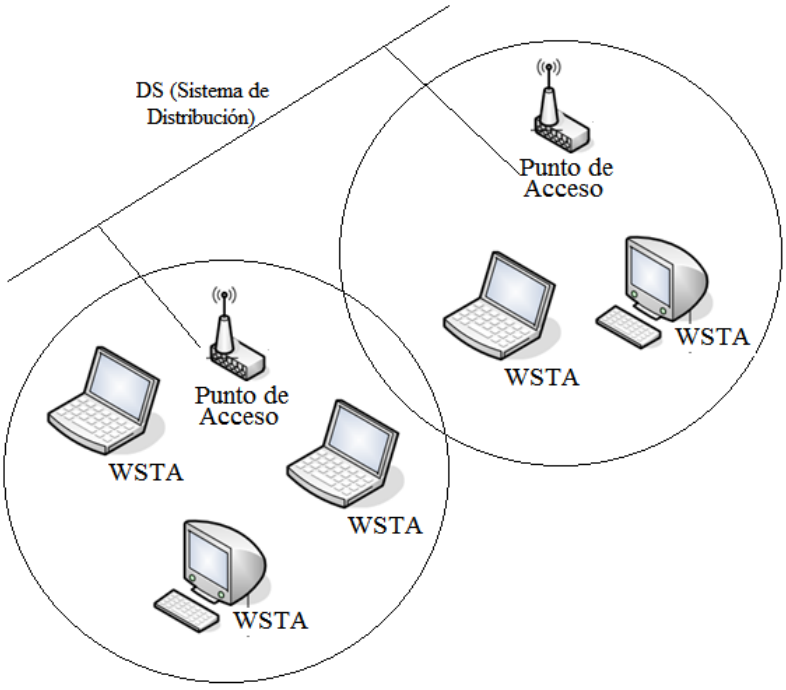

Figura 2.4: ejemplo de BSS extendido y DS [10]

De manera práctica la cobertura confiable para las WLAN depende de diversos factores, como la tasa de transferencia y su capacidad, fuentes de interferencia de radiofrecuencias, área y características físicas, potencia, conectividad y por último el uso de la antena.

Teóricamente los rangos son aproximadamente de 29 metros a una velocidad de 11 Mbps en un área cerrada y hasta 485 metros a una velocidad de 1 Mbps en un área abierta. Mientras que en un análisis empírico, los rangos varían desde 50 metros en interiores a 400 metros en exteriores, por lo cual las WLAN son consideradas como ideales para diversas aplicaciones. Es importante reconocer que con la adición de antenas especiales con alta ganancia, se puede incrementar el rango de cobertura a varios kilómetros. La **Figura 2.5** muestra con un ejemplo de manera grafica los rangos de cobertura dependiendo de la ubicación del PA [27].

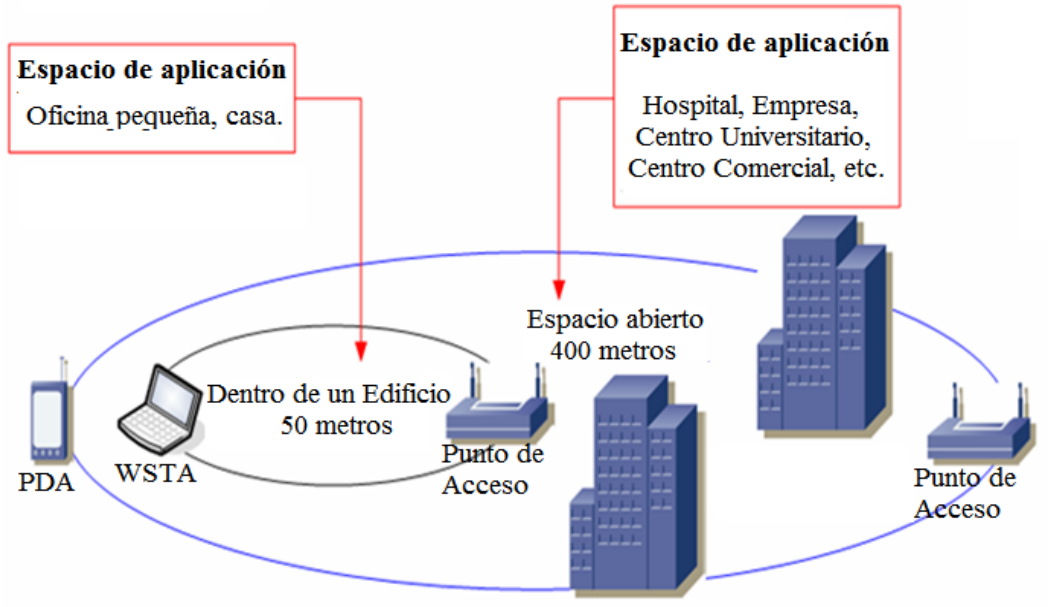

Figura 2.5: rango típico de cobertura de una WLAN [27]

La principal diferencia entre una LAN y una WLAN radica en que la primera requiere que los usuarios se conecten con sus dispositivos de cómputo a un Switch para que se encuentren comunicados o asociados a una determinada red de datos, en la segunda, no sólo se conecta equipo de cómputo sino que también admite otros dispositivos a la red ya sea mediante un PA o no [27].

2.5 Topologías de las WLAN

Las topologías de las WLAN constan de dos elementos clave, las WSTA y los PA. La comunicación puede realizarse directamente entre las WSTA o a través del PA. El intercambio de datos sólo es posible cuando existe una autenticación entre ambas terminales de datos. El mundo de la WLAN se rige principalmente por dos topologías [36, 5, 27]:

Modo Ad-Hoc (Red Autónoma Ad-Hoc): estas redes nacen bajo el concepto de autonomía e independencia, ya que no se requiere contar con algún tipo de infraestructura física pre existente, no opera bajo esquemas de control centralizado, su topología cambia de forma dinámica y de manera aleatoria, se conecta a los demás dispositivos de la red regularmente a través de múltiples saltos radioeléctricos. Los nodos que conformen una red Ad-Hoc operarán como dispositivos finales ya sea como emisores, receptores o enrutadores, funcionando en un ambiente colaborativo de conectividad.

Básicamente las redes en modo Ad-Hoc no tienen controlador central ni PA, están formadas por las WSTA y no tienen acceso a otras redes. Aun que para que este tipo de redes tenga salida a otras redes o acceso a Internet, una WSTA deberá actuar como Servidor Proxy, además de que deberá contar con dos interfaces de red. Las opciones de configuración de seguridad, nombre de red y canal de comunicación se configuran en la propia WSTA. Una vez que las WSTA pertenecen a la misma red, se transmiten los datos por el aire y los otros dispositivos reciben y reenvían la información. La configuración que forman las WSTA es el conjunto de servicio básico independiente (IBSS).

En resumen, este tipo de redes inalámbricas consisten en que los dispositivos inalámbricos se comunican directamente, mediante su tarjeta de red inalámbrica, teniendo como limitante la distancia de cobertura entre los dispositivos en la red. La **Figura 2.6** ilustra el esquema de la topología Ad-Hoc.

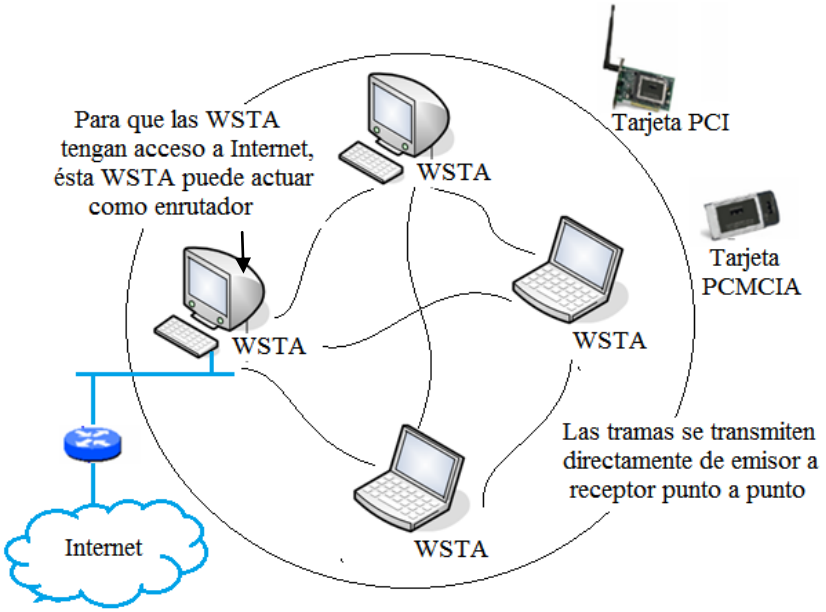

Figura 2.6: topología en modo AD HOC

Modo infraestructura (Topología en estrella): contrario al modo Ad-Hoc donde no hay un elemento central, en el modo de infraestructura existe un elemento de coordinación; un PA o estación base, dicho modo utiliza el concepto de celda ya usado en otros sistemas de comunicación inalámbrica como la telefonía móvil. En este caso, si el PA se conecta a una red cableada, las WSTA pueden acceder a la red fija a través del PA, para interconectar varios PA y WSTA todos los dispositivos deberán configurarse con el mismo ESSID, además para asegurar que se maximice la capacidad total de la red, es recomendable no utilizar el mismo canal en todos los PA que se encuentran dentro de su cobertura. En redes regidas por el estándar IEEE 802.11 el modo infraestructura es conocido como Conjunto de Servicios Básicos (BSS), o de igual manera conocido como Maestro y Cliente. La **Figura 2.7** ilustra el esquema de la topología en modo infraestructura [9, 4].

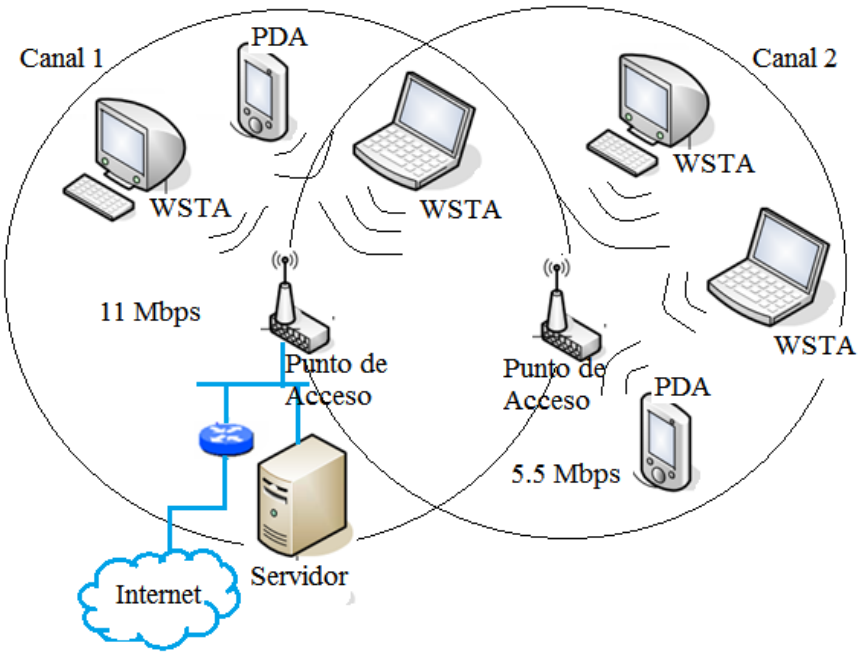

Figura 2.7: topología en modo infraestructura

Dentro de la topología en modo infraestructura, los PA pueden utilizarse de tres maneras diferentes, la primera como puerta de enlace (*Gateway*) para comunicar redes internas con externas o como puente (*bridge*) para unir varios PA y así extender los servicios/rangos de transmisión y como enrutador para unir diferentes WLAN dentro del área de cobertura del PA. Cada PA tiene teóricamente un límite de 64 WSTA que pueden estar conectadas hacia él, aunque este límite puede ampliarse colocando múltiples PA. También puede darse el caso de que una red esté formada por varios PA y WSTA que se conecten a ellos. A este grupo de PA y WSTA se le llama conjunto de servicio extendido o ESS [12].

2.6 Estándar IEEE 802.11

Las redes WLAN cumplen con los estándares genéricos aplicables al mundo de las LAN cableadas (IEEE 802.3) pero necesitan una normativa específica adicional que defina el uso y acceso de los recursos radioeléctricos. Estas normativas definen de forma detallada los protocolos de la capa física (PHY), la capa MAC y Control del Enlace de Datos (DLC) que regulan la conexión vía radio. El primer estándar de WLAN lo generó el organismo IEEE en 1997 y se denomina IEEE 802.11 [24].

Desde entonces varios organismos internacionales han desarrollado una amplia actividad en la estandarización de normativa de WLAN y han generado un abanico de nuevos estándares. En Estados Unidos, el auge de la actividad lo mantiene el organismo IEEE con los estándares IEEE 802.11 y sus variantes (b, g, a, e y h) y en Europa el organismo es el ETSI con sus actividades en *HiperLAN-BRAN*, de esta manera se puede diferenciar entre dos tipos de redes WLAN, las procedentes de la IEEE norteamericana y las procedentes de la ETSI europeas. En el año de 1990 se crea el comité IEEE 802.11 con el propósito de desarrollar un estándar, que definiera la forma de establecer comunicaciones para las redes libres de cables o bien redes inalámbricas, dicho estándar define el uso de los dos niveles más bajos del modelo OSI, es decir en las capas física y de enlace de datos, especificando sus normas de funcionamiento en una WLAN.

El estándar IEEE 802.11 original se ha modificado en numerosas ocasiones para optimizar el ancho de banda disponible o para especificar componentes de mejor manera, con el fin de garantizar mayor seguridad (IEEE 802.11i), calidad (IEEE 802.11e), etc., [20].

La capa enlace de datos del estándar IEEE 802.11 está compuesta por dos subcapas [25]:

- LLC. Capa que se ocupa del control del enlace lógico. Define cómo pueden acceder múltiples usuarios a la capa MAC.

- MAC. Conjunto de protocolos que controlan cómo los distintos dispositivos comparten el uso del espectro radioeléctrico. Es más compleja que las de otras especificaciones (IEEE 802.3, IEEE 802.5, etc.,). En WLAN se utiliza CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*).

Donde **CSMA/CA** es un protocolo de control de redes de bajo nivel que permite que múltiples WSTA utilicen un mismo medio de transmisión.

Utilizado, comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente información, de esta forma, el resto de dispositivos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio esta libre, se espera un tiempo adicional corto y aleatorio llamado DIFS (Espacio entre tramas), el tiempo que tarda en transmitir la trama después del DIFS se denomina ventana de contención, ésta se encuentra seccionada en tiempos de *Backoff* que dependen de la capa física, y solamente sí tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal (**Figura 2.8**) [21].

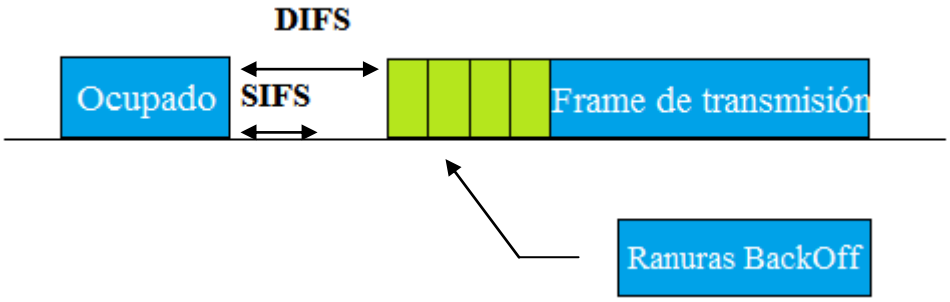

Figura 2.8: representación de los tiempos que intervienen en el mecanismo de acceso al medio CSMA/CA [21]

En la **Figura 2.9** se muestra el diagrama de flujo utilizado por el protocolo de control CSMA/CA en forma de diagrama de flujo.

Cuando se prepara para transmitir una trama, se escucha el canal, para saber si está libre; si lo está, se espera un IFS (*Interframe Space*) para realizar el intento de transmisión y si en ese momento no está libre el canal, se realiza otro reintento esperando un IFS y entonces se aplica el tiempo de *Backoff*. Es dicho diagrama hace uso del término ACK (*Acknowledgement*, en español notificación de recibo o asentimiento), donde este refiere a un mensaje que el destino de la comunicación envía al origen de ésta para confirmar la recepción de un mensaje [21].

Las redes inalámbricas se rigen hasta el momento principalmente por tres estándares IEEE 802.11b, IEEE 802.11a e IEEE 802.11g diferentes, descritos un poco más a detalle a continuación [25]:

IEEE 802.11b: en la práctica el estándar IEEE 802.11b, logra alcanzar velocidades entre 2 - 5 Mbps, dependiendo del número de usuarios, de la distancia entre emisor y receptor (entre la WSTA y el PA). Además de los obstáculos y de la interferencia causada por otros dispositivos de radiofrecuencia, dicho factor es uno de los más influyentes.

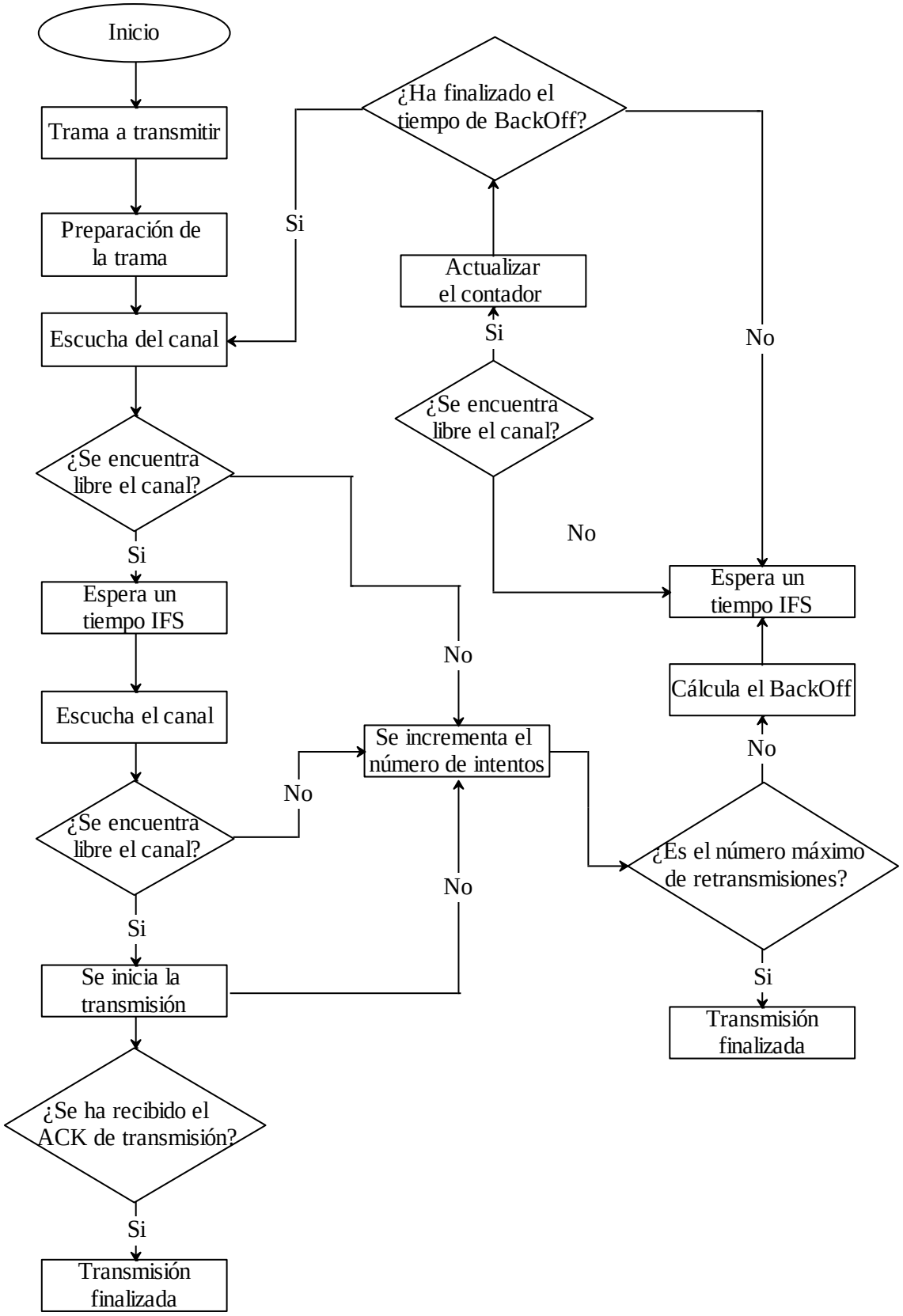

Figura 2.9: diagrama de flujo del funcionamiento del CSMA/CA [21]

Los dispositivos del estándar IEEE 802.11b operan en la banda de 2.4 GHz, en esta frecuencia se presentan interferencias de dispositivos como teléfonos móviles y hornos microondas. Con el estándar IEEE 802.11b las WLAN proporcionan un rendimiento comparable a una LAN Ethernet tradicional de la época, por lo cual la mayoría de las WLAN instaladas actualmente funcionan con arreglo a este estándar el cual es la base para la certificación Wi-Fi proporcionada por la WECA.

La certificación Wi-Fi posibilita que productos con esta certificación, puedan utilizarse conjuntamente aunque sean de distintos fabricantes. A pesar de sus problemas, el estándar IEEE 802.11b se ha convertido en el más popular [23].

IEEE 802.11a: en la actualidad ya se maneja también éste estándar, conocido como Wi-Fi 5, aprobado en 1999 utiliza el mismo juego de protocolos de base que el estándar original, con la intención de constituirla en la norma para redes inalámbricas de uso empresarial a diferencia del IEEE 802.11b que se enfocó hacia las redes caseras y para pequeños establecimientos. IEEE 802.11a ofrece velocidades de hasta 54 Mbps. En la práctica, se logran velocidades entre 22 Mbps, además de que opera en la banda de 5 GHz, tiene 12 canales sin solapa, 8 para red inalámbrica y 4 para conexiones punto a punto, este estándar disfruta de una operatividad con canales relativamente limpios. La banda de 5 GHz ha sido recientemente habilitada, además de que no existen otras tecnologías *(Bluetooth, microondas, ZigBee, WUSB)* que la estén utilizando, por lo que existen muy pocas interferencias. Por otro lado un inconveniente apreciable del estándar IEEE 802.11a es que no puede inter operar con dispositivos del estándar IEEE 802.11b, excepto si se dispone de dispositivos que implementen ambos estándares. Su alto precio, el hecho de que la banda de 5 GHz esté regulada en algunos países, y su menor cubrimiento ha hecho que los dispositivos IEEE 802.11a sean menos populares que los IEEE 802.11b, ya que su alcance es algo menor que el de los estándares que trabajan a 2.4 GHz (aproximadamente un 10%), debido a que la frecuencia es mayor (a mayor frecuencia, menor alcance) [3, 21].

IEEE 802.11g: en junio del año 2003, se ratificó un tercer estándar de modulación IEEE 802.11g, como la evolución del estándar IEEE 802.11b. Esta norma opera a una velocidad teórica máxima de 54 Mbps, que en promedio es de 22 Mbps de velocidad real de transferencia, similar a la velocidad del estándar IEEE 802.11a. Es compatible con el estándar IEEE 802.11b ya que utiliza las mismas frecuencias, sin embargo, en redes bajo el estándar IEEE 802.11g la presencia de nodos del estándar IEEE 802.11b reduce significativamente la velocidad de transmisión [23].

Los dispositivos diseñados para trabajar con el estándar IEEE 802.11g se introdujeron al mercado muy rápidamente, incluso antes de su ratificación, tal cual fue aprobada el 20 de junio de 2003. Esto debido en parte a que para construir dispositivos bajo este nuevo estándar se podían adaptar los ya diseñados para el estándar IEEE 802.11b. Actualmente se venden dispositivos con esta especificación, con potencias de hasta medio vatio, que permite hacer comunicaciones de hasta 50 km con antenas parabólicas o dispositivos de radio apropiados [2, 23].

En la **Tabla 2.1,** se muestra un resumen de las características de los principales estándares utilizados en las WLAN:

Tabla 2.1: comparativa entre versiones del estándar IEEE 802.11 [20]

	IEEE 802.11b	**IEEE 802.11a**	**IEEE 802.11g**
Popularidad	Muy utilizado	Poco utilizado	Muy utilizado
Velocidad	11 Mbps	54 Mbps	54 Mbps
Costo	Muy bajo	Elevado	Bajo
Frecuencia	2.4 GHz	5 GHz	2.4 GHz
Alcance	30-45 metros	7-23 metros	30-45 metros
Compatibilidad	IEEE 802.11g	N/A	IEEE 802.11b

2.6.1 Modelo de capas del Estándar IEEE 802.11

El estándar IEEE 802.11 cubre la capa física y la capa de enlace o MAC. En concreto el estándar define tres capas físicas diferentes, el espectro ensanchado por secuencia directa (DSSS), el espectro ensanchado por salto en frecuencia (FHSS) e infrarrojos. La capa de MAC es común para las tres capas físicas, proporcionado una interfaz única a los protocolos de capas superiores. MAC soporta funciones como la Fragmentación, Retransmisión y Aceptación de paquetes [24].

Capa física

La capa física de cualquier red define la modulación y la señalización características de la transmisión de datos. Esta capa se compone de dos subcapas, donde la primera de ellas es conocida como *PLCP* (*Physical Layer Convergence Protocol*), encargada de codificación y modulación y la segunda es *PMD* (*Physical Medium Dependence*) que crea la interfaz y controla la comunicación hacia la capa MAC (a través del *SPA: Service Access Point*) [25].

Capa de enlace (MAC)

Diseñar un protocolo de acceso al medio para las redes inalámbricas es mucho más complejo que hacerlo para redes cableadas, ya que deben tenerse en cuenta las dos topologías de una red inalámbrica. Además, se deben de tener en cuenta otros factores como las posibles interferencias, las variaciones en la potencia de la señal, las conexiones y desconexiones repentinas en la red, el roaming, los nodos móviles que van pasando de celda en celda, etc.,

A pesar de todo ello el estándar IEEE 802.11 define una única capa MAC (divida en dos subcapas) para todas las redes físicas, facilitando de este modo la fabricación en serie de chips. Esta capa controla el flujo de paquetes de comunicación entre dos o más puntos de una red, empleando el algoritmo CSMA/CA, donde es importante considerar aspectos como la exploración que consiste en el envío de tramas BEACON que incluyen los ESSID, también llamados SSID máximo de 32 caracteres; la autenticación, es decir, el proceso previo a la asociación, que le dará acceso a la red y sólo puede ser llevado a cabo una vez autenticado; la seguridad, la cual se proporciona el cifrado de los datos pero no de los encabezados; el modo ahorro de energía, ya que cuando está activado este modo, quiere decir que la WSTA envió previamente al PA una trama indicando hibernara , se debe tener en cuenta que por defecto este modo suele estar inactivo; y por último la fragmentación, es decir, la capacidad que tiene un PA de dividir la información en tramas más pequeñas. La **Figura 2.10** muestra de manera grafica como se lleva a cabo el modelo de capas.

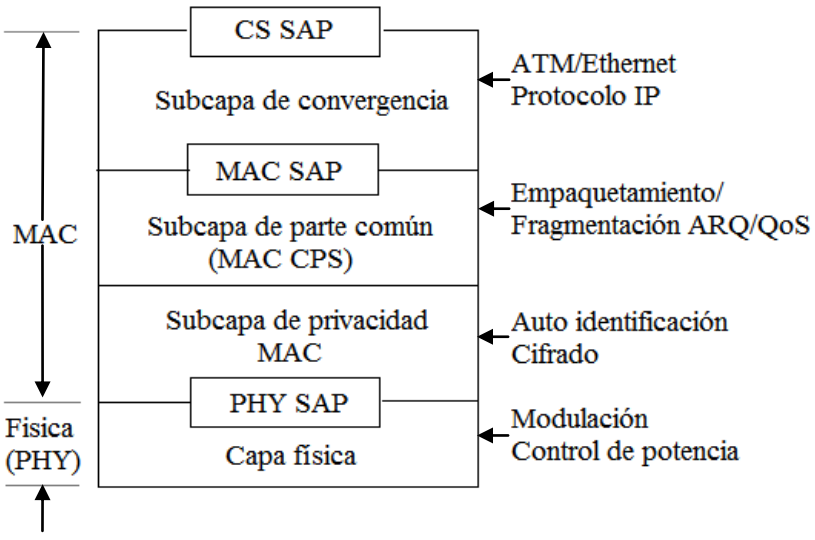

Figura 2.10: modelo de capas IEEE 802.11 [25]

2.7 Ventajas y Desventajas de las WLAN

Resulta sencillo comprender el atractivo que representa el uso de la tecnología Wi-Fi para las empresas de hoy en día. La adopción de una WLAN empezó a adquirir popularidad cuando pudo producirse una tecnología fiable, basada en estándares y de bajo costo que respondiera a la creciente demanda de formas más flexibles de conseguir mayor conectividad en el trabajo. Sin embargo, el rápido incremento en el uso de este sistema ha revelado una serie de vulnerabilidades serias en la primera generación de WLAN [28].

Ventajas

Las ventajas de esta tecnología se dividen en dos categorías, las empresariales esenciales y las operativas. Las primeras son aquellas que mejoran la productividad de los empleados, permiten que los procesos empresariales sean más rápidos y eficaces o posibilitan la aparición de dichos procesos totalmente nuevos. Las ventajas operativas están relacionadas con aspectos como la reducción de los costos administrativos o de los gastos de capital, etc., por tanto existen ventajas que se aprecian de manera clara como las que se presentan a continuación [28]:

Movilidad: los usuarios pueden acceder a archivos, recursos de la red, y a Internet sin la necesidad de tener ninguna conexión física a la red, por lo que los usuarios se pueden desplazar dentro del área de cobertura teniendo una alta velocidad de transferencia de datos, es decir dentro de la zona de cobertura de la red inalámbrica los nodos se podrán comunicar y no estarán atados a un cable para poder estar comunicados, esta característica provee al usuario de ciertos privilegios y comodidades [17, 27].

Poca planificación y costos reducidos de instalación: con respecto a las redes Ethernet, cabe mencionar que antes de cablear un edificio o unas oficinas se debe pensar mucho sobre la distribución física de las máquinas y cableado estructurado que contendrá dicha red, mientras que con una red inalámbrica sólo hay que preocuparse de que el edificio o las oficinas queden dentro del ámbito de cobertura de la red, en este caso sólo basta con que los dispositivos cuenten con una tarjeta de red inalámbrica y con una correcta configuración de la misma para que puedan establecer una comunicación exitosa con el PA o bien con los demás nodos que conforman la red [16].

Flexibilidad: éste beneficio se aprecia de mejor manera en las empresas que requieren de alto movimiento de usuarios ya que con mover la posición del PA cubren la zona en la que se mueven los usuarios, un ejemplo seria en las conferencias, salas de juntas, etc. [27].

Diseño: hoy en día los dispositivos que implementan la tecnología de redes inalámbricas (Wi-Fi, Bluetooth, etc.,) son muchos y variados, es por eso que una de sus principales características es que con el paso del tiempo estos dispositivos son de tamaño más pequeño y con esto se dice que se pueden integrar dentro de un dispositivo y fácilmente poder llevarlo en un bolsillo o bien ser portables totalmente [16].

Robusta y confiable: considera soluciones inalámbricas robustas que tienen alcances de hasta 100 metros. Estos sistemas les ofrecerán a los empleados de una compañía una considerable movilidad dentro sus instalaciones. Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el PA y las WSTA. Para garantizar una conectividad las velocidades más rápidas posibles incluyendo largo alcance o ambientes ruidosos, el usuario debe asegurarse que su nuevo sistema pueda hacer cambios dinámicos de velocidades, basándose en las diferentes intensidades de señal y distancias del PA. Además, el usuario debe seleccionar tarjetas de red inalámbricas para computadoras portátiles que ofrezcan antenas retractables para prevenir rupturas durante la movilización de los dispositivos [16].

Escalabilidad: un buen PA deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red. Las impresoras u otros dispositivos periféricos que no puedan conectarse en red tradicional, se conectan a su red inalámbrica con un adaptador USB inalámbrico o un *Ethernet Client Bridge*, además de que las topologías de red de la WLAN pueden ser fácilmente configuradas para una aplicación en especifico de acuerdo a las necesidades de la instalación, para escalar de una red pequeña de punto a punto a una red empresarial que permita roaming sobre un área de cobertura [17, 27].

Facilidad de uso: sí un usuario planea conectar múltiples PA inalámbricos a una red, debe considerar una solución que ofrezca conexiones automáticas a la red. Cuando un usuario se desplace fuera de los límites de un PA al campo de otro, debe existir una capacidad automática de conexión a la red, transferirá sus datos sin interrupciones al siguiente PA, aún al cruzar límites de los PA, sin siquiera tener que reconfigurar la dirección IP manualmente. Esto resulta ser especialmente útil para aquellas compañías con múltiples instalaciones que están conectadas por medio de una red de área amplia (WAN). Como resultado, los usuarios podrán movilizarse libremente dentro de sus instalaciones y más allá y permanecer conectados a la red [16].

Desventajas

A pesar de todas las ventajas ofrecidas, las WLAN presentan ciertos problemas de seguridad que han llevado a muchas empresas a evitar la adopción de esta tecnología, sobre todo en sectores particularmente sensibles a aspectos de seguridad, como el sector financiero y gubernamental. El riesgo que representa la difusión de datos de la red corporativa sin protección parece obvio; aun así, existen multitud de instalaciones de WLAN en funcionamiento, sin ningún tipo de seguridad activada. La mayoría de las empresas han implementado algún método de seguridad inalámbrica, sin embargo esta seguridad suele presentarse únicamente con las características básicas de primera generación, que no ofrecen la protección adecuada en consonancia con los estándares de hoy en día. En la actualidad existen diversas desventajas que se presentan por la implementación de redes inalámbricas sin una planificación adecuada, como las que se presentan a continuación [11, 12, 17, 26]:

Calidad de Servicio: las redes inalámbricas ofrecen menor calidad de servicio que las redes cableadas, se habla de velocidades que no superan habitualmente los 10 Mbps, esto frente a los 100 Mbps que puede alcanzar una red cableada. Por otra parte se debe tomar en cuenta la tasa de error debida a las interferencias existentes, la cual se puede situar alrededor de 10-4 frente a las 10-10 de las redes cableadas, esto significa que hay 6 órdenes de magnitud de diferencia y eso es mucho, se habla de 1 bit erróneo cada 10,000 bits o lo que es lo mismo, aproximadamente de cada Megabyte transmitido, 1 Kbit será erróneo. Por lo cual este tipo de redes pueden llegar a ser imposible de implantar en algunos entornos industriales con fuertes campos electromagnéticos y ciertos requisitos de calidad.

Soluciones Propietarias: debido a que la estandarización de los productos ha sido relativamente lenta, ciertos fabricantes han lanzado al mercado algunas soluciones propietarias que sólo funcionan en un entorno homogéneo, esto supone un gran problema ante el mantenimiento del sistema, tanto para ampliaciones del sistema, como para la recuperación ante posibles fallos. Tales aspectos implican que cualquier usuario que desee mantener su sistema funcionando se verá obligado a acudir de nuevo al mismo fabricante para comprar otra tarjeta, PA, etc.,

Restricciones: las redes inalámbricas operan en una sección del espectro radioeléctrico, es bien conocido que hoy día éste se encuentra muy saturado, además de que las redes deben acoplarse a las normas que existan dentro de cada país. Concretamente en Países tales como España, Francia y Japón, existen limitaciones en el ancho de banda a utilizar por parte de ciertos estándares.

Seguridad: éste aspecto en las redes inalámbricas es el de mayor relevancia, ya que en comparación con las redes alámbricas que proporcionan a los usuarios una buena seguridad y la

capacidad de transmitir grandes cantidades de datos de manera rápida y efectiva, además de ser más rápidas que las redes inalámbricas, es decir, en una red cableada es necesario tener acceso al medio que transmite la información, mientras que en la red inalámbrica el medio de transmisión es el aire, es por eso que son consideradas como altamente vulnerables. Al utilizar la difusión como medio de transmisión, la información puede llegar a cualquier estación que se encuentre dentro de esa cobertura, pertenezcan o no a la red, proporcionando un agujero dicha característica hace a las redes inalámbricas más susceptibles a sufrir ataques.

Capítulo 3

Wi-Fi

(*Wireless Fidelity*)

En este capítulo se presenta un análisis de la fidelidad inalámbrica mejor conocida como Wi-Fi, tecnología que surgió por la necesidad de establecer un mecanismo de conexión inalámbrica que fuese compatible entre los distintos dispositivos inalámbricos. El estándar IEEE 802.11 fue diseñado para sustituir el equivalente a la capa física y MAC del estándar IEEE 802.3 (Ethernet). Lo único en que se diferencia una red Wi-Fi de una red Ethernet es en cómo se transmiten los paquetes de datos, el resto es idéntico. Por tanto, cualquier aplicación LAN, sistema operativo o protocolo, incluido TCP/IP y *Novell Netware*, serán compatibles por igual en una WLAN como lo son en una LAN Ethernet [25,34].

3.1 Historia

Nokia, Symbol Technologies, 3Com, Cisco, Intersil y *Agere* fundaron en Agosto de 1999 una asociación conocida como WECA, ésto con la finalidad de impulsar y fomentar más fácilmente la comunicación inalámbrica regida bajo el estándar IEEE 802.11. Además de asegurar la compatibilidad de los dispositivos. En Abril del 2000, la WECA certifica la interoperabilidad de dispositivos según el estándar IEEE 802.11, bajo el nombre de Wi-Fi, por lo cual con dicha certificación el usuario posee la garantía que todos los dispositivos que contengan el logotipo Wi-Fi, pueden operar juntos sin problemas, independientemente del fabricante al que pertenezcan, por lo cual se puede obtener un listado completo de dispositivos que tienen la certificación Wi-Fi en la *Alliance certified products.* Desde entonces, *Intermec*, *Microsoft* e *Intel* han formado el comité de dirección de WECA [12, 21].

Wi-Fi es un certificado proporcionado por el consorcio industrial sin ánimo de lucro Alianza Wi-Fi, que asegura la interoperabilidad de los productos que implementan estándares Wi-Fi, además también es considerado como un conjunto de estándares para redes inalámbricas, basadas en IEEE 802.11 del Instituto de Ingenieros en Electricidad y Electrónica (IEEE). En algunas ocasiones se interpreta a Wi-Fi como un sistema libre de cables, que establece la transmisión de paquetes de datos sobre redes de dispositivos de tipo inalámbrico, además de que

dicha tecnología utiliza ondas de radio propagadas en el aire. La tecnología Wi-Fi fue creada para ser utilizada en redes locales inalámbricas, en la actualidad es frecuente se utilice para acceder a Internet.

Existen tres tipos de Wi-Fi, basado cada uno de ellos en un estándar IEEE 802.11; los estándares IEEE 802.11a, IEEE 802.11b y IEEE 802.11g, los dos últimos de éstos disfrutan de una aceptación internacional debido a que utilizan la banda de 2.4 GHz, la cual está disponible casi universalmente. No obstante, la tecnología inalámbrica *Bluetooth* también funciona a una frecuencia de 2.4 GHz por lo que puede presentar interferencias con la tecnología Wi-Fi. Sin embargo, en la versión 1.2 y mayores de *Bluetooth* se ha actualizado su especificación para que no haya interferencias en la utilización simultánea de ambas tecnologías [25,34].

3.2 Seguridad

Una de las debilidades normalmente atribuidas a las tecnologías inalámbricas, y más en concreto a la tecnología Wi-Fi, es la falta de seguridad. Esto refiere no tanto a la seguridad física si no a la seguridad de la información, su integridad y a la no accesibilidad a terceros. Hoy día se puede notar que un alto porcentaje de las redes inalámbricas son instaladas sin tomar en cuenta el aspecto de la seguridad. Así, convirtiéndose en redes completamente abiertas sin protección de la información, con lo cual se está poniendo en peligro la confidencialidad e integridad de los datos [25].

Un sistema seguro, debe definir requerimientos esenciales, considerando tres aspectos de la seguridad en la información:

1. Servicios de seguridad.
2. Mecanismos de autenticación.
3. Ataques a la seguridad.

La seguridad de una red Wi-Fi se compone principalmente tres elementos básicos [11]:

1. *Autenticación del usuario o del dispositivo que se asocia a la red de datos*. Este aspecto representa un grado relativamente alto de confianza en lo que respecta a intentos de conexión a la red.
2. *Autorización del usuario o del dispositivo para utilizar la WLAN*. Aspecto que permite el control de acceso a la red.
3. *Protección de la información transmitida en la red*. Con la finalidad de protegerse contra intercepciones y modificaciones no autorizadas.

Es evidente que se puede dar solución a los problemas de seguridad en este tipo de redes o al menos aumentar la misma. Existen diversas alternativas para proporcionar seguridad, su implementación depende del uso que se vaya a dar a la red (personal o empresarial). Además depende si se trata de una red ya existente o una nueva red. Otro aspecto relevante es el presupuesto del que se disponga para implementar dicha red, entre algunos otros factores. En la mayoría de las ocasiones las soluciones de seguridad se basan en protocolos de cifrado de datos para la tecnología Wi-Fi, permitiendo la autenticación y autorización de usuarios.

El cifrado de los protocolos WEP, WPA/WPA2, son los que se implementan de manera más frecuente en este tipo de redes. Dichos protocolos se encargan de cifrar la información que viaja a través de la red. Otra opción para garantizar aún más la seguridad de la información es hacer uso de IPSEC en el caso de las VPN, aun que lo más recomendable para las WLAN es utilizar el conjunto de estándares IEEE 802.1X-EAP (*Extensible Authentication Protocol*), ya que permite la autenticación y autorización de usuarios, él cual se analizara en el siguiente capítulo [12, 26].

Servicios de seguridad para WLAN: normalmente los ataques a éste tipo de redes, suelen provenir de nodos no autorizados, es decir de nodos instalados sin el conocimiento de los administradores de la red.
Por otro lado debido a las amenazas existentes y con el fin de poder enfrentarlas y/o prevenirlas, se especifican una lista de servicios de seguridad que garantizan la protección de los sistemas que tratan y transmiten la información, dicha seguridad abarca dos elementos importantes, el acceso a la red y la protección de la información [25].

Las redes inalámbricas basadas en el estándar IEEE 802.11, especifican los servicios que deben soportar las redes basadas en éste, los cuales son:

Autenticación: medida de seguridad diseñada para establecer la validez de una transmisión de los usuarios autorizados. Para el estándar IEEE 802.11 se utiliza la autenticación de sistema abierto o autenticación de llave compartida. Este servicio persigue que el origen de la comunicación sea correctamente identificada, dando completa seguridad que no es un nodo falso, es decir, antes de que un nodo pueda unirse a la red, debe establecer su identidad, para ello debe superar una serie de pruebas que permitan saber que quien se desea conectar es quien dice ser.

Confidencialidad: consiste en asegurar que la información no sea divulgada a personas, procesos o dispositivos no autorizados. El estándar IEEE 802.11 garantiza la confidencialidad a través del uso de técnicas de cifrado, ésta se puede aplicar a la totalidad de datos intercambiados

entre dispositivos autorizados, como también a sólo segmentos seleccionados de dichos datos [25].

Integridad: éste servicio asegura que los mensajes no son modificados durante su transmisión, de manera que siempre se pueda confiar en la información transmitida. Es decir, garantiza que la información pueda modificarse únicamente por los nodos autorizados. Dichas modificaciones abarcan la escritura, modificación, eliminación, creación y re-actuación de cualquiera de los mensajes en la transmisión [25].

Mecanismos de Autenticación en una WLAN: para que una WSTA pueda asociarse a un PA y lograr conseguir acceso total o parcial a la WLAN, debe de llevarse a cabo un proceso de autenticación, que se clasifica en dos principales tipos, definidos por el estándar IEEE 802.11 [20]:
Autenticación de Sistema Abierto: considerada como el protocolo de autenticación por defecto para el estándar IEEE 802.11b. Éste consiste en autenticar todas las peticiones de usuarios. Dicho proceso se lleva a cabo de la siguiente manera (**Figura 3.1**) [20]:

1. La WSTA que desea autenticarse ya sea con otra WSTA o directamente con el PA, envía una trama que contiene la identidad (ESSID) de esta WSTA emisora.

2. La estación receptora o bien el PA envía otra trama a la WSTA emisora, la cual indica si reconoció o no la identidad proporcionada por ella.

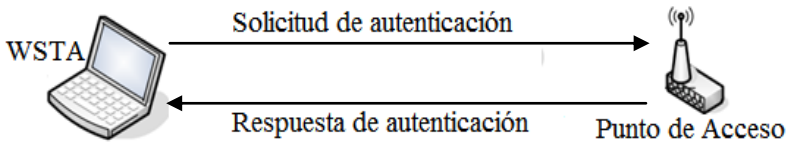

Figura 3.1: método de autenticación de sistema abierto

El ESSID es una cadena de 1 a 32 caracteres de longitud, que identifica a cada red inalámbrica, se emite en texto en claro dentro de las tramas *BEACON* de forma periódica, esto con la finalidad de anunciar la presencia de redes a las WSTA, dicha acción da lugar a un problema de seguridad para este tipo de redes, dado a que cualquier intruso podría obtener el ESSID, y así realizar un ataque de tipo pasivo (*sniffing*).

Autenticación de llave compartida: este mecanismo de autenticación consiste en determinar una llave secreta compartida entre la WSTA y el PA. Dicho proceso se lleva a cabo de la siguiente manera (**Figura 3.2)** [20]:

1. Cuando una WSTA trata de asociarse a un PA, éste responde con un texto aleatorio, que construye el desafío.
2. La WSTA debe utilizar la llave secreta compartida, para cifrar el texto de desafío y devolverlo al PA, con el fin de autenticarse.
3. El PA descifra la respuesta utilizando la misma llave compartida y compara con el texto de desafío enviado anteriormente.
4. Si los dos textos son idénticos, el PA envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la WSTA no dispone de una llave, o si envía una respuesta o llave incorrecta, el PA la rechaza, evitando que la estación acceda a los recursos de la red.

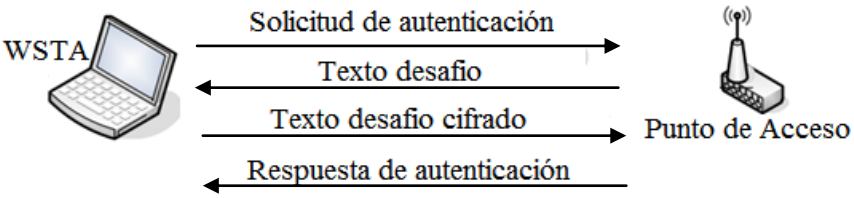

Figura 3.2: mecanismo de autenticación de llave compartida

Ataques

Un ataque es cualquier acción que compromete a la seguridad de la información perteneciente a alguna empresa, clasificándose como ataques pasivos y ataques activos [12, 26].

Retomando el tema de la difusión que maneja este tipo de redes resulta ser un problema ya que las señales llegan a todos los dispositivos que se encuentren dentro de la cobertura de la red. Sí bien se puede notar que normalmente las violaciones de seguridad de dichas redes suelen provenir de dispositivos no autorizados, la difusión por aire posee vulnerabilidades aprovechadas por intrusos, pudiendo lograr asociarse al PA y con esto hacer uso inapropiado de la red [10].

En la **Figura 3.3** se muestra un ejemplo de cómo puede presentarse un ataque. Cualquier persona desde el exterior, con el equipo y conocimientos necesarios puede lograr asociarse a un PA determinado. Con dicha acción el atacante tendrá acceso a la red, sus consecuencias serian algo tan simple como tener acceso a Internet mediante el PA al que logro asociarse, tener la posibilidad de un completo acceso a la información, emplear la red de la empresa como punto de ataque y después desconectarse para no ser detectado, robar software, tener acceso a la información que se transmite por la red, etc., con esto se deduce que una red mal configurada se convierte en una puerta trasera que vulnera por completo la seguridad informática [10].

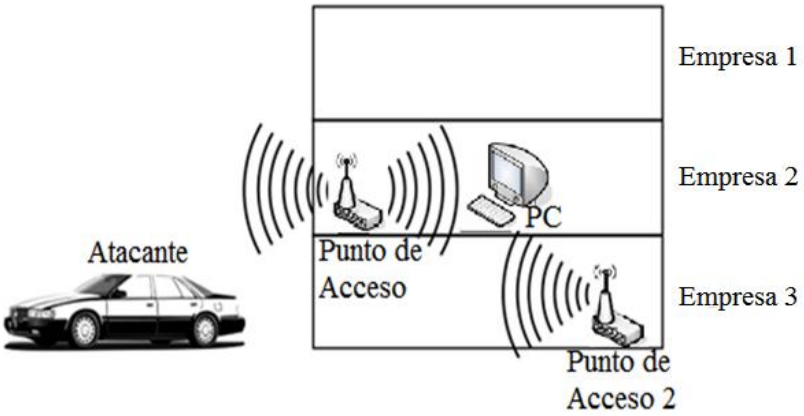

Figura 3.3: acceso no autorizado a la red inalámbrica [10]

Los ataques de tipo pasivo, no alteran la comunicación en la red, actúan únicamente como "escucha", además de que monitorizan en búsqueda de información que se esté transmitiendo. El propósito general de este tipo de ataques es lograr la intercepción de datos y el análisis del tráfico de la red, siendo ésta una técnica capaz de registrar situaciones como la posibilidad de leer los paquetes obtenidos con el monitoreo de la red (origen y destino) [25].

Por la función tan básica que tienen este tipo de ataques, no generan alteración en los datos que se están transmitiendo, por lo tanto son considerados como muy "difíciles" de detectar, sin embargo, se pueden combatir de manera adecuada con el cifrado de la información o con la implementación de otros mecanismos de seguridad, reduciendo así sus probabilidades de éxito a cifras casi nulas.

El tráfico de las redes inalámbricas puede espiarse con mucha más facilidad, en comparación con una red cableada. Un ejemplo práctico de ataques pasivos, es el ataque conocido como *sniffing* (escucha), donde basta con disponer de un dispositivo móvil con las características necesarias, para analizar el tráfico que no haya sido cifrado.

En el caso del análisis de tráfico, el atacante obtiene información por el simple hecho de examinar a éste y sus patrones, es decir, a qué hora se encienden ciertos dispositivos, cuánto tráfico envían, durante cuánto tiempo, etc., para realizar estadísticas con un determinado fin.

Por el contrario los ataques activos, implican algún tipo de modificación del flujo de datos transmitidos o la creación de un falso flujo de datos. Ataques que se clasifican en cuatro categorías [12, 25]:

1. *Usurpación de identidad:* caso que se presenta cuando el intruso o en sí una entidad finge ser otra, permitiendo a ésta acceder a una serie de recursos privilegiados usurpando a la entidad que posee esos privilegios. Generalmente se hace uso de un

sniffer para obtener varias direcciones MAC válidas en la red inalámbrica, además de que el análisis de tráfico proporciona información para realizar estadísticas. Otra forma consiste en instalar PA ilegítimos (*rogue*) para engañar a usuarios legítimos con la finalidad de que se conecten al este PA, en lugar de a uno legítimo.

2. *Re-actuación:* se da a menudo cuando uno o varios mensajes legítimos son capturados y repetidos en la red. Implica la captura pasiva de una unidad de datos y su retransmisión posterior para producir un efecto no autorizado, como por ejemplo depositar la misma cantidad monetaria varias veces en una cuenta bancaria específica.

3. *Modificación de mensajes:* para esta situación el atacante borra, manipula, añade o reordena los mensajes transmitidos. Consiste en alterar una porción del mensaje original o los mensajes legítimos se han retrasado o reordenado en su transmisión, con el fin de producir un efecto no autorizado. Por ejemplo, un mensaje que contenga una llamada a un procedimiento depositar_Dinero(CuentaA) podría ser alterado para decir depositar_Dinero(CuentaB) .

4. *Denegación del servicio (Dos):* ataque que inhibe el uso normal o la gestión de recursos informáticos y de comunicaciones, este ataque podría tener un objetivo específico. Un atacante puede provocar un ataque de denegación de servicio de varios modos. Por ejemplo el intruso filtrado podría descartar o suprimir todos los mensajes dirigidos a una determinada entidad y el servicio de comunicaciones de la red podría sufrir interrupción de las señales de radio, lo cual se puede conseguir utilizando algo tan simple como un microondas. No obstante existen ataques más complejos cuyo objetivo son los protocolos inalámbricos de nivel bajo, y otros menos complejos cuyo objetivo son las redes mediante un gran incremento del tráfico aleatorio, consistentes en paralizar temporalmente el servicio de un Servidor de correo, Web, FTP, etc., este tipo de ataques también poseen la capacidad de inundar la red con solicitudes de autenticación de usuarios legítimos, tramas para silenciar la red, etc. [28].

Dentro de las técnicas para realizar ataques pasivo o activos se encuentran dos prácticas conocidas para localizar redes inalámbricas, *warchalking y wardriving* descritos a continuación:

Warchalking: Método que hace referencia a la utilización de un lenguaje de símbolos para reflejar visualmente la infraestructura de una red inalámbrica y las características de algunos de sus elementos. Dichos símbolos suelen colocarse en las paredes de edificios situados en las zonas en las que existen redes inalámbricas, para indicar su condición y facilitar el acceso a las mismas. En sí, consiste en caminar por la calle con un dispositivo portátil dotado de una tarjeta inalámbrica, buscando la señal de algún PA. Cuando se encuentra uno, se marca sobre un área territorial la existencia de las redes inalámbricas, indicando la presencia del PA y si tiene o no

configurado algún tipo de seguridad. De tal modo que otras personas pueden conocer la localización de la red (**Figura 3.4**).

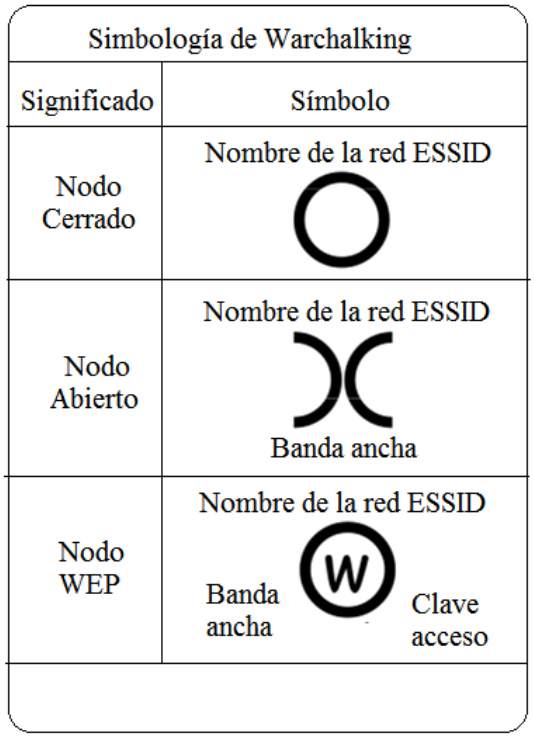

Figura 3.4: warchalking y su simbología

Wardriving: técnica que refiere a la acción de ir recorriendo una zona en busca de la existencia de WLAN y conseguir acceder a ellas. Requiere de un dispositivo portátil con una tarjeta inalámbrica, una antena adecuada, un GPS para localizar los PA en un mapa y un *software* especial que capture las tramas que difunden los PA (**Figura 3.5**).

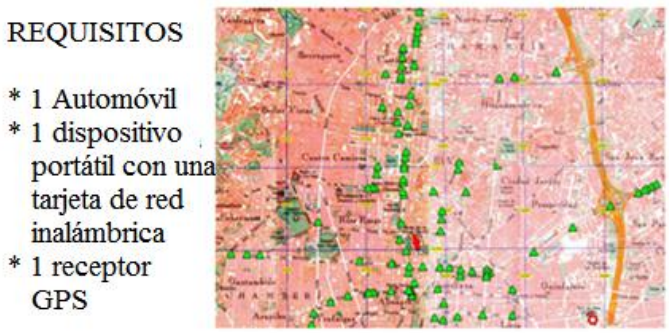

Figura 3.5: wardriving y sus requisitos

Los métodos de detección son una de las razones por las cuales las redes inalámbricas son consideradas como inseguras en comparación con las redes cableadas. Para que se pueda considerar una red inalámbrica como segura, deberá cumplir al menos con requisitos como que las ondas de radio deben confinarse tanto como sea posible, lo cual es difícil de lograr

totalmente, pero se puede hacer un buen trabajo empleando antenas direccionales y configurando adecuadamente la potencia de transmisión de los PA. Además que debe existir algún mecanismo de autenticación en doble vía que permita al cliente verificar que se está conectando a la red correcta, y a la red constatar que la WSTA está autorizado para acceder a ella. Para el caso de los datos deben viajar cifrados por el aire, con la finalidad de evitar que dispositivos ajenos a la red puedan capturar datos mediante escucha pasiva. La **Tabla 3.1,** presenta una descripción acerca de los algunos ataques existentes para las redes WLAN.

Los problemas de seguridad de las WLAN, sobre todo en lo que respecta al protocolo de seguridad WEP estática, han recibido mucha atención por parte de los medios de comunicación. A pesar de que existen efectivas soluciones de seguridad para hacer frente a estas amenazas, empresas de todos los tamaños se resisten a confiar plenamente en esta tecnología, hasta el punto de poner fin a su implementación o incluso prohibirla. Existen factores clave que han contribuido a la confusión y a la falsa idea de que la tecnología WLAN equivale a redes desprotegidas, tal es el caso de una falta de conocimientos sobre las tecnologías WLAN seguras y aquellas que no lo son. Tras el descubrimiento de una serie de errores en los protocolos de cifrado, las empresas desconfían de todas las medidas de seguridad de las WLAN, por lo cual la alarmante lista de estándares oficiales y soluciones propietarias que dicen solucionar los problemas, ha ayudado muy poco a aclarar la confusión. Otro aspecto importante es que la conexión inalámbrica es invisible, para los administradores de seguridad de la red, este hecho no es solamente perturbador, sino que representa un problema de administración de seguridad.

Para el caso de las LAN cableadas es posible ver a un atacante que intenta conectar un cable a la red, por el contrario la intrusión en una WLAN no se detecta tan fácilmente. Las defensas de seguridad físicas tradicionales de paredes y puertas utilizadas para proteger las redes cableadas no sirven de nada ante un intruso en entorno inalámbrico. En la actualidad se da mucho más importancia a la seguridad de la información, dado a que las empresas exigen niveles de seguridad superiores en sus sistemas y no confían en tecnologías que podrían introducir vulnerabilidades.

3.3 Herramientas criptográficas

Criptografía, del griego *kryptos*, es la disciplina que estudia las técnicas matemáticas relacionadas a la seguridad de la información que provee los servicios de confidencialidad, integridad de los datos, autenticación y no rechazo, así mismo esta ciencia busca garantizar que la información enviada sea autentica en doble sentido, es decir que la identidad del remitente sea verídica y que el del mensaje enviado no haya sido modificado durante su transmisión. Al hablar de criptografía debe de tomarse en cuenta principalmente dos aspectos [25]:

- *Criptología:* estudia los métodos matemáticos utilizados en el cifrado de la información.
- *Criptoanálisis:* estudia las técnicas para romper textos que hayan sido cifrados, con el fin de acceder a su información sin tener la llave.

Cuando se toca el tema de criptografía, se debe saber que el texto en claro consiste en la información que debe de ser protegida, es decir la información que se cifrará. El proceso de cifrado consiste en convertir el texto en claro en información ilegible denominada texto cifrado. La criptografía se divide en dos grandes grupos [25]:

- *Criptografía de llave simétrica:* emplea algoritmos de una única llave tanto en el proceso de cifrado como en el de descifrado, y son la base de los algoritmos de la criptografía clásica.
- *Criptografía asimétrica:* también llamada criptografía de llave pública, es una criptografía que se basa en utilizar dos llaves, una privada y una pública. Esta criptografía emplea problemas matemáticos fuertes como base para su seguridad. La seguridad de una criptografía de dos llaves depende de cuestiones matemáticas de manera que no se aplica a la criptografía de llave simétrica, y recíprocamente conectan el criptoanálisis con la investigación matemática en general de nuevas maneras, y son el principio de las técnicas de criptografía actuales.

El tipo de llave que se emplee para cifrar la información depende de las tareas a cumplir. Por un lado la criptografía de llave asimétrica posee dos principales ventajas, la primera de ellas es el hecho de eliminar el problema de transmisión segura de la llave, y la segunda consiste en permitir firmas electrónicas, sin embargo a pesar de dichas ventajas no reemplaza la criptografía de llave simétrica ya que ésta ultima presenta tiempos de cálculo más cortos, lo que representaría una ventaja para la este tipo de criptografía.

Según la forma en la que operan los algoritmos de cifrado o descifrado se clasifican en dos categorías: cifrado en flujo y cifrado por bloques, donde el primero se realiza bit a bit y están basados en la utilización de llaves muy largas que son utilizadas tanto para cifrar como para descifrar. Por lo contrario al anterior en el cifrado por bloques se descompone el mensaje en bloques de la misma longitud y cada bloque se va convirtiendo en un bloque del mensaje cifrado mediante una secuencia de operaciones.

A continuación se presenta una descripción general de las principales herramientas criptográficas utilizadas en las WLAN [25]:

Tabla 3.1: principales amenazas físicas para WLAN, extraído textualmente de [28]

Ataque	Descripción
Intercepción (revelación de datos)	La intercepción de datos transmitidos puede resultar en la revelación de datos confidenciales y de credenciales de usuario sin protección, además de la usurpación de la identidad. Permite también que usuarios malintencionados con cierto grado de sofisticación puedan recopilar información sobre su entorno de TI (tecnologías de la información) y la utilicen para atacar sistemas o datos que de otra forma, no serían vulnerables.
Imitación	El acceso fácil a la red interna permite a posibles atacantes falsificar datos aparentemente legítimos de modo que no sería posible hacerlo desde fuera de la red; por ejemplo, pueden imitarse mensajes de correo electrónico. Los usuarios, incluso los administradores de sistemas, suelen confiar en los elementos originados dentro de la red corporativa mucho más que en los procedentes del exterior
Carga libre (robo de recursos)	Es posible que el objetivo del intruso sea algo tan simple como el uso de su red como punto de libre acceso a Internet. Aunque este tipo de amenaza no es tan preocupante como las anteriores, la carga libre no sólo reducirá el nivel de servicio disponible para los usuarios legítimos, sino que podría dar lugar a la introducción de virus y otras amenazas
Amenazas accidentales	Algunas características de WLAN facilitan la incidencia de amenazas no intencionadas. Por ejemplo, un visitante autorizado podría iniciar su equipo portátil sin la intención de conectarse a la red pero la conexión a la WLAN de la compañía se produce de forma automática. Así, el equipo portátil del visitante se convierte en un punto de entrada de virus en la red. Este tipo de amenaza sólo se da en WLAN desprotegidas
WLAN falsas	Aunque su organización no disponga oficialmente de una WLAN, existe el riesgo de amenazas por parte de WLAN no administradas que pueden hacer su aparición en la red. Hoy día es posible comprar *hardware* de WLAN muy barato, con lo que pueden introducirse vulnerabilidades no intencionadas en la red

CRC (Control de redundancia cíclica): método matemático, normalmente empleado para la detección de errores en la transmisión de la información, se basa en la aplicación de un polinomio generador *G(x)* de grado *r*, y en el principio de que *n* bits de datos binarios se pueden considerar como los coeficientes de un polinomio de orden n-1. Por ejemplo, suponiendo los datos 10111, el polinomio generado sería:

$$x^4 + x^2 + x^1 + x^0$$

A estos bits de datos se le añaden *r* bits de redundancia de forma que el polinomio resultante sea divisible por el polinomio generador, sin generar un residuo. El receptor verificara si el polinomio recibido es divisible por *G(x)*, si no lo es, existirá un error en la transmisión.

Algoritmo de cifrado RC4: algoritmo diseñado por *Ron Rivest* en 1987 de la *RSA Security* (*Rivest, Shamir y Adelman*), su nombre completo es *Rivest Cipher 4*, teniendo el acrónimo RC un significado alternativo al de *Ron's Code* utilizado para los algoritmos de cifrado RC2, RC5 y RC6.

El algoritmo RC4 es el sistema de cifrado por flujo, donde el funcionamiento de este tipo de cifrado, radica en la expansión de una llave secreta (en el caso del protocolo WEP, un vector de inicialización (IV) público y una llave secreta) y una llave de amplia longitud de bits pseudoaleatorios (*keystream*) [30].

El sistema RC4 genera un flujo pseudoaleatorio de bits, que utiliza la operación lógica XOR para llevar a cabo el proceso de cifrado, el proceso de descifrado es exactamente el contrario. RC4 es un cifrador simétrico, es decir ambos extremos poseen la misma llave para cifrar y descifrar el mensaje y genera el mismo número de bytes cifrados que los existentes en el texto en claro. El principal motivo de utilizar este algoritmo de cifrado en los principales protocolos de seguridad, se debe a la simplicidad de cálculo en los procesos. Si las redes inalámbricas ya tienen que competir con los esfuerzos de una transmisión rápida, colisiones, acceso compartido al medio, etc., si se le añade un algoritmo de cifrado que ocupe mucho tiempo en calcularse o que genere un tamaño de texto cifrado mucho más grande, la comunicación sería muy lenta [30].

Algoritmo RSA: se trata de un algoritmo de cifrado asimétrico por bloques. Es un sistema criptográfico con llave pública que es distribuida, y otra llave privada, que está en la posesión del propietario. Antes de transmitir un mensaje, la estación emisora utiliza la llave pública de cifrado, la cual es entregada por el nodo receptor, la primera de éstas cifra el mensaje y lo transmite, una vez que dicho mensaje se entrega al nodo receptor, éste lo descifra con la llave privada que posee.

RSA utiliza mensajes que son representaciones de números y su forma de operación, está basada en el producto de dos números primos muy grandes (mayores a 768 bits) que son elegidos de forma aleatoria para formar la llave de descifrado, dicho algoritmo emplea

expresiones exponenciales en aritmética modular. Es seguro, debido a que con las computadoras actuales, no se conocen formas rápidas para factorizar un número grande en sus factores primos.

Los algoritmos descritos son los principalmente utilizados. Posteriormente se describirán los algoritmos de cifrado TKIP (*Temporary Key Integrity Protocol*), CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*) y MIC(*Message Integrity Check*) que se utilizan en protocolos de seguridad como WPA/WPA2, que son descritos en el próximo capítulo.

Capítulo 4
Protocolos de seguridad en las WLAN

Un protocolo de seguridad define las reglas que establecen las comunicaciones ya sean de telefonía, correo electrónico, radio, etc., o de dispositivos físicos como tarjetas de crédito, cédulas, etc., dichas reglas diseñadas con la finalidad de que el sistema sea resistente a ataques de carácter malicioso. Generalmente los protocolos de seguridad son diseñados bajo ciertas primicias con respecto a los riesgos existentes a los cuales el sistema se encuentra expuesto. En la actualidad existen diversos métodos para garantizar la seguridad de las WLAN. Normalmente se utilizan más a menudo las implementaciones de protocolos de cifrado para la seguridad de los datos.

Tales protocolos son especializados para transmitir información protegida desde la red, un ejemplo de ello son los protocolos WEP como parte del estándar IEEE 802.11, WPA como preámbulo del estándar IEEE 802.11i y finalmente WPA2 como parte del estándar IEEE 802.11i, todos ellos descritos en este capítulo.

4.1 Estándar IEEE 802.1X

IEEE 802.1X es el estándar definido por la IEEE para el control de acceso a la red basado en puertos. Éste permite la autenticación en una conexión punto a punto de dispositivos conectados a un puerto LAN. Dicho estándar es utilizado en algunos PA inalámbricos y se basa en el protocolo de autenticación extensible (EAP).

Un sistema basado en el estándar IEEE 802.1X define tres componentes para el proceso de autenticación (**Figura 4.1**) [33, 34]:

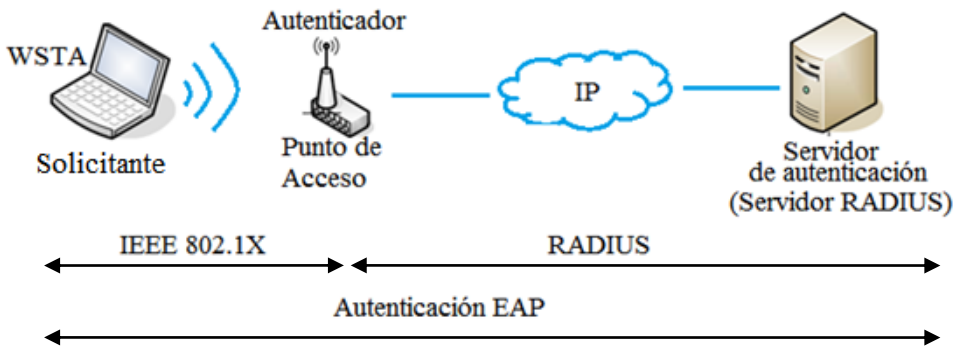

Figura 4.1: Diagrama general de autenticación IEEE 802.1X [34]

1. **Solicitante:** dispositivo del usuario final que busca el acceso a los recursos de la red.
2. **El autenticador:** en el caso de las WLAN se trata del PA, es el que recibe la conexión de la WSTA, y es considerado como el intermediario entre la WSTA y el Servidor RADIUS, solamente permite el acceso del usuario si el Servidor lo autoriza, es decir es el encargado de procesar realmente toda petición entrante.
3. **El Servidor de autenticación:** comprueba las credenciales del puerto solicitante remitida por él, al puerto autenticador y responde a este último con la aceptación o la denegación del acceso a los servicios de red. Existen dos tipos de Servidores de autenticación, *Servidor de autenticación integrado en el PA y Servidor de autenticación externo*, normalmente éste último suele tratarse de un Servidor RADIUS.

Es importante señalar que el Servidor RADIUS es considerado como la infraestructura recomendada por la Wi-Fi Alliance, como el sistema de gestión centralizada que brinda una solución de autenticación para entornos con un elevado número de usuarios, sin dejar de notar que este tipo de entornos utilizarán normalmente estructuras de LAN cableadas y WLAN. La utilización de este Servidor permite mejorar la capacidad de autenticación de la WSTA, proporcionando un nivel de seguridad superior, escalable y una gestión centralizada. A través de este sistema se puede obtener un certificado de cliente universal con la finalidad de permitir la autenticación mutua es decir permite la autenticación de la WSTA al PA y viceversa, además de permitir la gestión de llave protegida a través del soporte para RADIUS-EAP-TLS [10].

De manera general el proceso de autenticación se lleva a cabo entre el solicitante y el Servidor de autenticación, actuando el autenticador sólo como un puente y se utiliza el protocolo de autenticación EAP descrito a continuación.

4.2 EAP (*Extensible Authentication Protocol*)

EAP es un protocolo general de autenticación, autorización y contabilidad, compatible con varios métodos de autenticación, como la versión 5 de Kerberos, el protocolo de seguridad de la capa de transporte (*TLS, Transport Layer Security*) o el protocolo de Microsoft de autenticación por desafío mutuo (*MS-CHPA, Microsoft Challenge Handshake Authentication*).

En general, EAP es un protocolo de estructura, es decir, en lugar de especificar cómo se deben autenticar los usuarios, permite definir distintos métodos y sub protocolos que ejecuten la transición de la autenticación [28, 20].

El proceso de autenticación EAP se presenta de manera gráfica en la **Figura 4.2 [6]:**

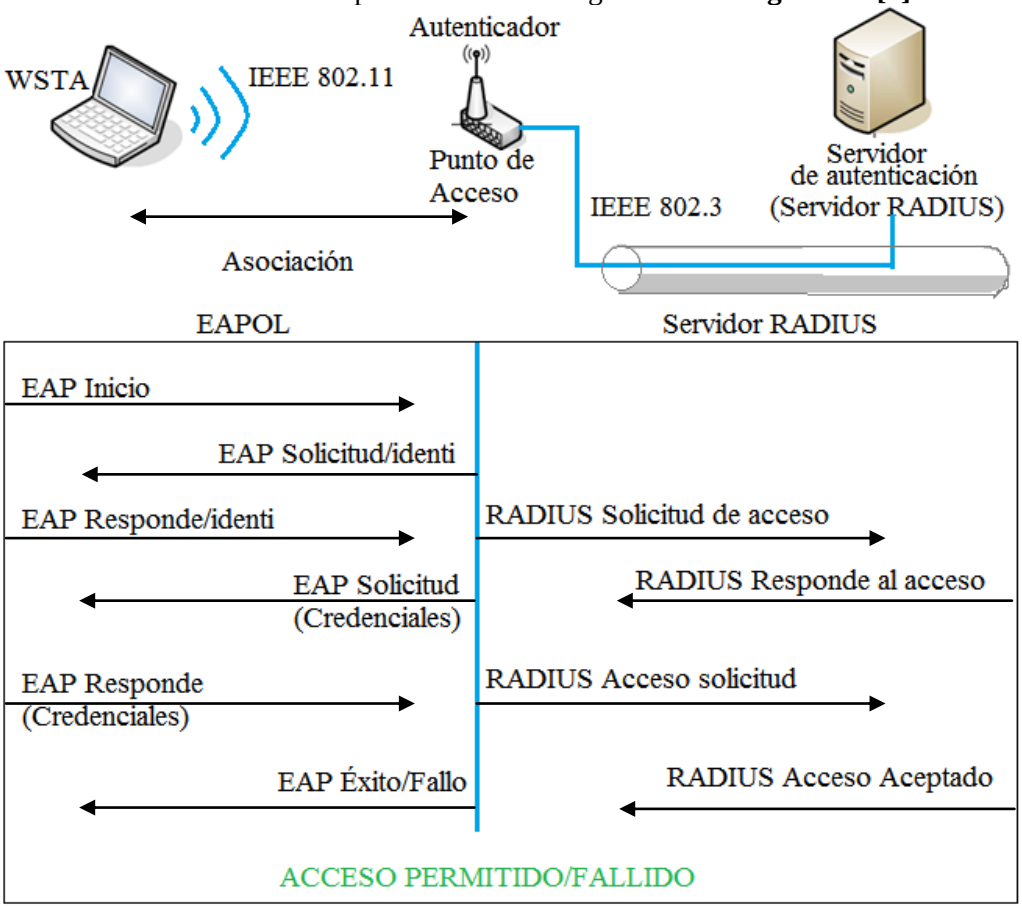

Figura 4.2: diálogo EAP-RADIUS

Para tener un mejor entendimiento del funcionamiento del protocolo EAP, a manera de ejemplo se presenta la siguiente explicación (extraído textualmente de [6]):

1. El cliente, que desea asociarse a la red, envía un mensaje de inicio de EAP que da lugar al proceso de autenticación. Por ejemplo, la persona que quiere acceder al banco pediría acceso al guardia de seguridad de la puerta.
2. El PA a la red respondería con una solicitud de autenticación EAP. En el ejemplo, el guardia de seguridad respondería solicitando el nombre y el apellido de la WSTA, así como su huella digital. Además, antes de preguntarle, el guardia de seguridad le diría una contraseña al cliente, para que éste sepa que realmente es un guardia de seguridad.
3. El cliente responde al PA con un mensaje EAP que contendrá los datos de autenticación. 'Nuestro cliente le daría el nombre y los apellidos al guardia de seguridad además de su huella digital.
4. El Servidor de autenticación verifica los datos suministrados por la WSTA mediante algoritmos, y otorga acceso a la red en caso de validarse. En este caso, el sistema del banco verificaría la huella digital, y el guardia validaría que correspondiese con la WSTA.
5. El PA suministra un mensaje EAP de aceptación o rechazo, dejando que la WSTA se conecte o rechazándolo. Nuestro guardia de seguridad le abrirá la puerta o no, en función de la verificación al cliente.
6. Una vez autentificado, el Servidor acepta al cliente, por lo que el PA establecerá el puerto de la WSTA en un estado autorizado. Nuestro cliente estará dentro del banco.

Los métodos de EAP principalmente utilizados con las WLAN son: LEAP (*Lightweight EAP*), EAP-TLS, TTLS (*Tunneled TLS*) y PEAP (*Protected EAP*) [28, 20].

Existen métodos EAP por contraseñas como LEAP, el cual utiliza un usuario y una contraseña para autenticar a los clientes, y soporta llaves WEP dinámicas (explicadas más adelante). A pesar de ser altamente utilizado, solamente funciona con *hardware* y *software* de Cisco, además exige que el Servidor RADIUS sea compatible con LEAP. Por otro lado, este método cuenta con varias vulnerabilidades en su seguridad, como el hecho de ser propenso a ataques de diccionario sin conexión y ataques de intermediario. LEAP únicamente puede llevar a cabo la autenticación del usuario y no del equipo, con la WLAN, por lo cual sin el proceso de autenticación de dispositivos, las directivas de grupo no se ejecutarán correctamente, pueden fallar los ajustes de instalación de *software*, los perfiles móviles y las secuencias de comandos de inicio de sesión, por tanto los usuarios no podrán cambiar las contraseñas caducadas [28].

En la actualidad se sabe de la existencia de diversas soluciones de seguridad para WLAN que hacen uso del protocolo IEEE 802.1X con otros métodos de EAP. Algunos de estos métodos, como EAP-MD5, utilizan nombre de usuario y contraseña para la autenticación.

El digesto de la contraseña producido por el algoritmo MD5 es transmitido, para proteger la contraseña original, pero este método no suministra un nivel de protección alto ya que puede sufrir ataques de diccionario, es decir, un atacante puede enviar varios digestos, de posibles contraseñas, hasta encontrar uno válido [28].

Por su parte, EAP-TLS es un estándar del IETF (*Internet Engineering Task Force*), que usa certificados de llaves públicas para autenticar los clientes y los Servidores mediante el establecimiento de una sesión TLS (una sesión TLS establece una conexión segura por medio de un canal cifrado entre el cliente y el Servidor) cifrada entre ellos. EAP-TTLS se trata de un protocolo de dos fases. Para este método el certificado únicamente se instala en el Servidor, por lo que permite la autenticación del Servidor por parte del cliente y en el caso de la autenticación por parte del Servidor se hace posteriormente a establecer una sesión TLS utilizando algún otro método EAP. En el caso de PEAP, se considera como un método de autenticación en doble fase, donde la primera de ellas consiste en establecer una sesión de TLS con el Servidor y permite que el cliente lleve a cabo la autenticación del Servidor, mediante el certificado digital de este mismo, para la segunda fase se requiere de un segundo método de EAP de túnel (EAP-TTLS), dentro de la sesión PEAP para llevar a cabo la autenticación del cliente con el Servidor [28].

4.2.1 Ventajas y desventajas

El hecho de hacer uso del protocolo EAP, deriva diversas ventajas las cuales se clasifican de la siguiente manera [3]:

- **Alto nivel de seguridad:** el protocolo proporciona un esquema de autenticación muy seguro, ya que puede utilizar certificados de cliente o nombres y contraseñas de usuario.
- **Cifrado más seguro:** permite el cifrado seguro de los datos de la red.
- **Transparencia:** proporciona transparencia en la autenticación y conexión con la WLAN.
- **Autenticación de usuarios y dispositivos:** permite el uso de métodos de autenticación independientes para los usuarios y los dispositivos del entorno. La autenticación de dispositivos independientes permite la administración de los dispositivos en el entorno aunque no se encuentren en uso por parte de los usuarios.
- **Rentabilidad:** bajo costo del *hardware* de red.
- **Alto rendimiento:** el cifrado se lleva a cabo en el *hardware* de WLAN en lugar de en la CPU del equipo cliente, de modo que el cifrado WLAN no influye de ningún modo en el rendimiento de este último.

Pero de igual manera la implementación de este protocolo trae consigo diversos inconvenientes o desventajas tales como [3]:

- **Interoperabilidad:** aunque este protocolo cuenta ya con una aceptación prácticamente internacional, el uso de métodos de EAP diferentes significa que el aspecto de interoperabilidad no puede garantizarse siempre.
- **Disponibilidad:** por ser compleja la configuración en lo que respecta a la seguridad de WLAN, muchas de las empresas no disponen del estándar.

La **Tabla 4.1** evalúa las posibles amenazas contra una solución basada en el protocolo IEEE 802.1X-EAP y protección de datos de WLAN (Extraído textualmente de [28]).

4.3 Protocolo WEP (*Wired Equivalent Privacy*)

El protocolo WEP es el mecanismo de cifrado básico opcional definido en el estándar IEEE 802.11. Su objetivo es proporcionar confidencialidad, autentificación y control de acceso en redes inalámbricas. Considerado como uno de los más débiles que hay en la actualidad, ya que no fue creado por expertos en seguridad o criptografía, pronto se demostró que es altamente vulnerable, siendo muy sencillo de romper su seguridad [24, 26].

WEP utiliza el algoritmo de cifrado RC4 para cifrar todos los datos que se intercambian entre las WSTA y el PA. En el año 2001 se publicó un artículo sobre WEP donde se mostraron las dos principales vulnerabilidades que presenta el algoritmo de cifrado RC4, es decir, la no-variación y los ataques al Vector de inicialización (IV) conocido, ambos ataques se basan en el hecho de que para ciertos valores de la llave es posible que los bits iniciales del flujo de la llave dependan de tan sólo unos pocos bits de la llave de cifrado. Como la llave de cifrado está compuesta concatenando la llave secreta con el *IV,* ciertos valores de este vector muestran llaves débiles. Estas vulnerabilidades fueron aprovechadas por herramientas de auditoría de redes como *AirSnort*, con la finalidad de que las llaves WEP fueran obtenidas analizando la suficiente cantidad de tráfico en la red. En un principio ésto resultó un problema ya que para poder obtener una llave, el tiempo requerido para el procesamiento de los datos era demasiado, por lo cual posteriormente *David Hulton* optimizó el método anterior, en este caso no sólo tomaba en cuenta el primer byte de la salida del algoritmo RC4, sino también de los siguientes bytes, con lo cual se logró una reducción considerable en la cantidad de análisis de trafico requerido para obtener la llave WEP [26].

Tabla 4.1: amenazas y soluciones del estándar IEEE 802.1X

Ataque	Mitigación
Intercepción (revelación de datos)	La asignación y modificación dinámicas de las llaves de cifrado con regularidad y el hecho de que las llaves sean exclusivas para cada sesión de usuario implica que no se pueden descubrir las llaves y el acceso a los datos de ninguna forma conocida (siempre y cuando la actualización de llaves se lleve a cabo con frecuencia)
Intercepción y modificación de datos transmitidos	Puesto que entre la WSTA y el PA se utiliza el cifrado mediante llaves dinámicas, ningún usuario malintencionado puede interceptar los datos y modificarlos. La autenticación mutua entre la WSTA, el Servidor RADIUS y el PA hace que sea muy difícil que un atacante pueda suplantar a alguno de ellos
Imitación	La autenticación segura en la red impide que usuarios no autorizados se conecten a la red e introduzcan datos falsos desde el interior
Denegación de servicio (DoS)	Pueden evitarse los ataques de exceso de datos, entre otros ataques de denegación de servicio, mediante el control de acceso a la WLAN con el protocolo IEEE 802.1X. No existe ningún modo de defensa contra ataques DoS de IEEE 802.11 de bajo nivel en WEP dinámica ni WPA. El estándar IEEE 802.11i se ocupará de esta cuestión. Sin embargo, este estándar tampoco será inmune a trastornos de la capa física (nivel de radio) de las redes
Carga libre (robo de recursos)	El requisito de autenticación segura impide el uso no autorizado de la red
Amenazas accidentales	El requisito de autenticación segura impide la conexión accidental a la WLAN
WLAN falsas	Si bien la solución IEEE 802.1X-EAP no se ocupa directamente de los PA falsos, la implementación de una solución inalámbrica segura como ésta elimina prácticamente los motivos para establecer una WLAN falsa. Sin embargo, debería considerar la creación y publicación de una directiva clara que prohíba el uso de WLAN no autorizadas

Un aspecto importante en la seguridad de redes inalámbricas es la integridad de los datos, WEP para garantizar la misma, se hace uso del algoritmo CRC32, algoritmo que se usa normalmente para la detección de errores, sin embargo debido a su linealidad nunca fue considerado como seguro desde el punto de vista criptográfico. Después de haber mostrado las principales vulnerabilidades del protocolo WEP, se consideró que dicho protocolo brinda un nivel de seguridad aceptable sólo para usuarios domésticos y aplicaciones básicas, sin embargo incluso

eso se desvaneció con la aparición de los ataques *KoreK* en 2004, y el ataque inductivo invertido *Arbaugh*, permitiendo que paquetes arbitrarios fueran descifrados sin necesidad de conocer la llave, utilizando la inyección de paquetes. Herramientas de auditoría de redes, como *Aircrack* de Christophe Devine ó *WEPLab* de José Ignacio Sánchez, ponen en práctica estos ataques y pueden extraer una llave WEP de 128 bits en menos de 10 minutos, esto dependiendo de los recursos de la red [26].

Posteriormente se dio la incorporación de la inyección de paquetes lo cual mejoró sustancialmente los tiempos de la obtención de la llave WEP, requiriendo tan sólo miles, en lugar de millones de paquetes con suficientes muestras de vectores de inicialización únicos, alrededor de 150,000 para una llave WEP de 64 bits y 500,000 para una llave de 128 bits. En la actualidad, WEP está completamente vulnerado y es considerado como obsoleto, sí bien ofrece una seguridad mayor que las WLAN desprotegidas o bien WLAN abiertas, este sistema conlleva serios inconvenientes de administración y seguridad, sobre todo para empresas de gran tamaño.

En la **Tabla 4.2** se muestra un cronograma de los ataques conocidos que ha sufrido el protocolo WEP.

Tabla 4.2: cronología de las vulnerabilidades en el protocolo WEP [26]

Fecha	Descripción
Septiembre 1995	Vulnerabilidad RC4 potencial (*Wagner*)
Octubre 2000	Primera publicación sobre las debilidades de WEP. Inseguro para cualquier tamaño de llave; Análisis de la encapsulación WEP (*Walker*)
Mayo 2001	Ataque contra WEP/WEP2 de *Arbaugh*
Julio 2001	Ataques CRC *bit flipping Intercepting Mobile Communications: The Insecurity of IEEE 802.11 (Borisov, Goldberg, Wagner)*
Agosto 2001	Ataques FMS(Fluhrer, Mantin, Shamir) – Debilidades en el algoritmo de programación de RC4, Publicación de *AirSnort*
Febrero 2002	Ataques FMS optimizados por h1kari
Agosto 2004	Ataques KoreK (IV únicos) – publicación de *chopchop* y *chopper*. Publicación de *Aircrack* (Devine) y WEPLab (Sánchez), poniendo en práctica los ataques *KoreK*

4.3.1 Funcionalidad

WEP opera a nivel enlace de datos (Subcapa MAC) del modelo OSI y es soportado por la gran mayoría de fabricantes de soluciones inalámbricas.

Se diseñó con el fin de proteger los datos que se transmiten en una WLAN mediante el cifrado de flujo simétrico (RC4). La llave secreta de flujo se obtiene de una llave estática de longitud variable de 64 bits, donde 24 de ellos forman parte del vector de inicialización IV. El IV se genera sin ningún patrón fijo y su finalidad es conseguir que el mismo texto en claro no vuelva a generar el mismo texto cifrado, por lo cual es recomendable cambiar su valor en cada trama y considerar que el destinatario lo necesita para descifrar la información [15, 24, 26].

La **Figura 4.3** muestra la arquitectura de una WLAN que cuenta con un mecanismo de seguridad basado en WEP, en un entorno corporativo.

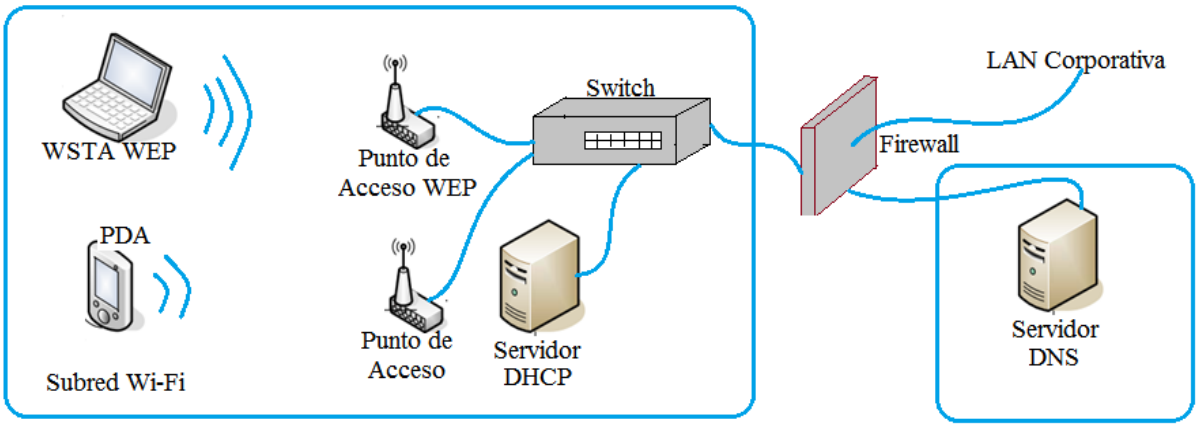

Figura 4.3: arquitectura de seguridad con WEP red corporativa [4]

El funcionamiento de WEP consiste en el proceso de cifrado que consiste en disfrazar los datos para ocultar la información que contienen. Recordando que, a los datos no cifrados se les denomina texto en claro, el texto disfrazado se le conoce como texto cifrado y al proceso de convertir el texto cifrado nuevamente en texto en claro, se le conoce como descifrado [35].

En la **Figura 4.4** se muestra de manera general el proceso de cifrado y descifrado en un canal de datos confidencial y que es utilizado por WEP.

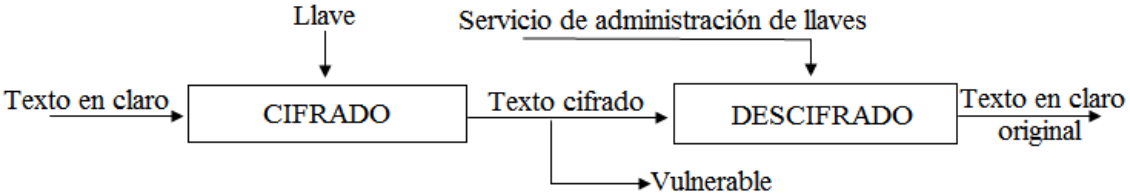

Figura 4.4: canal de datos confidencial [35]

El algoritmo RC4 consiste en generar una llave de forma pseudo-aleatoria que tiene la misma longitud que el texto original; utiliza un flujo de bits denominado, flujo de llave (*KEYSTREAM*) que se combina posteriormente con el mensaje para producir el texto cifrado. Para obtener el texto en claro, el receptor procesa el texto cifrado con un flujo de llave idéntico, además de que

utiliza la operación OR Exclusivo (XOR) para combinar el flujo de llave con el texto cifrado, la llave pseudo-aleatoria se genera utilizando una llave secreta que define el propio usuario con una longitud de 40 o 104 bits y un IV de 24 bits que lo genera aleatoriamente el sistema para cada trama. La llave secreta se concatena con el IV creado, lo que se conoce como semilla *(Seed)*, obteniendo la llave pseudo-aleatoria de 64 o 128 bits utilizando el algoritmo PRNG *(Pseudorandom Number Generator)*, el cual es un generador de números aleatorios que se rige bajo un conjunto de reglas utilizadas para extender la llave de flujo, con el fin de poder recuperar los datos. Ambas partes deben compartir la misma llave secreta y utilizar el mismo algoritmo para expandir la llave en una secuencia pseudo-aleatoria [35].

En teoría, WEP se puede utilizar con llaves de cualquier longitud, dado a que RC4 no requiere el uso de un determinado tamaño de la llave. La única longitud de llave presente en el estándar es una semilla WEP de 64 bits, de los cuáles 40 bits se comparten como secreto entre las dos estaciones que se están comunicando, más 24 bits del IV. La principal función del IV es cifrar con llaves diferentes para impedir que un atacante pueda capturar suficiente tráfico con la misma llave, y así obtener la llave WEP, como es lógico ambos extremos deben conocer tanto la llave secreta como también el IV [30, 35].

El proceso de cifrado comienza con una llave secreta que ha sido distribuida por un servicio de administración externa de llaves, como se mencionó anteriormente WEP es un algoritmo simétrico en el cual la misma llave es usada para cifrar y descifrar. WEP realiza el siguiente proceso para cifrar la información (**Figura 4.5**) [17]:

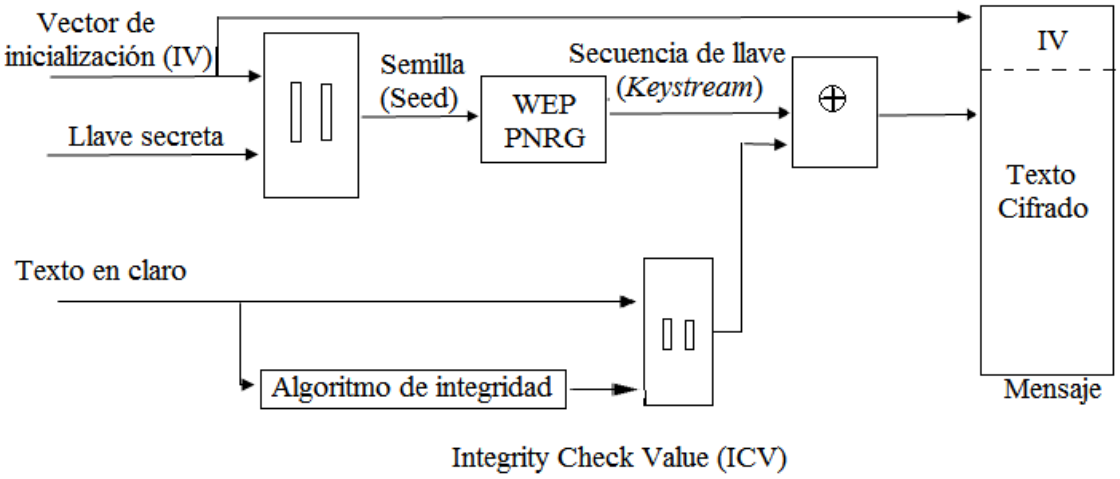

Figura 4.5: funcionamiento del algoritmo WEP en modalidad de cifrado [17]

1. Al texto en claro se le asigna un algoritmo de integridad conocido como ICV (*Integrity Check Value*) mediante el algoritmo CRC32, dicho algoritmo se concatena con la trama

(*texto en claro*) que posteriormente, es de utilidad para el receptor para comprobar si la trama ha sido alterada durante la transmisión.

2. Se establece una llave secreta compartida entre emisor y receptor con una longitud de 40 o de 128 bits.
3. Se concatena la llave secreta con un número aleatorio o bien con el IV de 24 bits, con lo cual se genera lo que se conoce como semilla. El IV debe cambiar con cada trama, ya que si se emplea siempre la misma llave secreta para cifrar todas las tramas, dos o más tramas iguales producirán tramas cifradas similares.
4. La semilla generada se emplea como entrada, de un generador de números pseudo-aleatorios (PRNG), RC4 genera una secuencia de caracteres pseudo-aleatorios (*keystream)* a partir de la semilla de la misma longitud que los bits obtenidos en el punto 1.
5. RC4 genera una cifra de flujo del mismo tamaño a la trama a cifrar de más de 32 bits con la finalidad de cubrir la longitud de la trama y el ICV.
6. Se realiza una operación XOR bit por bit de la trama con la secuencia de llave (El *KEYSTREAM* y el conjunto Mensaje+ICV, para así obtener como resultado la trama cifrada.
7. El IV y la trama se transmiten juntos.

Para el caso del descifrado de la información, el receptor es el encargado de dicho proceso, el cual se lleva a cabo de la siguiente manera (**Figura 4.6**) [17]:

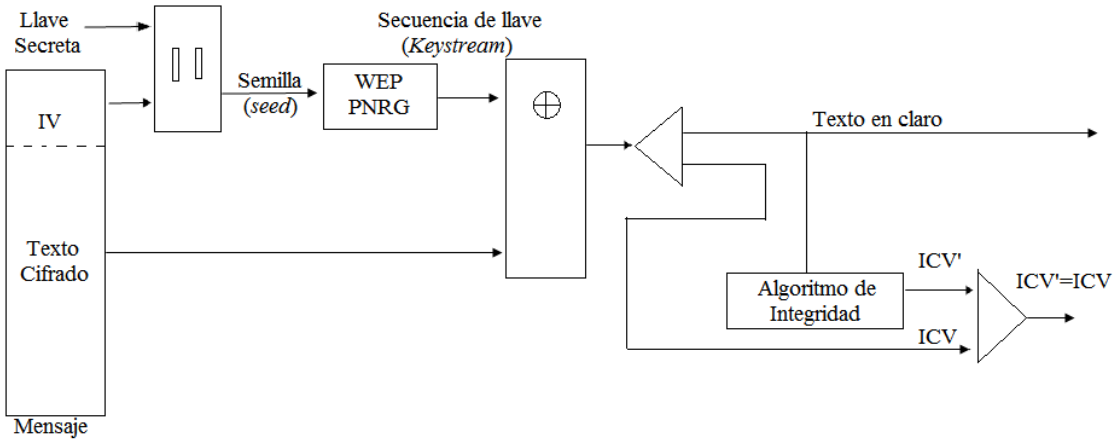

Figura 4.6: funcionamiento del algoritmo WEP en modalidad de descifrado [17]

1. Se concatena el IV recibido y la llave secreta compartida, con la finalidad de generar la semilla que se utilizó con el transmisor.

2. Un generador RC4 de números pseudoaleatorios (PRNG), produce la cifra de flujo a partir de la semilla. Si la semilla coincide con la empleada en la transmisión, la cifra de flujo también será indicada a la utilizada en la transmisión.
3. Se realiza una operación XOR bit por bit de la cifra de flujo y la trama cifrada, obteniéndose de esta manera el texto en claro y el ICV.
4. Al texto en claro se le aplica el algoritmo, CRC32 para obtener un segundo ICV (ICV') que se comparé con el recibido.
5. Sí los dos ICV son iguales, la trama se acepta; en caso contrario se rechaza.

Para comprender el funcionamiento de un código de flujo simétrico como RC4, se muestra el siguiente ejemplo, de una transmisión simplificada de datos. Se desea transmitir la siguiente trama entre dos estaciones inalámbricas (Ejemplo extraído textualmente de [18]):

0101 1000 1000 1110

Siendo la llave simétrica **0111**:

Asumiendo que el código del generador de números pseudoaleatorios implica la repetición secuencial de la llave secreta n veces hasta obtener una longitud igual a la del mensaje original, entonces el *KEYSTREAM* se obtiene al repetir cuatro veces la llave secreta (16/4 = 4 repeticiones), obteniendo:

***KEYSTREAM* = 0111 0111 0111 0111**

El proceso de transmisión y recepción del mensaje se puede ilustrar gráficamente como se muestra en la **Tabla 4.3:**

En la columna DATOS Tx se colocan los datos a transmitir (**0101 1000 1000 1110**). Aplicando XOR (DATOS Tx; KEYSTREAM) bit a bit como se muestra en la **Tabla 4.4**, se obtiene la columna FLUJO CIFRADO, que representa la trama cifrada a transmitir por el enlace inalámbrico [19].

El equipo receptor obtiene la trama cifrada y aplicando bit a bit XOR (FLUJO CIFRADO; *KEYSTREAM*) se obtiene el mensaje sin cifrar (texto en claro). Siempre se asumirá que el *KEYSTREAM* del equipo transmisor será igual al *KEYSTREAM* del receptor ya que RC4 es código de cifrado de flujo simétrico, lo que implica que la llave secreta debe ser compartida por ambas estaciones.

Tabla 4.3: transmisión y recepción del mensaje

TRANSMISOR		ENLACE	RECEPTOR	
Datos Tx	***Keystream***	**Flujo Cifrado**	***Keystream***	**Datos Rx**
0	0	0	0	0
1	1	0	1	1
0	1	1	1	0
1	1	0	1	1
1	0	1	0	1
0	1	1	1	0
0	1	1	1	0
0	1	1	1	0
1	0	1	0	1
0	1	1	1	0
0	1	1	1	0
0	1	1	1	0
1	0	1	0	1
1	1	0	1	1
1	1	0	1	1
0	1	1	1	0

Tabla 4.4: operación XOR

X	Y	XOR
0	0	**0**
0	1	**1**
1	0	**1**
1	1	**0**

Una vez descritas las formas en que se cifra y descifra la información en WEP el siguiente paso es describir el proceso de cómo se lleva a cabo la autenticación en este protocolo. Dicho proceso consiste en que cada cliente que desee asociarse a una determinada WLAN, debe ser autenticado, esto hace referencia al proceso por el cual el PA permite o deniega el acceso a los recursos de la red, es decir, antes de que una estación se asocie a la red debe de proporcionar unas credenciales válidas. WEP maneja dos tipos de autenticación (sistema abierto y autenticación mediante llave compartida), además de que este protocolo hace uso del procedimiento *four-way challenge-response handshake*, en el cual el usuario que desea

asociarse a la red debe superar un desafío que es emitido por el PA, en el que se transmiten 4 mensajes entre ambos nodos [1]:

1. La WSTA envía un mensaje al PA, solicitando la conexión.
2. El segundo mensaje corresponde a la respuesta que emite el PA, en la que se envía un texto generado aleatoriamente por él, y que corresponde a un desafío dirigido al solicitante.
3. La WSTA utiliza su llave para responder al desafío, que es emitido por el PA y éste envía un mensaje cifrado.
4. Por último el PA descifra el mensaje y lo compara con el original. Solo si ambos son iguales el solicitante pasa a ser parte de la red.

4.3.2 Variantes de WEP

Además de lo ya mencionado al tratar de resolver los inconvenientes del protocolo WEP, surgen algunas variantes de éste, la cuales se basan técnicamente en mejorar el problema con el IV, aumentando el tamaño de dicho vector, es por eso que surge la versión WEP2 que consiste en aumentar el tamaño del IV, y una protección de cifrado de 128 bits, en lugar de la de 64 bits. Sin embargo, se debe observar que la longitud del IV sigue siendo de 24 bits (las tramas IEEE 802.11 no contemplan un mayor número de bits para enviar el IV), por lo que lo único que se ha aumentado es la llave secreta de 40 bits a 104 bits. Debido a que la longitud del IV y su forma de utilizarlo no varían, las debilidades del IV pueden seguir siendo aprovechadas de la misma manera. WEP2 no resuelve los problemas de WEP [26].

Tratando de dar solución a los problemas del protocolo original, surge otra versión conocida como WEP+. Esta variante es un protocolo diseñado por la organización *Lucent Technologies*, su principal objetivo es la eliminación de los IV débiles, un punto importante de esta variante es que debe de utilizarse tanto en el emisor como en el receptor. Aunque, dada la situación de que es una tecnología propietaria no existen muchos fabricantes que lo integren y por tanto no presenta de una gran disponibilidad [26].

El estándar IEEE 802.11, no posee un mecanismo de distribución de llaves, para su uso con WEP. Existen dos estrategias para la gestión de llaves, donde la primera de ellas es ***WEP Estática,*** para este caso se hace uso de una sola llave para todas las WSTA que conforman la WLAN, durante un periodo de tiempo indefinido. Normalmente el periodo de vigencia de la llave es muy extenso, por lo cual la red no cuenta con el aspecto de seguridad, entonces no es recomendable esta estrategia. El punto más débil de WEP estática es que no existe ningún

mecanismo para asignar ni actualizar la llave de cifrado de red dinámicamente. Sin la utilización del protocolo IEEE 802.1X y EAP para implementar la actualización frecuente de la llave, el algoritmo de cifrado que utiliza WEP estática queda vulnerable a ataques de recuperación de llaves. La segunda estrategia es ***WEP Dinámica,*** donde cada WSTA hace uso de dos llaves; la de ASIGNACIÓN y la PREDETERMINADA, la primera de estas se comparte entre la WSTA y el PA, se utiliza para proteger las tramas UNIDIFUSIÓN. Por otro lado, la llave PREDETERMINADA se comparte por todas las WSTA, para así poder proteger las tramas de DIFUSIÓN y MULTIDIFUSIÓN. En este caso, se busca incorporar mecanismos de distribución automática de llaves y de autenticación de usuarios mediante IEEE 802.1X/EAP/RADIUS, tema que se abordará posteriormente [28, 20].

Dado lo anterior, se interpreta que WEP dinámica ofrece diversas ventajas sobre una WEP estática, ya que se reduce el ámbito de cada llave, dichas llaves son utilizadas con menor frecuencia, esta estrategia tiene por objetivo generar llaves WEP únicas para cada WSTA., además de que existe la posibilidad de cambiar las llaves estáticas, pero el proceso de modificación en las WSTA y el PA, resulta ser manual y laborioso. En el caso de que se opte por la solución WEP estática, las llaves deben actualizarse simultáneamente en las WSTA y los PA para conservar la conectividad de estas, en la práctica esto es tan difícil de conseguir que las llaves suelen dejarse sin cambiar permanentemente [19].

4.3.3 Ventajas y desventajas

A pesar de las deficiencias de seguridad que presenta WEP, en la actualidad es un hecho conocido que la implementación de este protocolo de cifrado es muy elevado, debido a diversas situaciones, sin descartar que este protocolo de seguridad presente diversas ventajas, así como desventajas.

Ventajas

Es mejor proteger la información con WEP antes de dejar la red completamente expuesta. Este protocolo presenta diversas ventajas como el hecho de que proporciona niveles de seguridad relativamente altos, sí se combina con otros mecanismos de seguridad como por ejemplo con el estándar IEEE 802.1X-EAP, la implementación de éstos y de otros métodos de autenticación y cifrado de datos garantizan que la seguridad en las WLAN sea proporcional o incluso mayor a la de las tecnologías LAN convencionales.

Otra ventaja apreciable es que hoy día es de los más empleados ya que viene como medida de seguridad básica en la mayoría de las tarjetas inalámbricas. Además, de que es compatible con la mayoría de los productos del estándar IEEE 802.11, éste modelo de autorización suele

complementarse con el filtrado de puertos, basado en direcciones de *hardware* de tarjeta de WLAN (Filtrado de direcciones MAC), aunque este proceso no forma parte de la seguridad IEEE 802.11 [17].

Desventajas

La vulnerabilidad de cualquier sistema criptográfico basado en un código de flujo, radica en la reutilización del flujo de llaves. Los principales problemas de WEP radican en su algoritmo de cifrado (RC4), ya que dicho algoritmo no implementa adecuadamente el IV, además por la corta longitud de este vector y la linealidad del algoritmo de verificación de la integridad (CRC32). La principal debilidad del algoritmo RC4 proviene del aprovechamiento de la operación XOR en el cifrado de la información, por ejemplo XOR (Texto claro) = XOR (Texto cifrado), por lo cual un atacante puede obtener la suficiente información cifrada con la misma llave. A pesar de que se pueden generar muchos vectores, la cantidad de información que pasa a través de un PA es muy grande, lo que hace que rápidamente se encuentren dos mensajes con el mismo IV, así que obteniendo los vectores que se utilizaron repetidamente, basta con aplicar técnicas relativamente simples de descifrado y la seguridad queda completamente vulnerada [1, 35].

La implementación del IV en el algoritmo RC4, conlleva varios problemas de seguridad. El IV es la forma que varía la llave (seed), para impedir que un posible atacante obtenga suficiente información cifrada con una misma llave. Sin embargo WEP no especifica cómo manejar el IV, lo ideal es que cambie en cada trama para mejorar la privacidad, pero WEP no obliga a ello, por lo cual los fabricantes definen esta cuestión de cómo variar el IV en sus productos [1, 35].

La forma en que WEP se protege del ataque mencionado es cambiando constantemente el IV, normalmente la forma en que cambia este vector es simplemente sumándole 1 cada vez que un nuevo paquete es transmitido, en sí este no es un defecto muy grande, sino que el problema radica en que después de 2^{24} el vector inevitablemente se va a repetir, dándose la condición que se desea para el ataque. La forma común en que se consiguen estos textos conocidos es inyectando tráfico al PA, de manera que éste responda y se pueda conseguir la información necesaria para conseguir la llave y así descifrar los mensajes transmitidos en la red, ésta situación da lugar a que WEP sea un sistema perfecto para romper por la fuerza bruta [1].

El protocolo WEP es vulnerable a los siguientes ataques [26]:

- Ataques pasivos basados en el análisis de paquetes para intentar descifrar el tráfico.
- Ataques activos basados en la introducción de paquetes.
- Ataques activos basados en el ataque/engaño al PA.

— Ataques de diccionario.

En resumen, se puede decir que en el caso de que se opte por implementar este mecanismo, se debe tomar en cuenta que utiliza una llave compartida para el control de acceso a la red, de igual manera esta llave sirve para cifrar la información que viaja de manera inalámbrica. WEP presenta serios inconvenientes de administración y seguridad de la información, es por esta razón que la implementación de éste, sería un grave error en empresas de gran tamaño, debido a que es considerado como un sistema simple de autorización. La mayor relevancia en este protocolo se debe a su sencillez, si bien ofrece mayor seguridad a las redes desprotegidas o bien redes abiertas. Además, el protocolo de seguridad original WEP, no posee un método para actualizar o distribuir la calve WEP, como se mencionó con anterioridad esta tarea se torna un tanto tediosa y complicada. Además, considerando que si se ha logrado un acceso no autorizado a una WLAN con WEP estática, resulta muy difícil restaurar la seguridad de misma [28].

4.4 Protocolo WPA (*Wi-Fi Protected Access*)

Cuando la seguridad de WEP quedó totalmente vulnerada, la IEEE declaró que resolvería el problema con el diseño de un nuevo estándar, el IEEE 802.11i. El desarrollo de dicho estándar se prolongó, trayendo como consecuencia que la venta de los dispositivos Wi-Fi, disminuyera considerablemente, lo que es lógico, sí no se posee la seguridad óptima para trabajar en una red inalámbrica. Después de un tiempo, la fecha de liberación del estándar IEEE 802.11i no se hacía oficial, así que la Wi-Fi Alliance decidió crear una versión basada en el estándar IEEE 802.11i, esto debido a la insistencia por parte de la industria de la liberación del estándar prometido. Wi-Fi Alliance determinó, entonces, que los avances de dicho estándar eran lo suficientemente sólidos y fue así como lanzó un borrador del estándar original. Así, nació el acceso protegido Wi-Fi mejor conocido como WPA, el protocolo que solucionaba los problemas de seguridad del protocolo WEP y era considerado como un puente entre el protocolo WEP y el estándar IEEE 802.11i (WPA2). Hoy en día IEEE 802.11i está completo y funcionando en plenitud [16, 30].

4.4.1 Funcionalidad

En realidad WPA es un subconjunto del estándar IEEE 802.11i, retomando ciertas piezas ya disponibles como IEEE 802.1X, para garantizar el proceso de autenticación de usuarios, además WPA utiliza, un mecanismo que retoma el CRC empleado por WEP y le añade otra capa de verificación que mejora la comprobación de la integridad de los datos enviados.

Con la intención de solucionar el problema de cifrado de los datos, WPA usa el protocolo TKIP, el cual cambia llaves dinámicamente a medida que el sistema es utilizado cada cierto tiempo, para evitar ataques que permitan revelar la llave. Así, WPA no elimina el proceso de cifrado de WEP, sólo lo fortalece con una llave de 128 bits y un IV de 48 bits, lo que reduce significativamente la reutilización del mismo y por tanto reduce la posibilidad de que un atacante obtenga suficiente información para romper la seguridad [16, 34].

WPA fue diseñado con el objetivo de operar en dos entornos diferentes. Modo personal (WPA-PSK) es utilizado en entornos domésticos o de pequeñas empresas. WPA-PSK (*Pre-Shared Key*, frase entre 8 y 63 caracteres), es empleado cuando no se dispone de un Servidor de autenticación en la red. Se requiere de la introducción de una contraseña compartida entre el PA y las WSTA, dicho intercambio genera una llave de cifrado para cada proceso de autenticación llamada PTK (*Pairwise Transient Key*). La llave PSK nunca se transmite por el aire ni se utiliza para cifrar el flujo de datos, simplemente, se usa iniciar el proceso de llaves dinámicas TKIP, por lo que es mucho más seguro que WEP [34].

Una vez que el cliente está autenticado, el protocolo TKIP utiliza 6 llaves de cifrado por cada sesión (4 de ellas para comunicaciones *unicast* y 2 para *broadcast*) que son generadas a partir de las direcciones MAC, ESSID y la PTK.

En el modo empresarial (*Enterprise mode*) se utilizan sofisticados mecanismos de autenticación, tal es el caso de la implementación de un Servidor de autenticación, que en la mayoría de las ocasiones se opta por un Servidor RADIUS, el cual permite a los usuarios ser identificados con nombre y contraseña o la posesión de un certificado digital, además de la distribución automatizada de llaves especiales, llamadas *máster keys*, a partir de las cuales se generan automáticamente las llaves de trabajo lo que hace que esta modalidad sea considerada como altamente segura. El PA emplea entonces IEEE 802.1X y EAP para la autenticación y el Servidor RADIUS suministra las llaves compartidas que se usarán para cifrar los datos [34].

La combinación de estas dos modalidades (**Tabla 4.5**) proporciona un cifrado dinámico y un proceso de autentificación mutuo. Así entonces, WPA involucra dos aspectos, un sistema de cifrado mediante TKIP y un proceso de autentificación mediante IEEE 802.1X [26].

Tabla 4.5: diferentes modos de WPA

Modalidad	**WPA**	
Empresarial	Autenticación:	IEEE 802.1X/EAP
	Cifrado:	TKIP/MIC
Personal	Autenticación:	PSK
	Cifrado:	TKIP/MIC

WPA utiliza algoritmos de cifrado similares a los utilizados por WEP, de modo que es posible implementar este estándar en *hardware* existente por medio de una simple actualización de firmware. Las principales características de WPA son la distribución dinámica de llaves, por lo cual la gestión dinámica de llaves aumenta notoriamente su nivel de seguridad, además, de la utilización más robusta del IV y nuevas técnicas de verificación de integridad y autenticación, dadas estas razones hipotéticamente se cree que WPA soluciona los problemas que presenta WEP [17]. La **Figura 4.7** muestra la arquitectura de una red WLAN que cuenta con un mecanismo de seguridad basado en WPA en un entorno corporativo (empresarial).

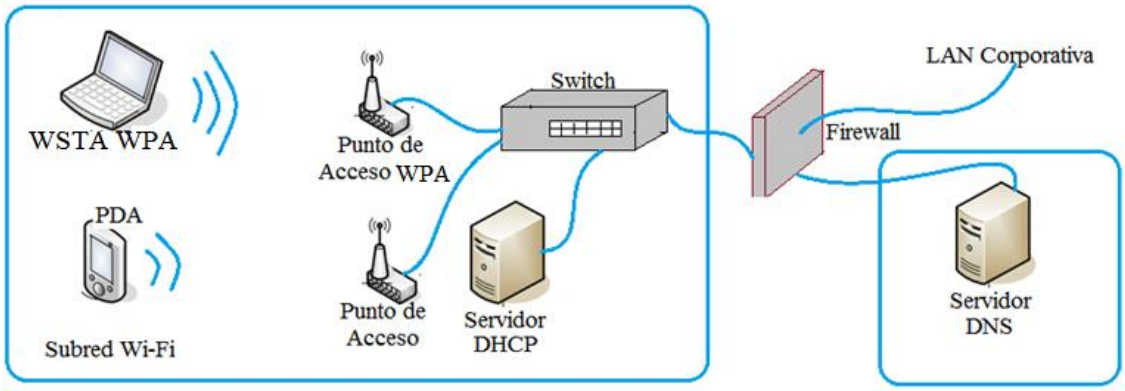

Figura 4.7: arquitectura de seguridad con WPA [4]

4.4.2 Ventajas y desventajas

El protocolo de seguridad WPA proporciona diversas ventajas ya que soluciona de manera total o parcial las vulnerabilidades que presenta su antecesor (WEP), además de que posee características que lo hacen más seguro, tales como la implementación de un Servidor de autenticación de usuario mediante el IEEE 802.1X (control de acceso a red basada en puertos), una llave de cifrado única para cada paquete, además de que soluciona la debilidad del IV de WEP mediante la inclusión de vectores del doble de longitud (48 bits) y especificando reglas de secuencia.

Los 48 bits permiten generar 2^{48} combinaciones de llaves diferentes, lo cual es un número suficientemente elevado como para tener duplicados. Incluye un valor de comprobación de integridad de mensaje firmado imposible de alterar o imitar. Utiliza el intercambio dinámico de llaves mediante el protocolo TKIP. Un contador de marcos cifrado incorporado para impedir ataques de reproducción. Establece nuevos protocolos para cambiar llave compartida entre AP y cliente cada cierto tiempo. Permite trabajar en dos modalidades personal o empresarial, entre otras situaciones [26].

Pero de igual manera este estándar no es del todo seguro y posee ciertos inconvenientes, como que no todas las tarjetas inalámbricas son compatibles con este estándar. Además de que el manejo de este protocolo aun no es altamente conocido. WPA se considera una solución provisional y no cumple la norma IEEE 802.11i.

4.5 Protocolo WPA2

El estándar IEEE 802.11i, fue creado por la Wi-Fi Alliance, asignándole el nombre comercial de WPA2. Publicado oficialmente el 24 de Junio de 2004, la creación de este estándar representa la corrección de una lista de vulnerabilidades existentes en su antecesor (WPA). La segunda versión del WPA, es considerada como una implementación temprana del estándar IEEE 802.11i, ya que no implementa todas las funcionalidades y procedimientos que establece dicho estándar, es común que se mencione a WPA2 como la versión certificada de IEEE 802.11i, a pesar de lo ya mencionado. Al igual que en el caso de su antecesor, por la normativa de la Wi-Fi Alliance, la autenticación por llave compartida es denominada WPA2-Personal (WPA2-PSK), mientras que la versión con autenticación por IEEE 802.1X/EAP es denominada WPA2-Enterprise [34].

Así, WPA2 es un sistema que se implementa para protección de redes inalámbricas que cumplen con el estándar IEEE 802.11 (Wi-Fi). WPA2 está actualmente disponible en los PA más modernos del mercado, no obstante WPA2 es compatible con WPA original, por lo cual algunos dispositivos WPA pueden ser actualizados a WPA2 por *software*, y algunos otros requieren de un cambio en el *hardware*, esto debido al alto nivel de procesamiento del cifrado requerido por WPA2.

4.5.1 Funcionalidad

Con la llegada del estándar IEEE 802.11i se dieron cambios elementales, como la separación de la autenticación de usuario de la integridad y privacidad de los mensajes, construyendo una arquitectura con estructura más robusta y escalable, que sirve igualmente para las redes locales domesticas como para los grandes entornos de red empresariales. Al estudiar más a fondo este protocolo, se puede notar que usa un número de estándares, protocolos y sistemas de cifrado, que ya están definidos fuera de IEEE 802.11i, una serie de normas también son definidas en su interior como, RADIUS, IEEE 802.1X/EAP, AES (*Advanced Encryption Standard*), RSN (*Robust Network security*), TKIP, etc., La **Tabla 4.6** muestra de manera más precisa de los elementos que requiere este protocolo de seguridad [19]:

Tabla 4.6: diferentes modos de WPA2 [26]

Modalidad	WPA2	
Empresarial	Autenticación:	IEEE 802.1X/EAP
	Cifrado:	CCMP(AES)/CBC-MAC
Personal	Autenticación:	PSK
	Cifrado:	CCMP(AES)/CBC-MAC

La principal diferencia existente entre WPA y WPA2, es que este último sustituye el cifrado RC4 por CCMP, que a su vez utiliza AES, tal como se muestra en la **Tabla 4.6.** AES es un cifrador simétrico por bloques (RC4 es por flujo), que tiene como características principales la longitud del bloque de entrada es de 128 bits y la longitud de la llave de 128,192, 256 bits, IV de 48 bits. Otro aspecto importante es que WPA2 requiere un *hardware* potente para realizar sus algoritmos, esto implica que dispositivos antiguos sin suficientes capacidades de procesamiento no pueden incorporar WPA2 a su seguridad. Es importante destacar que el protocolo de modo de contador con CBC-MAC (CCMP) es un protocolo de seguridad a nivel capa de enlace basado en AES, emplea un IV de 48 bits denominado PN (*Packet Number*) que en conjunto con otra información inicializa el algoritmo de cifrado AES. Tanto el cifrador como el cálculo del MIC emplean la misma llave temporal derivada de la autenticación IEEE 802.1X. En el caso del receptor, el proceso es idéntico, aunque hay que añadirle la verificación del MIC [34, 20].

RSN es denominada como la nueva arquitectura de las WLAN, ésta implementa una autenticación por medio de IEEE 802.1X y cifrado de datos a través del protocolo TKIP o CCMP, dicha arquitectura consiste en una distribución de llaves robustas y nuevas implementaciones de integridad y privacidad. RSN normalmente es utilizada para negociar que tipo de algoritmo de cifrado puede soportar una WSTA.

Al tener una arquitectura más compleja, RSN proporciona soluciones seguras y escalables para la comunicación inalámbrica. La redes que se rijan bajo esta arquitectura admitirán únicamente dispositivos operables con RSN, sin embargo, WPA2 define también una red de transición de seguridad TSN (*Transitional Security Network*), permitiendo la operatividad de sistemas bajo RSN y WEP [34,20].

Un elemento fundamental de WPA2, consiste en la habilidad para utilizar el protocolo EAP, ya que se determinó que este protocolo no especificaría un modo o tipo de autenticación, ya que permitiría poder realizar múltiples tipos de autenticación dentro de sí mismo, los cuales van desde llaves, tarjetas inteligentes, certificados, entre otros basados en el mismo método de petición (aceptar/rechazar). Para que EAP funcione adecuadamente, es decir que la transmisión

sea correcta entre las WSTA confiables y no confiables, es aquí donde entra la labor del estándar IEEE 802.1X, ya que este actúa como un Servidor fuerte de autenticación y administración de llaves [15].

Un elemento fundamental de WPA2, consiste en la habilidad para utilizar el protocolo EAP, ya que se determinó que este protocolo no especificaría un modo o tipo de autenticación, ya que permitiría poder realizar múltiples tipos de autenticación dentro de sí mismo, los cuales van desde llaves, tarjetas inteligentes, certificados, entre otros basados en el mismo método de petición (aceptar/rechazar). Para que EAP funcione adecuadamente, es decir que la transmisión sea correcta entre las WSTA confiables y no confiables, es aquí donde entra la labor del estándar IEEE 802.1X, ya que este actúa como un Servidor fuerte de autenticación y administración de llaves [15].

WPA2 se divide en dos categorías por lo cual necesita de una opción donde no se cuente con un Servidor de autenticación, es entonces que para el entorno personal se implementa el método de llave compartida (PSK) [15].

El establecimiento de un contexto seguro de comunicación que define *Guillaume Lehembre* para WPA consta de cuatro fases (**Figura 4.8**) [35]:

1. Acuerdo de la política de seguridad.
2. Autenticación IEEE 802.1X o llave PSK.
3. Derivación y distribución de las llaves.
4. Confidencialidad e integridad de los datos.

Fase 1: acuerdo sobre la política de Seguridad [25]: para iniciar la comunicación, es necesario que exista un acuerdo entre los participantes acerca de que política de seguridad que utilizarán. Las políticas de seguridad soportadas por el PA son mostradas en un mensaje *BEACON* o *PROBE RESPONSE*, posteriormente de un *PROBE REQUEST* de la WSTA. Dando continuidad a esto sigue una autenticación abierta, la respuesta de la WSTA se incluye en el mensaje *ASSOCIATION REQUEST* validado por una *ASSOCIATION RESPONSE* que emite el PA.

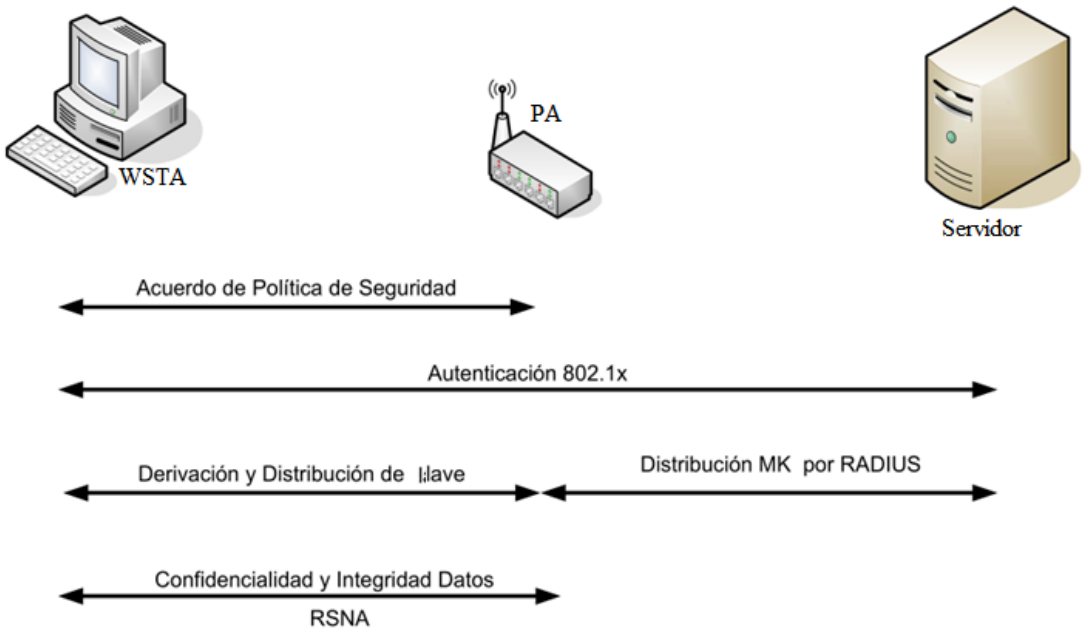

Figura 4.8: fases operacionales de WPA2 por *Guillaume Lehembre* [35]

La información sobre la política de seguridad se envía dentro del campo RSN IE (*Information Element*) conteniendo la siguiente información:

— Métodos de autenticación soportados por el PA (IEEE 802.1X, Pre-Shared Key (PSK)).

— Algoritmos criptográficos que aseguran el tráfico *unicast* (CCMP, TKIP, etc.,), donde estos pertenecen a una suite criptográfica basada en pares.

— Algoritmos criptográficos que aseguran el tráfico *multicast* (CCMP, TKIP, etc.,), en este caso una suite criptográfica de grupo.

— Soporte para la pre autenticación, que permite a los usuarios pre autenticarse antes de cambiar de PA en la misma red para un funcionamiento sin retrasos. La **Figura 4.9** ilustra esta primera fase.

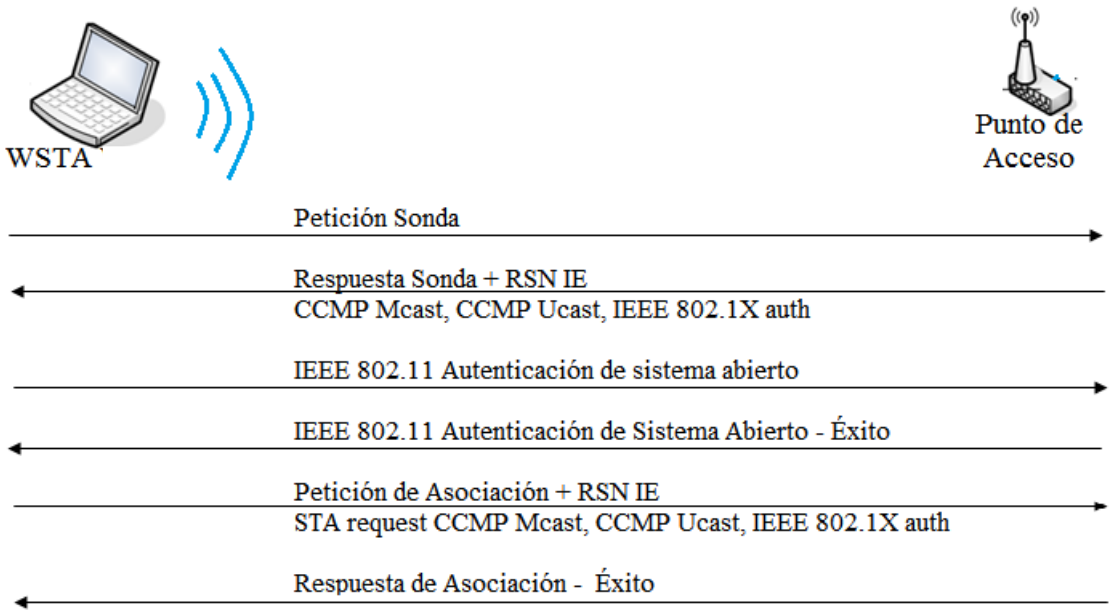

Figura 4.9: fase 1 acuerdo sobre política de seguridad [25].

Fase 2: autenticación

Autenticación mediante Servidor de autenticación (IEEE 802.1X): autenticación basada en EAP y en el método específico de autenticación elegido (EAP/TLS con certificados de cliente y Servidor, EAP/TTLS o PEAP). La autenticación mediante Servidor se inicia cuando el PA solicita los datos de identidad a la WSTA y esta responde al PA, incluyendo el método de autenticación elegido. Posteriormente se intercambian mensajes apropiados entre la WSTA y el Servidor de autenticación, para generar una llave maestra común (MK: *Master Key*). Para finalizar el proceso, se envía un mensaje de aceptación emitido por el Servidor (*RADIUS ACCEPT*) que contiene la llave maestra común, generada para la WSTA además de un mensaje *EAP Success* que le notifica de su autenticación exitosa. De manera grafica la **Figura 4.10** ilustra esta segunda fase [25].

Autenticación mediante llave compartida (WPA2-PSK): en este contexto, WPA2 se ejecuta en un modo especial conocido como PSK, el cual permite la utilización de llaves configuradas manualmente y facilitar así el proceso de configuración del usuario doméstico, donde este únicamente debe introducir una llave entre 8 a 63 caracteres (llave maestra) en el PA, así como en cada dispositivo que desee asociarse a la red. De esta forma sólo se permite acceso a aquellos dispositivos conocedores de la llave compartida [15].

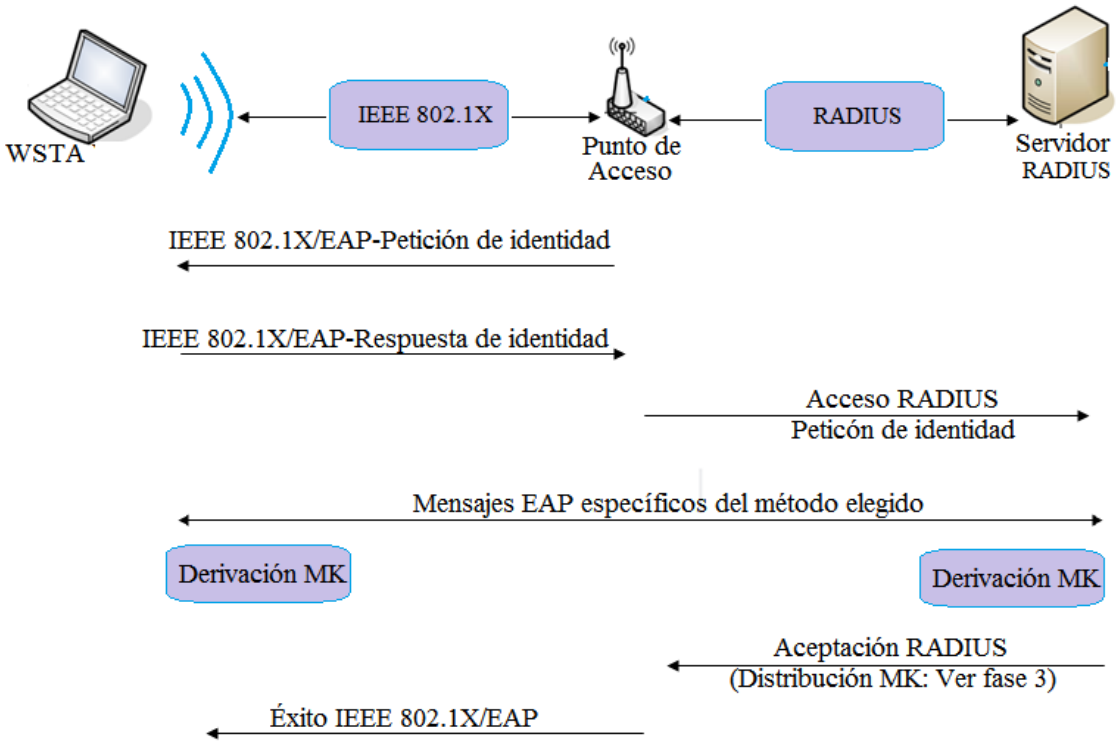

Figura 4.10: fase 2 autenticación mediante IEEE 802.1X [25]

La llave PSK es conocida por todas las WSTA del medio y el PA, está formada por una serie de valores dependientes del escenario, esta llave no es la cadena utilizada para cifrar los paquetes de datos, ni siquiera se utiliza como tal para la autenticación de la WSTA en el PA, sino que para ello se construye la llamada PMK (*Pairwise Master Key*) a partir de la PSK de acuerdo a la siguiente expresión:

PMK = PBKDF2 (Frase, ESSID length, 4096, 256)

PBKDF2 (*Password-Based Key Derivation Function 2*) método utilizado en PKCS#5(*Password-based Encryption Standard*), **ESSID length** refiere a la longitud del nombre de la red, **4096** es el número de *hashes* y **256** la longitud del resultado. Después de obtener la PMK se da paso a la fase de distribución de llaves [25].

Fase 3: jerarquía y distribución de llaves. La seguridad en la conexión depende directamente de las llaves. La arquitectura RSN garantiza la seguridad de la integridad al hacer uso de un arreglo de llaves que cuentan con un tiempo de vida finito organizadas según una jerarquía. Cuando se establece un contexto de seguridad tras la autenticación exitosa, se crean llaves temporales de sesión y se actualizan regularmente hasta que se cierra el contexto de seguridad. La tercera fase busca la generación e intercambio de las llaves, por lo cual la derivación de las mismas produce 2 *handshakes* (**Figura 4.11**):

1. Un 4-Way Handshake para la derivación de la PTK y la GTK (*Group Transient Key*).
2. Un Group Key Handshake, para la renovación de la GTK.

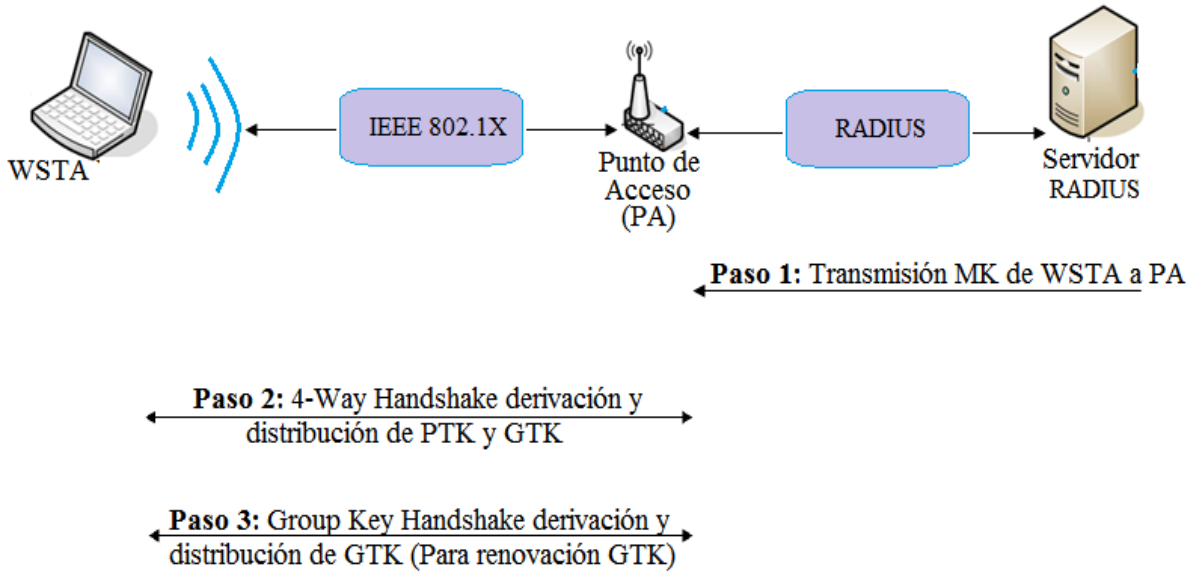

Figura 4.11: fase 3 derivación y distribución de llaves [25]

Con un 4-Way Handshake que se inicie desde el PA, permite [25]:

- La confirmación que la WSTA conoce la PMK.
- La derivación de una nueva PTK.
- La implementación del uso de llaves para el cifrado e integridad de los datos.
- La implementación de cifrado al transportar la GTK.
- La confirmación de la suite de cifrado.

Derivación de llaves

La derivación de la llave PMK depende del método de autenticación, es decir, si se opta por PSK, entonces PMK = PSK. La PSK es generada desde una contraseña (8 a 63 caracteres) o una cadena de 256 bits y proporciona una solución para redes domésticas o pequeñas empresas que no cuentan con un Servidor de autenticación, o sí se hace uso de un Servidor de autenticación, PMK se deriva de la MK de autenticación IEEE 802.1X.

La PMK nunca es utilizada en el proceso de cifrado de la información o la comprobación de la integridad, únicamente es utilizada para la generación de una llave de cifrado temporal, así entonces para el tráfico unicast esta actúa como la PTK, por otro lado su longitud depende directamente del algoritmo de cifrado (TKIP: 512 bits, CCMP: 384 bits). Entonces la PTK a su vez consta de diversas llaves temporales dedicadas [25]:

— **KCK (*Key Confirmation Key*).** Esta posee una longitud de 128 bits, los cuales actúan como llave de autenticación de mensajes (MIC), mientras surge el 4-Way Handshake y el Group Key Handshake.

— **KEK (*Key Encryption Key*)**. La función de esta llave es brindar seguridad en la confidencialidad de los datos transmitidos, en lo que se desarrolla el 4-Way Handshake y el Group Key Handshake, dicha llave tiene una longitud de 128 bits.

— **TK (*Temporary Key*).** Llave temporal que es utilizada para el cifrado de los datos transmitidos, algoritmos como TKIP o CCMP hacen uso de ésta, al igual que en las anteriores su longitud es de 128 bits.

— **TMK (*Temporary MIC Key*).** Esta llave es utilizada por ambas partes comunicantes, actuando esta como una llave dedicada, además de que es utilizada como llave para el proceso de autenticación de datos usada sólo por Michael con TKIP.

Como ya se mencionó la PMK se deriva a partir de la PSK, esta es producida a partir de una función pseudoaleatoria, ésta hace uso de una función *hash* criptográfica, en conjunto con una llave secreta (*HMAC-SHA1*), proceso que se aprecia de manera grafica en la **Figura 4.12** [15]:

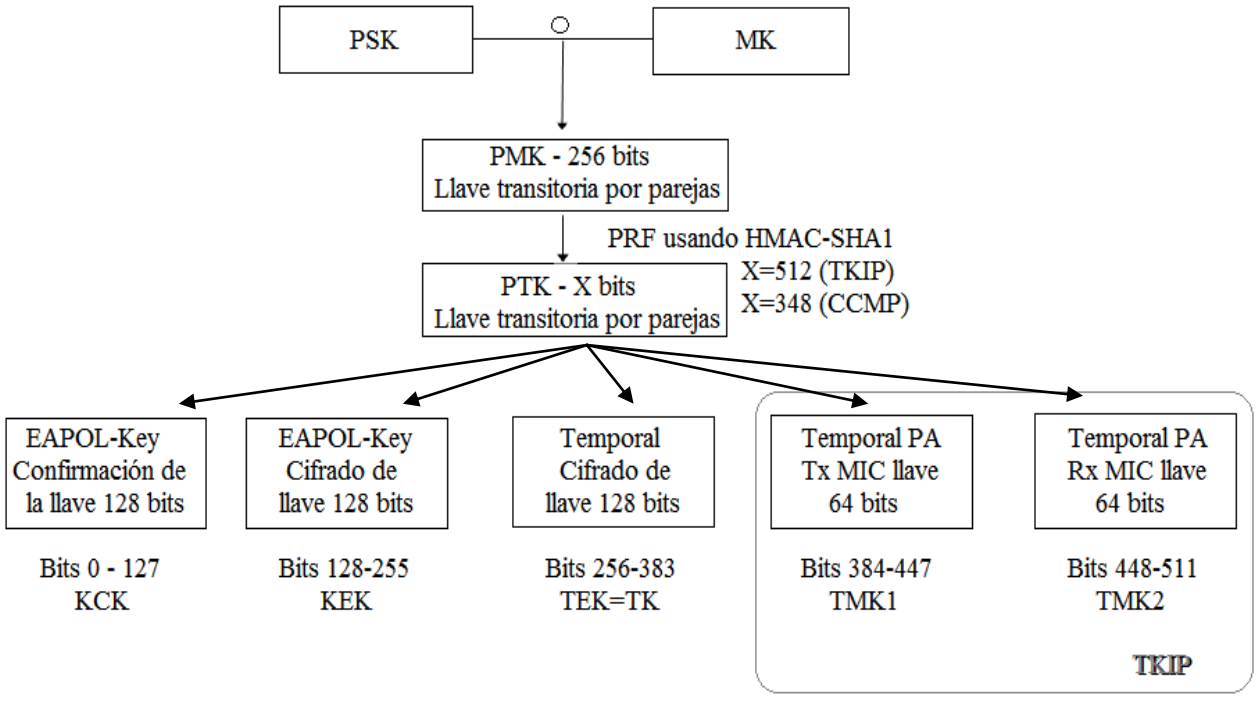

Figura 4.12: fase 3 jerarquía de llave por parejas [15]

Fase 4: confidencialidad e integridad de datos

Todas y cada una de las llaves generadas en las fases anteriores, son utilizadas en los protocolos que implementan la confidencialidad e integridad de los datos en las WLAN (TKIP, CCMP y WRPA (*Wireless Robust Authenticated Protocol*))[25].

Existe un concepto importante que debe ser entendido antes de detallar estos protocolos, la diferencia entre MSDU (*MAC Service Data Unit*) y MPDU (*MAC Protocol Data Unit*), ya que ambos términos se refieren a un sólo paquete de datos, pero MSDU representa a los datos antes de la fragmentación, mientras las MPDU son múltiples unidades de datos posteriores a la fragmentación [15].

TKIP está basada en el algoritmo de cifrado RC4. El esquema de la mezcla de llave TKIP, se divide en dos procesos él primero de ellos encargado de los datos estáticos, de la llave TEK de sesión secreta, dirección MAC del transmisor y los 32 bits más altos del IV. Para el segundo proceso se incluye el resultado de la fase 1 y los 16 bits más bajos del IV, cambiando todos los bits del campo *Per Packet Key* para cada nuevo IV. El IV siempre se inicializa en 0 y se incrementa de uno en uno para cada paquete enviado, y los mensajes cuyo contador de repetición no es mayor que el último mensaje, son rechazados. El resultado del segundo proceso y parte del IV extendido, componen la entrada para RC4, el flujo generado se une con el MPDU de sólo texto, el MIC calculado del MPDU y el viejo ICV de WEP. Cabe mencionar que las MPDU son distintas unidades de datos después de la fragmentación. Todo este proceso se resume en la **Figura 4.13** [15].

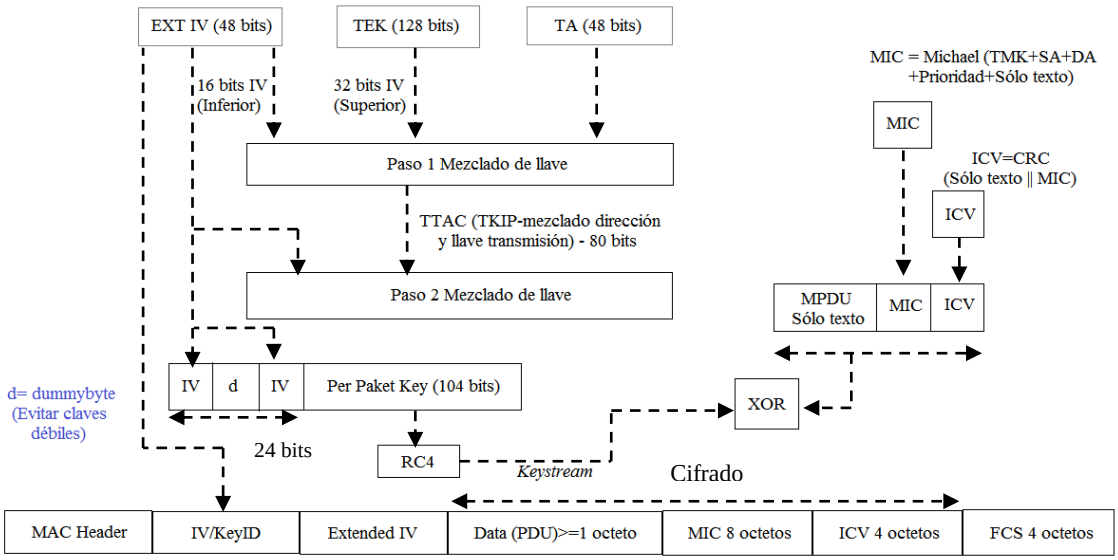

Figura 4.13: fase 4 esquema y cifrado de TKIP *Key Mixing* [25]

CCMP se basa en la suite de cifrado de bloques AES en su modo de operación CCM, el cual se crea mediante la combinación del CTR (*Counter Mode*), que garantiza la confidencialidad en conjunto con un método de autenticación de mensajes, CBC-MAC (*Cipher Block changing*), para poder introducir un MIC, CCMP agrega 16 bytes al MPDU, 8 bytes para el encabezado CCMP y 8 bytes más para el MIC. El encabezamiento CCMP es un campo no cifrado incluido entre el encabezado MAC y los datos cifrados, que incluyendo el PN (*Packet Number = IV Extendido*) de 48 bits y el Group KeyID. El PN se incrementa de uno en uno para cada MPDU siguiente [15].

El cálculo de MIC utiliza el algoritmo CBC-MAC que cifra un bloque Nonce de inicio y realiza operaciones XOR sobre los bloques siguientes para obtener un MIC final de 64 bits. El MIC entonces se añade a los datos de texto para el cifrado mediante AES en modo contador. El contador se construye con un Nonce similar al del MIC, pero con un campo de contador extra inicializado a 1 e incrementa para cada bloque (**Figura 4.14) [15]:**

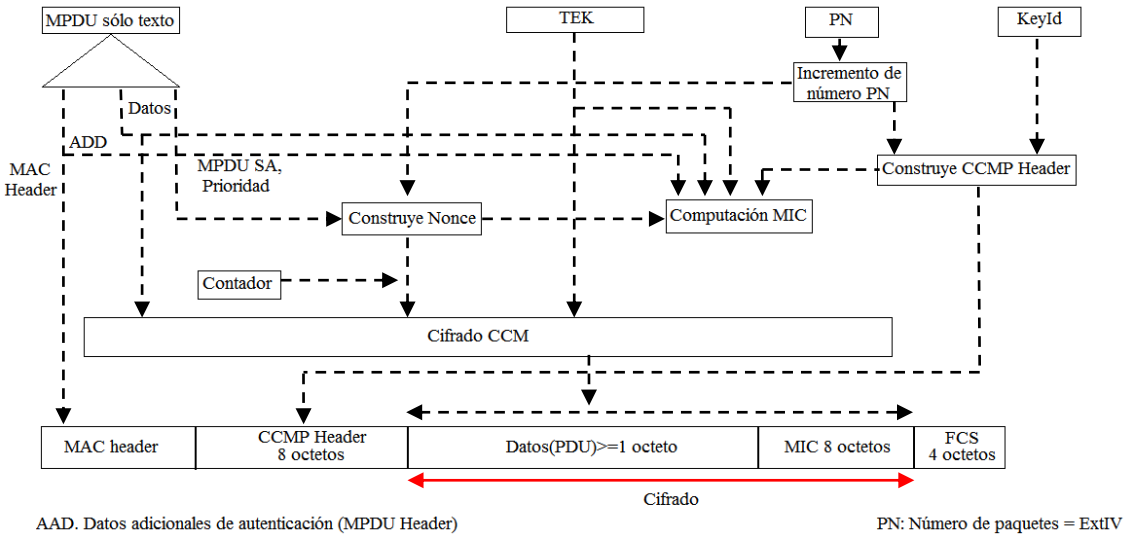

Figura 4.14: Cifrado CCPM [25]

Para finalizar, debe mencionarse el protocolo WRPA, que también opera con los fundamentos de AES pero haciendo uso del marco de cifrado autenticada OCB (*Offset Codebook Mode*), donde se realiza el proceso de cifrado y autenticación en una sola operación. El equipo de trabajo de IEEE 802.11i optó inicialmente por el modo OCB, sin embargo fue cambiado después debido a problemas de propiedad intelectual y licencias. Por lo tanto, se estableció CCMP como obligatorio [25].

4.5.2 Ventajas y desventajas

Una ventaja apreciable de este protocolo de seguridad es el hecho de que se encuentra dentro de los tres mecanismos de seguridad disponibles para proteger el cifrado y la autenticación de una

WLAN; el acceso protegido Wi-Fi (WPA), acceso protegido Wi-Fi 2 (WPA2) y conexión de redes privadas virtuales (VPN). El mecanismo de seguridad que se elija debe de ser específico al tipo de WLAN a la que se está accediendo y del nivel de cifrado de datos requerido.

WPA2 ofrece certificaciones de seguridad basados en normas que establece la Wi-Fi Alliance para redes locales de grandes empresas, empresas en crecimiento y para las redes personales, este protocolo proporciona autenticación mutua para verificar a usuarios individuales y cifrados avanzados.

En la actualidad se sabe que la seguridad de una WLAN, sólo es efectiva cuando está activada y se utiliza de forma uniforme en toda la red, por este motivo, las políticas del usuario son también una parte importante de las buenas prácticas de seguridad. El desafío es elaborar una política de usuarios de WLAN que sea lo suficientemente sencilla como para que los usuarios la cumpla. Además, lo suficientemente segura como para proteger la red. Actualmente, ese equilibrio es más fácil de lograr porque WPA2 se incorporan a los PA Wi-Fi y los dispositivos de cliente certificados.

Además, este protocolo posee ciertas características que lo hacen muchos más seguro que sus antecesores tales como, proporcionar autenticación y confidencialidad, separar la autenticación del usuario del cifrado de la información, ofrecer la distribución de llaves y nuevos mecanismos de integridad y privacidad de los datos mediante un Servidor RADIUS,

Dentro de las desventajas, se puede mencionar que aunque se han descubierto algunas pequeñas debilidades en WPA2 desde su lanzamiento, ninguna de ellas es peligrosa si se siguen unas mínimas recomendaciones de seguridad. La principal vulnerabilidad de WPA2-PSK, radica en la llave compartida entre las WSTA, ya que cuando un sistema basa su seguridad en una contraseña o llave, está totalmente expuesto a sufrir ataques por fuerza bruta, es decir ir comprobando contraseñas, aunque dada la longitud de la contraseña y si está bien elegida no debería representar mayor problema.

Para WPA2 existe la posibilidad de denegación del servicio durante el *4-Way Handshake*, capturando los cuatro mensajes, esto debido a que el primer mensaje del *4-Way Handshake* no existe autenticación previa, y cada WSTA tiene que guardar cada primer mensaje hasta que reciban un tercer mensaje legítimo, dejando a la WSTA potencialmente vulnerable, ante el agotamiento de memoria. Por otro lado mediante técnicas conocidas como es el caso de *spoofing* del primer mensaje transmitido por el PA, un atacante podría realizar un ataque de denegación del servicio (DoS) sobre la WSTA si es posible que existan varias sesiones simultáneas.

La debilidad final conocida es la posibilidad teórica de un ataque contra el *Temporal Key Hash* de WPA2, que implica una complejidad de ataque reducida bajo ciertas circunstancias, WPA2 se ven sometidas a vulnerabilidades que afectan a otros mecanismos, como son los ataques con *spoofing* de mensajes IEEE 802.1X (*EAPoL Logoff*, *EAPoL Start*, *EAP Failure* etc.,) revelados en primicia por *William A. Arbaugh* y *Arunesh Mishra* y probablemente alguna falta de autenticación [25].

Por último, es importante destacar que el uso del protocolo WPA2 no tiene protección alguna frente a ataques sobre las tecnologías en que se basan, es decir, en la intercepción de frecuencias de radio, la denegación del servicio a través de violaciones de IEEE 802.11, de-autenticación, de-asociación, etc., por otro lado el uso del algoritmo de cifrado AES requiere de un elevado número de recursos para su procesamiento, lo que implica que los dispositivos antiguos con pocos recursos informáticos no puedan operar junto a él, por razones obvias, por otro lado esto traería como consecuencia hace un cambio total o parcial de los dispositivos que no soporten el cifrado AES [25].

Capítulo 5

Mecanismos y estrategias de seguridad en redes Wi-Fi

Un mecanismo de seguridad está diseñado para detectar y prevenir un ataque de seguridad, o en su defecto recuperarse de él. En ninguno de ellos se puede lograr proteger totalmente la información de todos los ataques de seguridad, así que es protegida bajo ciertas condiciones.

Las vulnerabilidades informáticas de las WLAN son muchas y variadas, los proveedores de redes y empresas internacionales de estándares, como la IEEE y analistas han trabajado arduamente para combatir dichas vulnerabilidades en cuanto a su seguridad, por lo cual se han diseñado estrategias que van desde lo básico, hasta mecanismos más complejos, los cuales ofrecen un mayor grado de seguridad en cuanto a redes inalámbricas se refiere **[28].**

En la actualidad existen una serie de mecanismos y estrategias de seguridad encargados de proteger a las WLAN de acuerdo a la complejidad (**Tabla 5.1**) [11].

5.1 Estrategias básicas de seguridad

Existen una serie de estrategias conocidas que mejoran considerablemente la seguridad en las WLAN, las cuales consisten en tareas muy básicas de configuración, con la finalidad de reforzar los mecanismos de seguridad más robustos.

5.1.1 No implementar tecnología WLAN

El optar por esta estrategia trae como consecuencia no poder beneficiarse de las ventajas derivadas del uso de las WLAN. Más que evitar la implementación de esta tecnología se debe considerar el uso de mecanismos que brinden un nivel de seguridad adecuado al usuario, además de hacer uso de sistemas de exploración y monitoreo de paquetes de red inalámbrica para detectar el uso no autorizado de componentes inalámbricos [28].

Tabla 5.1: mecanismos y estrategias de seguridad

No.	Mecanismo/Estrategia	Complejidad
Estrategias básicas de seguridad		
1	No implementar tecnología WLAN	N/A
2	Cambiar el ESSID por defecto	Baja
3	Cambiar la contraseña por defecto	Baja
4	Desconectar el PA cuando no se encuentre en uso	Baja
5	Desactivar el broadcasting ESSID	Media
6	Establecer el número máximo de dispositivos que pueden conectarse	Media
7	Cambiar las llaves WEP regularmente	Media
8	Desactivar DHCP (*Dynamic Host Configuration Protocol* - Protocolo de configuración dinámica de host)	Media Alta
9	Activar el filtrado de direcciones MAC	Media Alta
Mecanismos de seguridad a nivel capa encale de datos		
10	Hacer uso de protocolos de cifrado de datos	Media Alta
11	Utilizar cifrado de datos y autenticación IEEE 802.1X	Alta
Mecanismos de seguridad a nivel capa de red		
12	Utilizar una red privada virtual VPN	Alta
13	Utilizar IPSec para proteger el tráfico de la WLAN	Alta

5.1.2 Cambiar el ESSID por defecto

El ESSID es el nombre de la WLAN, aunque no lo parezca el nombre que asignan los fabricantes a los PA, por defecto aporta mucha información sobre la red de datos, por este motivo es mejor modificarlo por otro completamente distinto. En sí esta estrategia se basa técnicamente en determinar un nombre no tan evidente como identificador de la red, ya que en algunos casos esto sirve de pista para averiguar el proceso con el que se ha generado la contraseña por defecto de la WLAN. Se dan casos en que el administrador o usuario opta por utilizar como nombre algo tan evidente como el nombre de la organización o en su defecto su propio nombre, es entonces que este factor puede ser aprovechado a favor de los atacantes, es decir esta técnica de seguridad trata de no llamar la atención del atacante para que exista menos posibilidades de que éste intente acceder a la red de datos [11].

5.1.3 Cambiar la contraseña por defecto

Los PA establecen políticas de seguridad, como una contraseña, esto con la finalidad poder acceder a él. Todos los fabricantes establecen una contraseña de acceso por defecto para la administración del PA. Por otro lado, al usar un fabricante la misma contraseña para todos sus dispositivos, aumenta la posibilidad que el atacante la conozca, es principalmente por este motivo la importancia de esta estrategia [11].

5.1.4 Desconectar el PA cuando no se encuentre en uso

Esta estrategia consiste técnicamente en desconectar el PA de la alimentación eléctrica cuando no esté en uso, cuando no vaya a ser utilizado durante una temporada o por la noche. El PA almacena la configuración y no se necesitará introducirla de nuevo cada vez que se conecte. También se puede desactivar el Wi-Fi en un enrutador sin necesidad de apagar toda la red, por lo cual se determina que sin red inalámbrica, no hay ataque Wi-Fi [11].

5.1.5 Desactivar el broadcasting ESSID

El broadcasting ESSID es el nombre de la red inalámbrica Wi-Fi; código que consiste en un máximo de 32 caracteres alfanuméricos, éste es difundido por un enrutador en el espectro de radiofrecuencia, se puede deshabilitar esta función de difusión y con esto lograr que no se encuentre a la vista de todos los dispositivos a donde llegue la señal del PA, dicha acción implica que los nuevos dispositivos que deseen asociarse a la red identifiquen automáticamente los datos de la red. Al desactivarlo se tendrá que introducir manualmente el ESSID en la configuración de cada nueva WSTA que desee asociarse a la red. Aun que esta estrategia parece ser la mejor solución para proteger a la red no lo es, únicamente debe de utilizarse como un método adicional a la implementación de un mecanismo de seguridad más fuerte y por lo tanto más seguro, ya que la debilidad de esta estrategia radica en que si el atacante puede hacer uso de algún *software* de monitoreo encontrara la red oculta o en su defecto si éste conoce el ESSID tal sea el caso de que se encuentre publicado en algún sitio WEB de acceso libre, esta estrategia queda totalmente vulnerada [11].

5.1.6 Establecer el número máximo de dispositivos que pueden conectarse

Para esta estrategia es necesario verificar las características del PA y si dentro de estas permite, establecer el número máximo de dispositivos que pueden asociarse al mismo tiempo, con esto se delimita a que sólo se encuentren conectados el número de WSTA que estén contempladas por el administrador de la red, en sí esta tarea requiere de constante actualización ya que el

administrador debe actualizar este número máximo cada que se vaya a asociar una nueva WSTA [11].

5.1.7 Cambiar las llaves WEP regularmente

Existen diversas herramientas de auditoría de redes encargadas de obtener la llave WEP de una determinada WLAN, esto se logra con el análisis de los datos transmitidos por la misma, se requiere de un análisis de 1-4 Gb de datos aproximadamente para romper la seguridad y así obtener una llave WEP. Sin embargo esto depende de la complejidad de las mismas. Para que esta estrategia sea efectiva, debe existir comunicación entre los usuarios de la red y el administrador de la misma, para que todos cuenten con la actualización de la llave WEP de la red, es decir que tanto el PA como las WSTA que se van a conectar a él, deben poseer la misma llave [11].

5.1.8 Desactivar DHCP

El DHCP es el protocolo de auto configuración para las estaciones de la red, es decir cada WSTA posee un identificador único conocido como dirección física o dirección MAC. El optar por esta estrategia implica que la configuración de las WSTA se tendrá que introducir manualmente tanto la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario. La efectividad de esta estrategia queda totalmente vulnerada sí el atacante conoce el formato y el rango de IP que se usan en la red, por otro lado no es considerado como la mejor estrategia de seguridad, ya que además de lo anteriormente mencionado, hoy en día existe una gran diversidad de *software* que poseen la capacidad de falsificar las direcciones MAC con gran facilidad, en general esta estrategia suele ser mayor la molestia que la posible seguridad que puede ofrecer a la red [11].

5.1.9 Activar el filtrado de direcciones MAC

Esta estrategia consiste en la creación de tablas de datos conocidas como ACL (*Access Control List*) en cada uno de los PA de la red inalámbrica. El administrador de la red, diseña una lista en la cual se alojan las direcciones MAC de las WSTA que pertenecen a la red, esto con la finalidad de permitir el acceso sólo a ciertos dispositivos de los cuales conoce sus respectivas direcciones MAC. Las listas de control de acceso deben ser llenadas manualmente en cada uno de los PA, esto puede ser una ardua tarea dependiendo del tamaño de la red. Rompiendo la teoría de que las direcciones MAC de cada dispositivo son únicas, es donde surge uno de los principales inconvenientes de esta estrategia de seguridad, dado a que estas direcciones viajan

sin cifrar por el aire por lo cual un atacante puede capturar direcciones MAC de tarjetas matriculadas en la red empleando un *sniffer*, y posteriormente asignarle una de estas direcciones capturadas a la tarjeta de un determinado dispositivo. En la actualidad existe *software* con el cual es muy fácil cambiar la dirección MAC, como por ejemplo *AirJack* o *WellenReiter*, etc., [2,11].

En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un PA el problema es más serio, porque éste contiene toda la tabla de direcciones válidas en su memoria de configuración, es importante mencionar que en este mecanismo el cifrado de la información es completamente nulo, por lo cual la información se encuentra mucho más expuesta [20].

Sin descartar que esta estrategia posea ciertas ventajas como el hecho de poder establecer una seguridad media/baja ya que las tarjetas MAC pueden ser clonadas. Además de que dicha estrategia posee gran sencillez para la administración de redes pequeñas o caseras. Por otro lado, también trae consigo diversos inconvenientes como el hecho de que no hay forma de asociar una dirección MAC a un nombre de usuario, por lo que sólo se puede autenticar por identidad de equipo y no por identidad de usuario. El formato MAC no es amigable generando así errores de manipulación en las listas, no es escalable ya que se tiene que autorizar o dar de baja a un equipo manipulando las tablas de todos los PA. En caso de extravío o robo de la tarjeta inalámbrica se compromete la seguridad de toda la red dando un tiempo prolongado hasta tomar las acciones debidas. Cabe mencionar que si existen dos o más dispositivos en la red con la misma dirección MAC pueden ocasionar conflictos, aunque por lo general en las WLAN esto no suele ser un problema de mucha relevancia, ya que el PA no puede distinguir que verdaderamente existen dos o más direcciones MAC iguales en la red, aun que esto no resultaría un problema mayor para un atacante experimentado, ya que si el atacante lo considera necesario puede implementar un ataque de Denegación de Servicio, con lo cual se lograría anular el dispositivo del que se ha robado la dirección MAC[11].

Como conclusión de esta estrategia, no es perfecta dado a que sólo es recomendable para pequeñas redes, ya que en medianas o grandes redes de datos la tarea de configuración se torna tedioso y complicado. Después de cierto número de dispositivos o de PA, la situación se torna inmanejable. Esto sin dejar de lado que hoy en día existen técnicas como la clonación de direcciones MAC por lo que esta técnica no es 100% segura [2, 18].

5.2 Mecanismos de seguridad a nivel capa de encale de datos

5.2.1 Hacer uso de protocolos de cifrado de datos

Esta estrategia consiste en determinar un protocolo de seguridad (WEP/WPA/WPA2) para activarlo en el PA. La finalidad de este tipo de protocolos de seguridad radica en que internamente se realiza un proceso, para que la información de la red no esté disponible a cualquier usuario, es decir estos protocolos se diseñaron con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante el cifrado de la información. Los PA más actuales proporcionan la posibilidad de soportar también el cifrado WPA, cifrado dinámico más seguro que WEP. En el PA hay que escribir una frase a partir de la cual se generan automáticamente las llaves, dicha frase debe consistir en una combinación de minúsculas, mayúsculas y números, en la posibilidad hay que evitar palabras incluidas en el diccionario o secuencias de teclado. Posteriormente de haber configurado el PA, lo que sigue es configurar las WSTA pertenecientes a la red, dicha configuración consiste en colocar la misma llave en todas las estaciones como en el PA [11].

5.2.3 Utilizar cifrado de datos y autenticación IEEE 802.1X-EAP

Con el propósito de proporcionar un método de autenticación y autorización mucho más seguro, diversos proveedores propusieron aumentar la seguridad de una WLAN con la implementación del estándar IEEE 802.1X, permite autenticar a usuarios en lugar de sólo a máquinas y se puede utilizar para asegurar que los usuarios se conecten a redes legítimas y autorizadas en lugar de a redes falsas que intentan robar credenciales [11, 20].

El uso de una solución basada en IEEE 802.1X permite la modificación frecuente de las llaves de cifrado, como parte del proceso de autenticación segura de IEEE 802.1X, el método EAP genera una llave de cifrado única para cada cliente. El estándar IEEE 802.1X mejora la seguridad proporcionando las siguientes mejoras sobre WEP, proporciona un modelo de seguridad con administración centralizada, además de que la llave de cifrado principal es única para cada estación, por lo tanto, el tráfico de esta llave es reducido (no se repite en otros clientes), existe una generación dinámica de llaves por parte del Servidor de autenticación, sin necesidad de administrarlo manualmente y aplica una autenticación fuerte en la capa superior [11].

5.3 Mecanismos de seguridad a nivel capa de red

5.3.1 Utilizar una red privada virtual (VPN)

Una vez descritas las estrategias que basan su seguridad en protocolos de cifrado más conocidos e implementados con mayor frecuencia (WEP,WPA/WPA2), se hace necesario mencionar que existe la opción de la adopción de estrategias alternativas, como la red privada virtual (VPN) y la seguridad del protocolo Internet (IPSec).

Una estrategia basada en una red privada virtual entre dos sedes es conocida como VPN, normalmente utilizada para enlazar dos sedes geográficamente distantes garantizando la privacidad, integridad y confidencialidad de los datos transmitidos. Una VPN es posible gracias a la combinación de determinados protocolos de seguridad y cifrado, así como de algoritmos de funcionamiento, VPN no es una tecnología en sí, es una forma de utilizar la tecnología para un objetivo concreto, por otro lado diversas soluciones VPN de distintos fabricantes no son compatibles entre sí, dado a que utilizan protocolos diferentes, por la diversidad de versiones propietarias o sistemas de cifrado [14].

Esta solución provee una especie de túnel donde los datos viajan totalmente cifrados desde un sitio hasta otro. En la **Figura 5.1** se muestra un esquema básico de VPN, donde ésta trabaja a través de un Servidor VPN, creando un protocolo de cifrado para transferir datos a usuarios que se encuentran fuera de la cobertura de la WLAN. El *software* especial de VPN en la WSTA remoto utiliza el mismo protocolo de cifrado, habilitando los datos para que sean transmitidos de forma segura sin oportunidad de intercepción [33].

Cuando los usuarios se conectan a una red empresarial a través de Internet esperan que existan requisitos de autenticación adicionales y límites de tiempo de espera asociados al uso de una VPN, estos pasos adicionales pueden resultar pesados para los usuarios que están acostumbrados a conectarse fácilmente a recursos desde el interior de una WLAN. En el mundo empresarial existen principalmente dos tipos de conexiones diferentes a la red de la organización [28]:

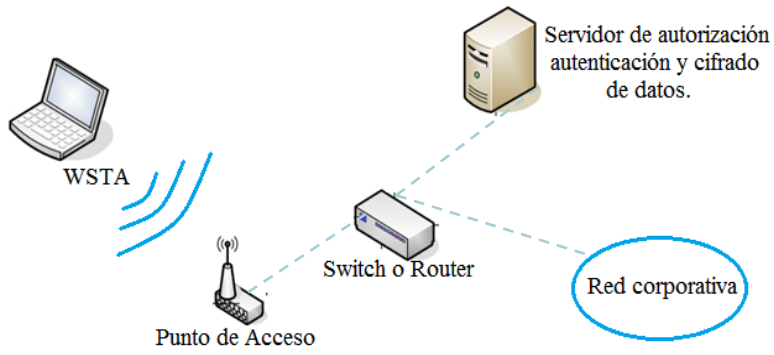

Figura 5.1: funcionamiento básico de VPN

1. **Conexión VPN entre las dos sedes (modo túnel).** Permite la unión transparente de las dos redes para así poder compartir datos, Servidores, impresoras, etc.,
2. **Conexiones puntuales (acceso remoto).** Consiste en el hecho de una WSTA se desplaza cambiando de ubicación, y que por el motivo que sea tiene que tener acceso a los recursos de la red (*roaming*).

VPN constituye una solución excelente desde el punto de vista de la seguridad, sin embargo, no es necesariamente la mejor solución para asegurar WLAN internas, para este tipo de entorno una VPN no ofrece prácticamente ningún grado de seguridad adicional, en comparación con las soluciones WPA2 con autenticación IEEE 802.1X, que se diseñó específicamente para hacer frente a las amenazas de los sistemas inalámbricos, además de que VPN incrementa la complejidad y los costos significativamente, reduce la capacidad de uso y anula el funcionamiento de características importantes. Aunque es perfectamente posible implementar soluciones WPA junto con la tecnología VPN para garantizar la seguridad de una red inalámbrica, dicha solución no ofrece ninguna ventaja con respecto a una solución pura basada en WPA/WPA2, especialmente si se considera el nivel adicional de complejidad que se agrega a la red inalámbrica si se utiliza en combinación con una solución VPN [2, 28].

5.3.2 Utilizar IPSec para proteger el tráfico de la WLAN

Esta solución está basada en un conjunto de estándares abiertos desarrollados por el IETF. IPSec es ejecutado por un sistema de protocolos criptográficos para otorgar al tráfico IP propiedades de integridad, autenticado y/o cifrado, además de que opera en la capa 3 (*capa de red*) del modelo OSI, al contrario de los protocolos de seguridad especializados en el cifrado de la información, los cuales trabajan en la capa de enlace de datos. Para asegurar todos los usos de la red y las comunicaciones que utilizan la red IP, se hace uso de combinaciones de *hashing*, de llave simétrica y de algoritmos criptográficos asimétricos [8, 14].

Los protocolos con los que trabaja IPSec son conocidos como *Authentication Header (AH)* el cual proporciona integridad, autenticación y no repudio si se eligen los algoritmos criptográficos apropiados y otro conocido como EAP (*Encapsulating Security Payload*), este proporciona confidencialidad y proporciona la opción de autenticación y protección de integridad [14].

Al igual que otros sistemas de seguridad, IPSec ofrece servicios de seguridad, como [8]:

- Autenticación del par (*Peer Authentication*)
- Confidencialidad de los datos (*Data confidentiality*)
- Integridad de datos (*Data integrity*)
- Autenticación del origen de datos (*Data origin Authentication*)
- Detección de la respuesta (*Replay detection*)
- Control de acceso (*Access control*)
- Confidencialidad del tráfico(*Traffic flow confidentiality*)

IPSec define algoritmos criptográficos tal cuales incluyen HMAC-SHA-1 para garantizar la integridad de los datos y en el caso de la confidencialidad se hace uso de triple DES-CBC y AES-CBC, además de definir dos principales métodos para la propagación de los datos a través de una red, en modo túnel (de sitio a sitio o de acceso de cliente) y en modo transporte (protección de un extremo a otro; sin túnel) [8].

La utilización de las soluciones VPN basadas en IPSec para garantizar la seguridad de las redes inalámbricas surge de la misma necesidad que utilizar VPN para hacer seguras las WLAN. Ésta solución es recomendable en el caso en que la empresa sea nómada e itinerante, es decir que necesiten el acceso a Internet, a datos corporativos fuera de la misma, para proporcionar seguridad al conectarse a Internet o a la red de la empresa desde otras redes [4].

IPSec permite a dos usuarios de red autenticarse mutuamente de forma segura y autenticar o cifrar paquetes de red individuales, lo cual resulta ser una cualidad que no todas las soluciones para WLAN poseen. Además de que se puede usar IPSec para colocar una red sobre la otra en modo de túnel de forma segura o simplemente para proteger paquetes IP transmitidos entre dos dispositivos.

Los elementos clave de la arquitectura de una red WLAN, en la que se emplea una solución VPN basada en IPSec para asegurar el tráfico de datos son los siguientes [15, 28]:

- **Clientes y adaptadores inalámbricos.** Proporcionan conectividad inalámbrica a los PA.

- **Cliente IPSec VPN.** Es el extremo del túnel IPSec en el terminal de usuario. El cliente de VPN debe conectarse al concentrador VPN al iniciarse la sesión por parte del terminal de usuario.
- **El PA inalámbrico**. Proporciona conectividad Ethernet a la red corporativa. Si el PA tiene capacidades de filtrado, se puede filtrar el tráfico para permitir únicamente los protocolos DHCP e IPSec.
- ***Gateway*/concentrador IPSec VPN.** Autentica a usuarios inalámbricos y termina los túneles de IPSec. Puede también actuar como Servidor DHCP para las WSTA.
- ***Firewall*.** Se recomienda ubicar un *firewall* después del concentrador VPN que aplique políticas de seguridad al flujo no cifrado.

En función del método de autenticación utilizado pueden ser empleados opcionalmente los siguientes elementos [4]:

- **Servidor RADIUS.** Proporciona la autenticación de usuario para los WSTA que se conectan al Gateway/concentrador VPN.
- **Servidor PKI.** Proporciona certificados X.509 para la autenticación de usuario y de Servidor. Se recomienda que los certificados de cliente sean accesibles solamente mediante *hardware* protegido con contraseña como, por ejemplo, *smart-cards* o llaves USB.
- **Servidor OTP.** Proporciona autenticación OTP mediante Servidores RADIUS.

Es altamente recomendable la utilización de políticas basadas en certificados para establecer los túneles IPSec en lugar de llaves compartidas por los riesgos que implican estas últimas, implicando sobrecarga en el mantenimiento al obligar a todos a cambiar las llaves compartidas. Además, se recomienda que el concentrador VPN compruebe el estado de los certificados de cliente contra las autoridades CRL (*las principales Autoridades Certificadoras internacionales actualmente son Verisign y Thawte*) o un Servidor de OCSP (*Online Certificate Status Protocol*).

La implementación de esta tecnología presenta diversos inconvenientes, si es que se opta por esta solución para proteger la WLAN, ya que IPSec no maneja autenticación a nivel de usuario, únicamente maneja autenticación a nivel de equipo, en muchas ocasiones esta cuestión no representa un gran problema, pero si un usuario no autorizado consigue asociarse a la red, podrá acceder también a otros dispositivos protegidos por IPSec en la red. Por otro lado en entornos de mayores dimensiones, la administración de direcciones IP puede resultar muy complicada si IPSec se utiliza para proporcionar una protección de un extremo a otro para otras aplicaciones, o

para el tráfico de la red inalámbrica. Existe la posibilidad de que ciertos dispositivos no sean compatibles con IPSec, lo cual representa un gran problema, ya que la seguridad completa exige el cifrado de todo el tráfico de extremo a extremo, pero en este caso de no compatibilidad el tráfico se transmitirá a estos dispositivos sin cifrar, es decir IPSec no proporcionará ningún tipo de protección a estos dispositivos, de modo que se encontraran expuestos a cualquiera que se asocie a la WLAN [28].

Aunque IPSec es transparente para los usuarios, no lo es totalmente para los dispositivos de red porque funciona en el nivel de red, no en el de MAC. Esto agrega requisitos adicionales para las normas del *firewall*. Además de que IPSec no puede proteger el tráfico de difusión o multidifusión, ya que sólo controla la comunicación entre dos partes que se han autenticado mutuamente y que han intercambiado llaves. IPSec no protege la red inalámbrica, sólo los paquetes de red, por lo cual en este caso el cifrado y descifrado de tráfico de red IPSec incrementa la carga en los dispositivos. A su vez, esto puede sobrecargar los Servidores de uso intensivo. Esta carga de procesamiento puede desviarse a tarjetas de red especiales pero no suelen venir integradas en los Servidores. Al igual que la solución basada en VPN esta versión de IPSec, no se ocupa de la seguridad de la WLAN interna, además de que en cuestión de la autenticación, IPSec utiliza un esquema de autenticación de llave compartida poco seguro (*XAuth*). Si se quiere ofrecer la misma solución de seguridad tanto en entorno empresarial como para los empleados fuera del límite físico de la oficina, la solución IPSec VPN es altamente recomendada así como el uso de *firewalls* que filtren el tráfico de la red de la organización [28].

5.4 Comparativa entre protocolos de cifrado WEP, WPA y WPA2

Haciendo énfasis en las secciones de los protocolos de cifrado y las estrategias basadas en VPN, se realiza una comparativa que muestra de manera general las principales diferencias de los protocolos de seguridad más utilizados por las WLAN (*enfoques de seguridad; autenticación y cifrado*); WEP, WPA, WPA2, además de estrategias alternativas de seguridad conocidas VPN e IPSec. Para cumplir con este propósito, la **Tabla 5.2** presenta las principales características de dichos protocolos y estrategias de seguridad, los parámetros a considerar para poder realizar dicha comparativa, son por un lado aspectos relacionados con la autenticación y por otro lado los aspectos relacionados con el cifrado de la información.

Tabla 5.2: comparativa de los enfoques de seguridad (autenticación y cifrado) [35]

		WEP	**WPA**	**WPA2**	**VPN / IPSec**
Autenticación	**Autenticación**	WEP	IEEE 802.1X + EAP	IEEE 802.1X + EAP	IKE de máquina, X-AUTH de usuario
	Pre-Autenticación	No	Si	IEEE 802.1X EAPOL	Si
C I F R A D O	**Negociación de cifrado**	No	Si	Si	Sí (DES, 3DES, AES)
	Cifrado	RC4 40 bits/104 bits	TKIP: RC4 128 bits	CCMP: AES 128 bits	ESP: DES 56bit, 3DES 168bit, AES 168bits, 128bits, 192bits, 256bits
	IV	24 bits	48 bits	48 bits	DES-CBC 8 bytes
	Integridad de la cabecera	No	MIC	CCM	AH
	Integridad de datos	CRC32	MIC	CCM	AH/ESP
	Protección de respuesta	No	Forzar secuencia de IV	Forzar secuencia de IV	Si
	Gestión de llaves	No	Basa en EAP	Basada en EAP	IKE (*Diffie-Hellman*)
	Distribución de llaves	Manual	IEEE 802.1X (EAP)	IEEE 802.1X (EAP)	*Diffie-Hellman*
	Llave asignada	Red	Paquete, sesión y usuario	Paquete, sesión y usuario	Usuario
	Llave por paquete	Concatenación de IV	Mezclado TKIP	N/A	ESP
	Seguridad ad-hoc	No	No	Sí (IBSS)	No

5.5 Comparativa entre soluciones de seguridad a nivel capa enlace de datos y a nivel capa de red

En la **Tabla 5.3,** se realiza otra comparativa pero en esta ocasión se contemplan aspectos más generales, que de igual manera hacen la diferencia entre las estrategias contempladas.

Tabla 5.3: comparativa de los enfoques de seguridad para las redes WLAN [28]

Característica	WLAN IEEE 802.1X (WPA/WPA2)	WEP estática	VPN	IPSec
Autenticación Segura	Sí	No	Sí, sólo cuando no se utiliza autenticación de llave compartida.	Sí, siempre y cuando se use la autenticación de certificados o de Kerberos.
Cifrado de datos de alta seguridad	Sí	No	Sí	Sí
Conexión y reconexión transparente	Sí	Sí	No	Sí
Autenticación de usuarios	Sí	No	Sí	No
Autenticación de dispositivos	Sí	Sí	No	Sí
Protección del tráfico de difusión y multidifusión	Sí	Sí	Sí	No
Se requieren dispositivos de red adicionales	Servidores RADIUS	No	Servidores VPN, Servidores RADIUS	No
Acceso seguro a la WLAN en lugar de sólo a los paquetes	Sí	Sí	No	No

Capítulo 6

Proceso de la toma de decisiones para una red Wi-Fi segura

En las secciones anteriores se ha analizado el funcionamiento sobre los diversos mecanismos y estrategias de seguridad disponibles para garantizar la seguridad de la información en una WLAN. Además de la descripción de las amenazas más frecuentes a las que se enfrentan este tipo de redes y cómo es que cada una de éstas hace frente o es vulnerable a dichas amenazas. Con esa información es posible tomar decisiones justificadas sobre cómo aplicar cada opción ya sea a entornos personales o empresariales.

Las últimas mejoras de seguridad realizadas en los estándares de redes inalámbricas con la implementación de WPA y WPA2 se han centrado en las graves brechas de seguridad basada en WEP y por tanto, han marginado la necesidad de buscar soluciones, como el uso de IPSec o de una VPN, para garantizar la seguridad de las conexiones inalámbricas. Con la explicación de todas y cada una de las estrategias de seguridad descritas. La solución basada en WPA2 en conjunto con el estándar IEEE 802.1X es la mejor de todas las estrategias disponibles, sin embargo, si se opta por implementar dicha solución se tendrá que elegir entre las diversas opciones para que su funcionamiento sea el requerido. Existen dos procesos de seguridad recomendados entre los que se puede elegir para el caso de las WLAN. Las dos opciones principales son las siguientes [28]:

- El uso de contraseñas o certificados para la autenticación de usuarios y dispositivos (WPA2 con EAP-TLS y Servicios de *Certificate Server*).
- El uso de protección de datos de WLAN WPA o WEP dinámica (WPA2 con PEAP-MS-CHPAv2).

Aparte del nivel de seguridad proporcionado por cada una de estas soluciones, el factor determinante básico para elegir entre estos dos enfoques se reduce a los recursos necesarios para implementar las soluciones y ofrecer compatibilidad con ellas. El uso de WPA o WPA2 con EAP-TLS es la opción disponible más segura para garantizar la seguridad de una WLAN, pero conlleva una implementación más elaborada y tiene asociados costos superiores de administración, ya que depende de la infraestructura de certificados subyacente. Sin embargo, muchos entornos de medianas empresas ya disponen de sistemas que cumplen los requisitos

necesarios para WPA2 con EAP-TLS, por lo que en realidad puede ser una opción más atractiva para muchas empresas. Incluso si no se dispone de la tecnología necesaria, dichas empresas necesitan la misma tecnología en la que se basa esta solución, los certificados y Servidor RADIUS para cubrir otras necesidades, por lo que incluso en ese caso existen muy buenos motivos empresariales y técnicos que justifican la implementación de esta solución [28].

WPA o WPA2 con PEAP-MS-CHPAv2 tiene menos requisitos en cuanto a conocimientos técnicos y equipamiento ya que no necesita una infraestructura de certificados subyacente. Puesto que la mayoría de los dispositivos que hay actualmente en el mercado están certificados para el uso con WPA2. Tiene cierto sentido utilizar dispositivos compatibles con WPA2, incluso si se decide utilizar WPA por las ventajas administrativas que presenta actualmente con respecto a WPA2.

El método de cifrado AES de WPA2 se consideró más seguro que el método TKIP de WPA y si se considera que está previsto ofrecer compatibilidad de GPO con WPA2 en versiones futuras, conviene ir preparando las bases para una implementación futura de WPA2. El diagrama de flujo siguiente (**Figura 6.1**) muestra un resumen de las opciones entre las dos guías de soluciones de seguridad de WLAN [28].

El resultado del diagrama de flujo mostrado en la **Figura 6.1** dependerá del tamaño de la empresa, así como de sus requisitos de seguridad específicos. La mayoría de las empresas pueden utilizar cualquiera de las soluciones de WLAN, sin necesidad de modificaciones. Por ejemplo, gran parte de las empresas pequeñas y medianas elegirán la solución más simple; seguridad en WLAN con PEAP y contraseñas. Las empresas más grandes suelen inclinarse por el uso de la solución de seguridad en WLAN con Servicios de *Certificate Server*, basada en certificados digitales [28].

Ambas soluciones brindan un alto grado de flexibilidad, ya que la primera de estas puede implementarse en empresas que tienen decenas o miles de usuarios asociados a la red de datos, en el caso de la segunda solución normalmente se aplica a empresas de cientos a decenas de miles de usuarios, ya que las empresas con menos de 500 usuarios no suelen disponer de los recursos de TI suficientes para implementar y mantener las entidades emisoras de certificados [28].

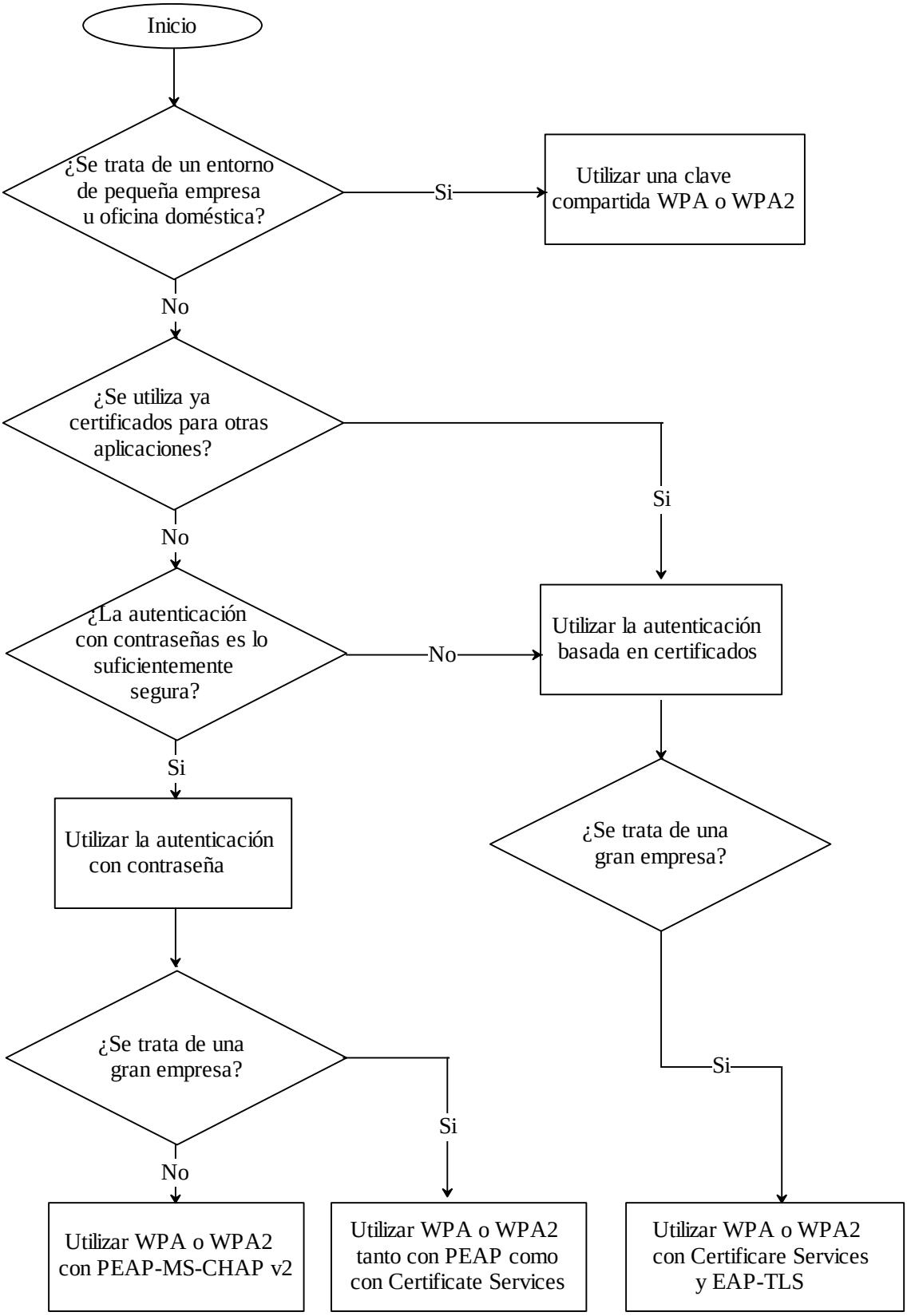

Figura 6.1: diagrama de flujo para la toma de decisiones para una WLAN [28]

Capítulo 7

Conclusiones y Trabajo futuro

La utilización de las WLAN, ha ido creciendo de manera exponencial, debido a las diversas ventajas que ofrece el uso de esta tecnología, de las más notorias es el hecho de proporcionar flexibilidad y comodidad en la conectividad entre dispositivos. Una WLAN representa mantener la comunicación sin tener ninguna conexión física, además de la facilidad de implementación y costo accesible de instalación. Hoy día la mayoría de estas redes son instaladas sin considerar el aspecto de la seguridad, por lo cual se convierten en redes totalmente vulnerables. Uno de sus principales inconvenientes es el medio por donde se transmite la información, por lo tanto la información de la red está disponible para cualquier usuario, pertenezca o no a la red, es por eso que es altamente recomendable la utilización de una estrategia y/o mecanismo de seguridad homogéneo y sin fisuras, que cubra todos los aspectos importantes sin afectar la velocidad de transmisión. Además que vaya de la mano con las ventajas que proporciona este tipo de tecnología.

Una red Wi-Fi en sí no es segura o insegura, éste valor lo determina la implementación de la misma. La seguridad meramente inalámbrica sólo incluye mecanismos de seguridad presentes en las capas 1 y 2 del modelo OSI. Numerosos estudios han demostrado que los mecanismos de seguridad implementados con mayor frecuencia en las redes WLAN (WEP, WPA, WPA2) son vulnerables desde su nacimiento, por lo cual con el pasar de los años se han realizado múltiples estudios de este tema con la finalidad de subsanar los problemas que presentan dichos mecanismos. Mecanismos que llevan a cabo el proceso de cifrado de datos a nivel de capa de enlace, pero no garantizan confidencialidad punto a punto. Existen mecanismos de seguridad como SSH, HTTPS, SSL e IPSec VPN los cuales pueden ser empleados con múltiples tecnologías de acceso, incluidas las WLAN. En la actualidad el nivel de seguridad que puede proporcionar una WLAN es comparable al de las redes cableadas.

Si lo que se requiere es seguridad a nivel capa de enlace, optar por una solución basada en WEP estática sería un grave error, ya que no proporciona una seguridad eficiente y de alto nivel, numerosos estudios han demostrado que WEP es altamente vulnerable, su principal problema radica en los niveles más bajos de su funcionamiento y lógica de cifrado; principalmente en la colisión de valores del vector de inicialización. La autenticación WEP de llave compartida es un mecanismo de seguridad muy débil y no se debe utilizar a no ser que sea absolutamente necesario, como para dispositivos que no admiten otro tipo de protocolos de seguridad más

avanzados. Pero si es posible y el entorno de trabajo lo permite lo mejor es hacer uso de un método de autenticación de más alto nivel, como por ejemplo un portal cautivo (Servidor de certificados digitales).

WPA2 es considerado como el único protocolo de seguridad para redes WLAN seguro. Este protocolo hace uso de IEEE 802.1X y AES(CCMP), los cuales son dos mecanismos extremadamente sólidos y que actualmente se les puede catalogar como seguros en los tres aspectos fundamentales que en la actualidad se ponen en dudas respecto a Wi-Fi; autenticación, control de acceso y confidencialidad. Sin embargo, la adopción del mismo representa un problema para algunas empresas ya que implica migrar de un mecanismo de seguridad a otro, lo cual requiere del cambio total o parcial de los PA instalados previamente, por un modelo que sea compatible con WPA2, además de que existen dispositivos inalámbricos que no son compatibles con el algoritmo de cifrado AES empleado por WPA2, dicho algoritmo de cifrado requiere de una gran capacidad para llevar a cabo el procesado de los datos.

WPA es la opción a considerar después de WPA2, dado que proporciona un nivel de seguridad aceptable y es una solución para todos los dispositivos móviles que no soporten WPA2, como ya se describió en su momento existe la posibilidad de hacer uso de WPA-PSK pero dicha solución debe ser implementada sólo para redes de bajo riesgo o para redes con usuarios invitados que necesiten la máxima protección, pero en cualquier otro caso se recomienda hacer uso de IEEE 802.1X. Sin descartar que WPA, aporta mejoras importantes con respecto a WEP, en el caso de WPA-Enterprise es mucho más seguro, la protección que brinda WPA radica en la gestión dinámica de llaves.

En el caso de WPA y WPA2, el factor de la autenticación de cliente, puede hacer uso de la combinación del estándar IEEE 802.1X y EAP, para la implementación de este último se debe de tomar en cuenta que existen diferentes tipos, entre los más destacados se encuentra el EAP-TLS si lo que se busca es una autenticación de cliente mediante certificados, EAP-TTLS y PEAP basan la autenticación de la WSTA mediante un ID de usuario y una llave secreta. Para la mayoría de los casos podría interpretarse que la solución más segura es hacer uso de la autenticación mediante certificados digitales.

Las soluciones basadas en el cifrado de datos como WEP, WPA y WPA2, cubren con la seguridad de los clientes cuando se conectan a la red inalámbrica local, pero en el caso de que se requiera la implementación de un mecanismo de seguridad en el entorno empresarial y para

clientes remotos, es decir usuarios que se conecten desde fuera de la empresa, la mejor opción sería la implementación de una solución basada en IPSec de VPN, o mediante el uso de *firewalls* que filtren el trafico que entre en la red de la empresa, en un mejor caso se pueden combinar las soluciones como IPSec de VPN con soluciones especificas que se especializan en el cifrado de la información como WEP, WPA, WPA2(IEEE 802.11i).

Posteriormente a todo el análisis realizado se puede concluir de manera clara, que si trata de una red empresarial o personal, la implementación de la solución con WEP estática, sería un grave error, esto debido a que como ya se mencionó en su momento dicho protocolo de seguridad presenta diversas vulnerabilidades, además de que hoy en día ya es considerado como obsoleto, la solución inmediata que se propone después de WEP sería una solución basada en WPA-PSK debido a que dicho protocolo corrige las principales vulnerabilidades que presenta su antecesor WEP. La principal ventaja de WPA es la gestión dinámica de llaves, para el caso de las medianas y grandes empresas la mejor solución es WPA2 con EAP-TLS y Servicios de *Certificate Server*, o implementar una solución VPN basada en IPSec siempre que sea posible [4].

7.1 Trabajo futuro

En el presente documento únicamente se abordó las principales estrategias y mecanismos de seguridad existentes para una red de área local regida por la tecnología Wi-Fi. Como trabajo futuro se considera mostrar diversos ataques con la utilización de *software* especializado en auditoria de redes, esto con la finalidad de poder apreciar los riesgos a los que se exponen con el uso de una tecnología tan observable. De igual manera mostrar el proceso de implementación de alguno de los mecanismos de seguridad más robustos, con la finalidad de mostrar al lector como hacer la implementación.

Referencias

[1] Agustín González, Patricio Fernández, *De WEP A Wpa2 Seguridad En Redes Inalámbricas*, Universidad Técnica Federico Santa María, Departamento de Electrónica, http://profesores.elo.utfsm.cl/~agv/elo322/1s08/project/PatricioFernandezWEPtoWPA.pdf, Fecha de consulta Noviembre de 2012.

[2] Álvarez Méndez, *Seguridad al acceso de información en la implantación de una Red Inalámbrica*, Universidad Central de Venezuela, http://saber.ucv.ve/xmlui/bitstream/123456789/2420/1/Tesis%20yelitza%20Alvarez.pdf, Fecha de consulta Diciembre de 2012.

[3] Bradley Mitchell, *Wireless Standards - IEEE 802.11b IEEE 802.11a IEEE 802.11g and IEEE 802.11n,* http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm, Fecha de consulta Marzo de 2013.

[4] *Capítulo 2. Topologías y requerimientos WLAN*, http://dspace.ups.edu.ec/bitstream/123456789/221/3/Capitulo%202.pdf, Fecha de consulta Abril de 2013.

[5] Carlos Varela/Luis Domínguez, *Redes Inalámbricas*, Escuela Técnica Superior de Ingeniería Informática, Universidad de Valladolid, http://www.blyx.com/public/wireless/redesInalambricas.pdf, Fecha de consulta Marzo de 2013.

[6] Claudio Armando Cabrera Proaño, *Capítulo III Análisis a la Seguridad de Redes Inalámbricas como extensión de una red LAN,* http://repositorio.utn.edu.ec/bitstream/123456789/593/3/CAPITULO%20III.pdf, Fecha de consulta Junio de 2013.

[7] CYBERCOM Cable & Wireless, *Redes LAN Inalámbricas* (Wireless LAN), Argentina, http://www.cybercom-cw.com.ar/pdf/Cybercom_WLAN_Paper.PDF, Fecha de consulta Abril de 2012.

[8] Daniel Omar Esmoris, *Control de acceso a redes*, Universidad Nacional De La Plata, http://postgrado.info.unlp.edu.ar/Carreras/Especializaciones/Redes_y_Seguridad/Trabajos_Finales/Esmoris.pdf, Fecha de consulta Enero de 2013.

[9] Domingo Alberto Ríos, *Seguridad en WLAN*, Universidad Nacional del Nordeste Facultad de Ciencias Exactas y Naturales y Agrimensura, Licenciatura en Sistemas de Información, http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MONOGRAFIA_DE_SEGURIDAD_EN_%20REDES_WIFI.pdf, Fecha de consulta Diciembre de 2012.

[10] Edgar Álvarez, Jasson Raúl, *redes de comunicación inalámbrica interfaces de comunicación protocolos tecnología*, http://repositorio.espe.edu.ec/handle/21000/702, Fecha de consulta Diciembre de 2012.

[11] Eduardo Tabacman, *Seguridad en redes wireless.* 2ª ed. Colombia: ACIS, Fecha de consulta Enero 2013.

[12] Emerson Alexander Gómez Morales, *Análisis de redes inalámbricas, sus tecnologías, arquitecturas físicas, lógicas y los diferentes componentes necesarios para su implementación,* Guatemala, http://biblioteca.usac.edu.gt/tesis/08/08_0299_EO.pdf, Fecha de consulta Febrero de 2013.

[13] Francisco José Molina Robles, *Instalación y mantenimiento de servicios de redes locales,* Editorial Ra-ma, Fecha de consulta Noviembre de 2012.

[14] Gaspar Homs García, *Enlace entre dos sedes distantes,* http://openaccess.uoc.edu/webapps/o2/bitstream/10609/14785/6/ghomsgTFC0612memoria.pdf, Fecha de consulta Febrero de 2013.

[15] Izaskun Pellejero, *Seguridad en redes WLAN Conozca lo esencial para su empresa,* Euskadi, Fecha de consulta Mayo de 2013.

[16] Javier Guillermo Horn Morgenstern Valdivia, *Estudio Sobre Situación Actual De Iluminación De WLAN En Valdivia Y Análisis De Sistemas De Encriptación De Datos Utilizados En Wi-Fi*, Universidad Austral de Chile, http://cybertesis.uach.cl/tesis/uach/2008/bmfcih813e/doc/bmfcih813e.pdf , Fecha de consulta Abril de 2013.

[17] Jesús Ramírez Sánchez, José Vicente Díaz Martínez, *Las redes inalámbricas, más ventajas que desventajas,* Universidad Veracruzana, http://www.uv.mx/iiesca/files/2012/12/redes2008-2.pdf, Fecha de consulta Diciembre de 2012.

[18] Jimmy Arthur Villanueva Llerena, *Seguridad avanzada en Redes Wireless IEEE 802.1X*, http://www.jacksecurity.com/files/publications/Jack42.pdf, Fecha de consulta Marzo de 2013.

[19] Jorge Alberto López Guerrero, *Redes inalámbricas wireless LAN,* Universidad Autónoma del Estado de Hidalgo, http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20inalambricas%20wireless%20LAN.pdf, Fecha de consulta Enero de 2013.

[20] José Rapallini, Francisco Roqué, Sistemas de transmisión y redes inalámbricas, *Capítulo II Seguridad En Redes Wireless LAN IEEE 802.11 (WLAN),* http://www.frlp.utn.edu.ar/materias/stri/wlan.pdf, Fecha de consulta Julio de 2013.

[21] José López López, Sergio Mena Doce, *Desarrollo de un demostrador para evaluar técnicas Cross-Layer en sistemas de comunicaciones inalámbricos*, Universidad Politécnica de Catalunya, http://upcommons.upc.edu/pfc/bitstream/2099.1/4987/1/memoria.pdf, Fecha de consulta Enero 2013.

[22] José A. Caballar, *Guía de campo Wi-Fi,* Alfaomega Ra-ma, Fecha de consulta Diciembre 2012.

[23] José Ignacio Claros V, *Sistemas & Telemática,* Revista de la Facultad de Ingeniería, http://www.icesi.edu.co/sistemas_telematica/, Fecha de consulta Mayo de 2013.

[24] José Manuel Luaces Novoa, *Seguridad en redes inalámbricas de área local (WLAN)*, Universitat Oberta de Cataluña, http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18804/6/jluacesTFC0113memoria.pdf, Fecha de consulta Junio de 2013.

[25] Juan Rodrigo Sac De Paz, *Estudio de vulnerabilidad de los cifrados WEP Y WPA, y su impacto en las redes inalámbricas de área local,* Universidad de San Carlos de Guatemala**,** http://biblioteca.usac.edu.gt/tesis/08/08_0466_CS.pdf, Fecha de consulta Febrero de 2013.

[26] Julio Cesar Ardita, *Análisis De WPA/WPA2 Vs WEP*, Escuela Politécnica del Ejército, Ecuador, http://cursos.delaf.cl/archivos/cursos/comunicaciones-inalambricas/material-de-apoyo/An%C3%A1lisis+entre+WEP+y+WPA.pdf, Fecha de consulta Noviembre de 2012.

[27] Manuel Suarez Gutiérrez, *Mecanismos De Seguridad En Redes Inalámbricas*, http://www.uv.mx/personal/mansuarez/files/2012/05/Mecanismos-de-Seguridad-en-Redes-InalambricasProtegido.pdf, Fecha de consulta Diciembre de 2012.

[28] Microsoft, *Capítulo 2: Determinación de una estrategia segura para Redes Inalámbricas del libro Seguridad en LAN inalámbricas con servicios de Certificate Server*, http://www.microsoft.com/latam/technet/articulos/wireless/pgch02.mspx#E5H, Fecha de consulta Junio de 2013.

[29] Microsoft, *Configuración de redes inalámbricas IEEE 802.11 de Windows XP para el hogar y la pequeña empresa*, http://www.microsoft.com/spain/technet/recursos/articulos/wifisoho.mspx, Fecha de consulta Junio de 2013.

[30] Miguel Iniesta Archidona, *Seguridad WIFI. Agresiones posibles*, Universidad politécnica de Valencia, http://riunet.upv.es/bitstream/handle/10251/8596/PFC%20-%20Miguel%20Iniesta%20Archidona.pdf, Fecha de consulta Marzo de 2013.

[31] Pablo Jara Werchau, *Estándar IEEE 802.11 X De Las WLAN*, Editorial de la Universidad Tecnológica Nacional – edUTecNe, http://www.edutecne.utn.edu.ar/monografias/standard_802_11.pdf, Fecha de consulta Marzo de 2013.

[32] Pedro Pablo Fábrega Martínez, *Seguridad En Redes Inalámbricas una Guía Básica*, http://dns.bdat.net/seguridad_en_redes_inalambricas/, Fecha de consulta Junio de 2013.

[33] Ricardo Alberto Andrade, *TECNOLOGÍA Wi-Fi*, http://www.cnc.gov.ar/publicaciones/N5_WI-FI.pdf, Fecha de consulta Junio de 2013.

[34] Roberto Hernando, *Seguridad en redes inalámbricas*, http://www.rhernando.net , Fecha de consulta Diciembre de 2012.

[35] Saulo Barajas, *Mecanismos De Seguridad En Redes WLAN*, Universidad Carlos III de Madrid, http://dspace.ups.edu.ec/bitstream/123456789/217/3/Capitulo%202.pdf, Fecha de consulta Junio de 2013.

[36] Wilac, *Seguridad en Redes inalámbricas*, http://www.wilac.net, Fecha de consulta Noviembre de 2012.