UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

TECNICAS DE ENCRIPTAMIENTO PARA LA SEGURIDAD EN EL ACCESO INALAMBRICO EN UNA RED CORPORATIVA

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

LUIS ALBERTO CABALLERO PACHECO

PROMOCIÓN
2004 - I

LIMA – PERÚ
2010

TÉCNICAS DE ENCRIPTAMIENTO PARA LA SEGURIDAD EN EL ACCESO INALAMBRICO EN UNA RED CORPORATIVA

DEDICATORIA

Lo dedico a mis Padres por su cariño, comprensión y esfuerzo durante todos estos años, a mi hermana mayor y su esposo, por su apoyo constante, y a mi nueva familia por la fuerza que me brindan para superarme.

SUMARIO

El presente trabajo describe, las distintas técnicas de cifrado o encriptamiento presentes en el sector de las tecnologías de la información utilizadas hoy en día para proteger la información de una empresa, estas se pueden utilizar en distintas aplicaciones, en este caso nos concentraremos en la problemática de brindar seguridad al acceso LAN inalámbrico para una empresa que cuenta con varios locales en el mundo y desea obtener una solución corporativa a su acceso inalámbrico que sea flexible y robusta a la vez, flexible en el sentido que la misma configuración de acceso inalámbrico sirva en cualquier local de la empresa y robusta en el sentido que no pueda ser acezada por personal externo sin que la empresa les brinde los permisos.

En el desarrollo de esta solución describiremos los métodos de encriptación más populares, brindando más detalle al método de encriptación utilizado para esta solución en cual se llama AES por sus siglas en ingles **Advanced Encryption Standard** (**AES**) o también conocido como **Rijndael**, también describiremos el método de autenticación que hace que aumente la seguridad.

El diseño de la red inalámbrica también se describirá en el presente documento como parte final de la implementación realizada en uno de los locales de la empresa.

ÍNDICE

INTRODUCCIÓN

La necesidad de las empresas de utilizar cada vez más los accesos inalámbricos para conectarse a la red LAN a través de distintos dispositivos móviles como laptop, celulares 3G o 4G, o los famosos tablets muy utilizados hoy en día por personal administrativo para sus reuniones, nos obliga a brindar acceso móvil, flexible y seguro dentro de una red corporativa. Para este propósito, se deben utilizar las técnicas de cifrado para brindar seguridad a estas redes.

En la actualidad se puede observar que hay una gama de soluciones que ofrece el mercado para brindar seguridad a los accesos inalámbricos, en este sentido este trabajo se basa específicamente en las técnicas de encriptación o cifrado y en el método de autenticación, que harán que nuestro acceso inalámbrico sea imposible de ser vulnerado por un intruso malintencionado.

Los métodos de cifrado son muy utilizados en el sector de las telecomunicaciones y de las tecnologías de la información. Como por ejemplo en los enlaces VPN (Virtual Private Network), en donde son utilizados para cifrar la información que se intercambiara entre equipos de comunicaciones. Así también en el cifrado de dispositivos de almacenamiento, estos pueden ser USB y discos duros internos o externos.

Como se puede observar el campo de aplicación de estas técnicas de cifrado es amplio y el objetivo de este documento es describir uno de estos.

CAPITULO I
PLANTEAMIENTO DE INGENIERÍA

1.1 Descripción del problema

La problemática nace debido a que cada vez es mayor el personal administrativo que utiliza dispositivos móviles (laptop y Smartphone) para su labor diaria en una empresa, la cual consta de tres locales separados físicamente. Se supone que el personal se moviliza por los tres locales ubicados en diferentes localidades del Perú y se tiene problemas de configuración de red, estabilidad en la red inalámbrica y sobre todo problemas de seguridad ya que se utiliza métodos de encriptación (como WEP) con autenticación por clave compartida que en la actualidad son vulnerables. Al ser estas medidas de seguridad obsoletas y siendo el acceso inalámbrico de gran importancia en la labor diaria del personal administrativo, la empresa opto en buscar una solución que sea móvil, flexible, sencilla y segura. Móvil en el sentido que no tenga problemas de conexión en cualquier lugar del local, Flexible en el sentido que pueda desplazarse por los 3 locales que tiene en Perú y se conecte de la misma manera, Sencilla en el sentido que no sea un problema para el usuario final conectarse a la red inalámbrica y que solo necesite configurar una sola vez las características de la red inalámbrica para que se pueda conectar en cualquier sede, y Segura en el sentido que la información va a viajar cifrada y la clave utilizada en el método de autenticación cambie cada cierto tiempo.

1.1.1 Requerimientos solicitados por la Empresa

Los requerimientos solicitados para esta implementación son:

- Movilidad
- Flexibilidad
- Sencillez
- Seguridad

Así también se debe tomar en cuenta la vigencia en el tiempo de la solución brindada, debido a que la tecnología avanza y con estos la capacidad de procesamiento, por lo tanto aumentara la capacidad para encontrar la clave de cifrado utilizando el

método de la fuerza bruta, por tal motivo el presente documento tiene una vigencia en el tiempo de 3 a 5 años que es el tiempo en que cambia la tecnología. En este panorama se detallan los requerimientos solicitados por la empresa, para la implementación del acceso a la red con seguridad basada en encriptamiento.

a) Movilidad

Este requerimiento indica que el usuario final pueda moverse por todo el local ya sea este un edificio o un campus y nunca se desconecte de la red, como se muestra en la Figura 1.1, esto se consigue aplicando roaming de capa dos.

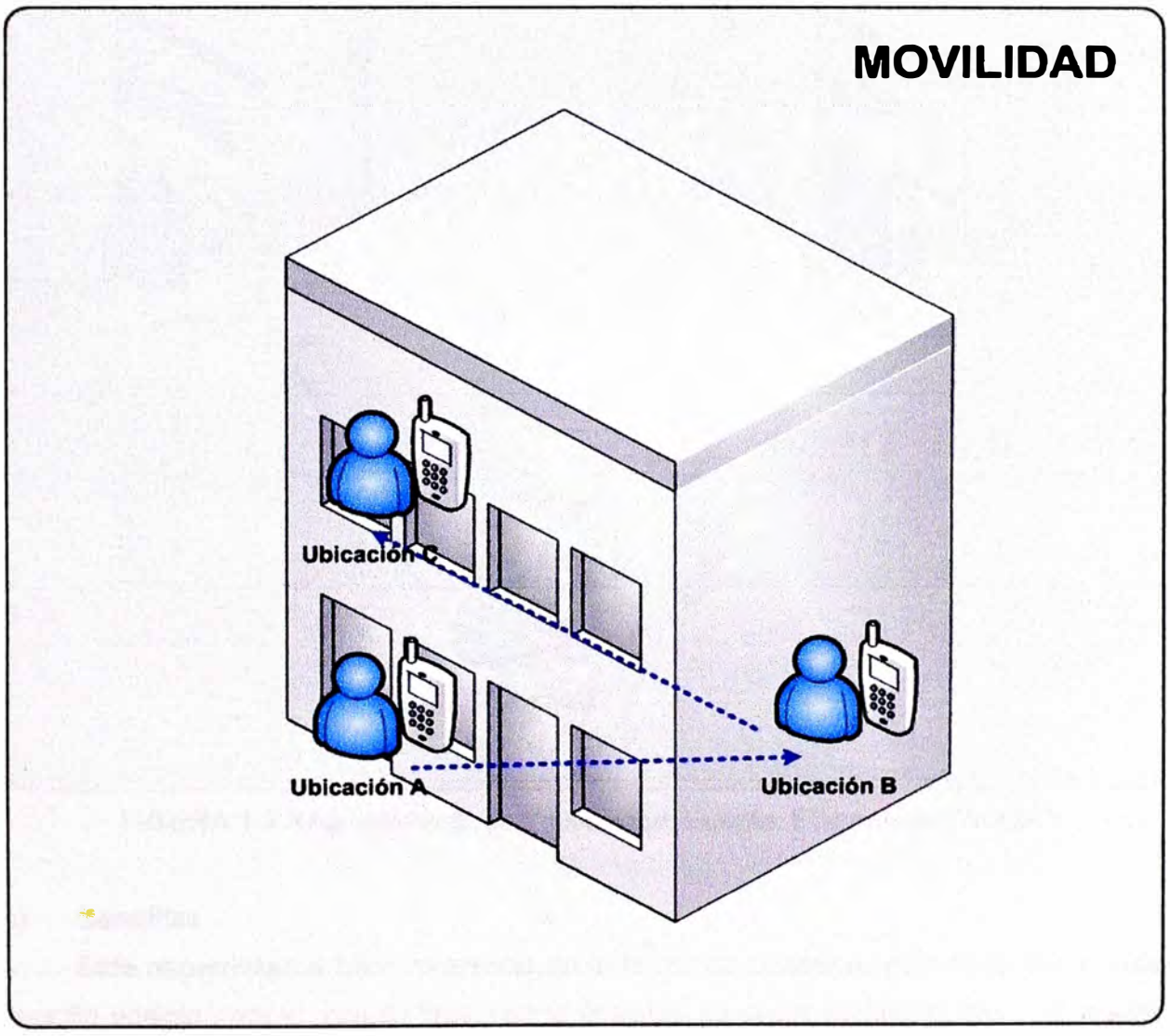

FIGURA 1.1 Requerimiento de Movilidad. Fuente: Elaboración Propia.

b) Flexibilidad

Este requerimiento indica que el usuario final pueda trabajar en cualquier sede de la empresa con la misma configuración de la interface inalámbrica, sin problemas de

conexión y sin la necesidad que un soporte tenga que configurar el acceso por cada local, ya que este proceso para el usuario final es burocrático y tedioso, lo cual generaría en un fastidio y una frustración.

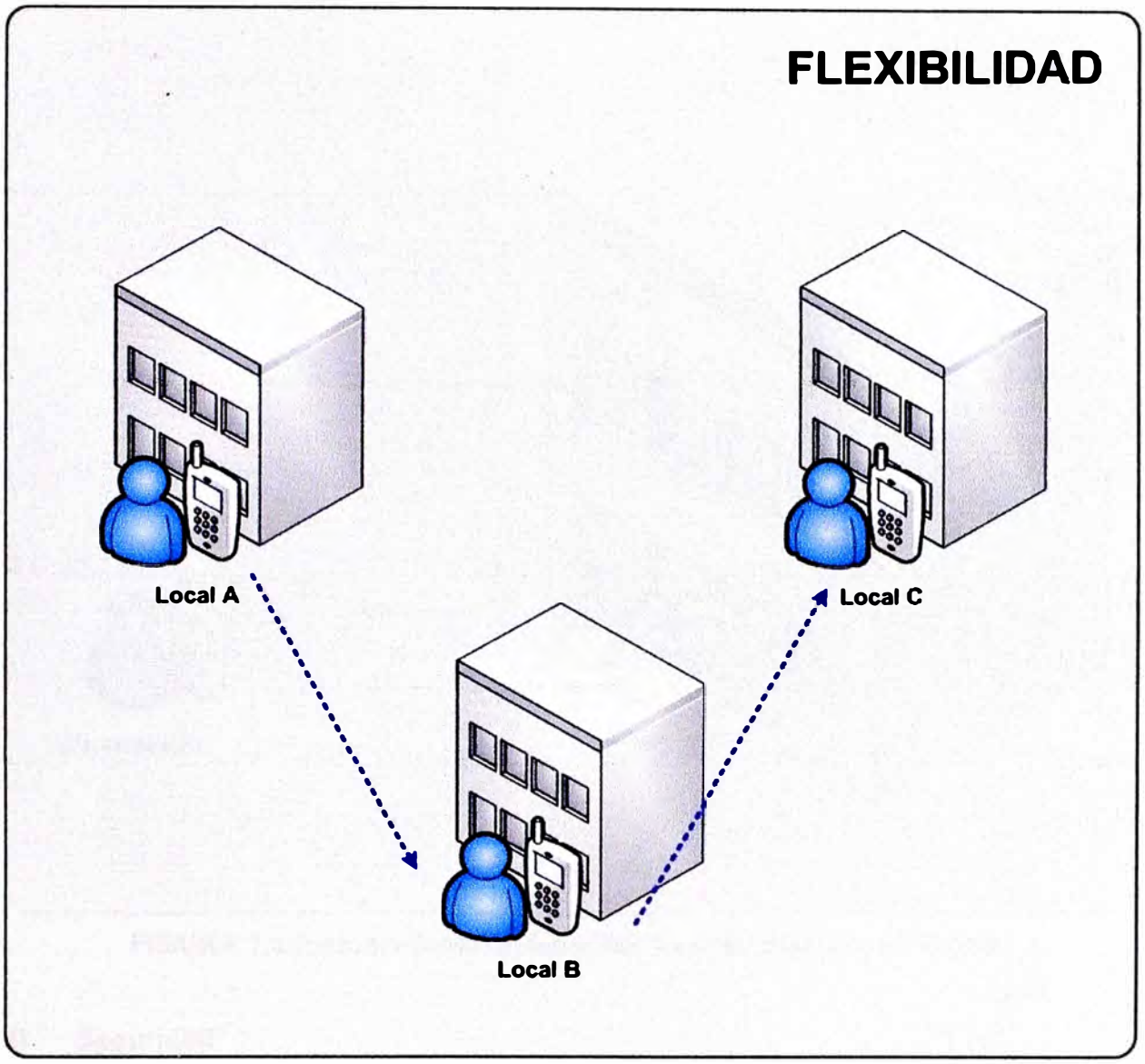

FIGURA 1.2 Requerimiento de Flexibilidad. Fuente: Elaboración Propia.

c) Sencillez

Este requerimiento hace referencia en la forma de conexión, esta debe ser lo más sencilla posible para el usuario final, con la finalidad de pasar desapercibido y no afecte sus labores diarias, como se ilustra en la Figura 1.3.

En esta figura se observa que cuando el usuario ingresa a un local de la empresa, la conexión del equipo móvil es brindada automáticamente, este requisito beneficia al usuario el no tener que estar ingresando una clave de acceso cada vez que desee ingresar a la red inalámbrica.

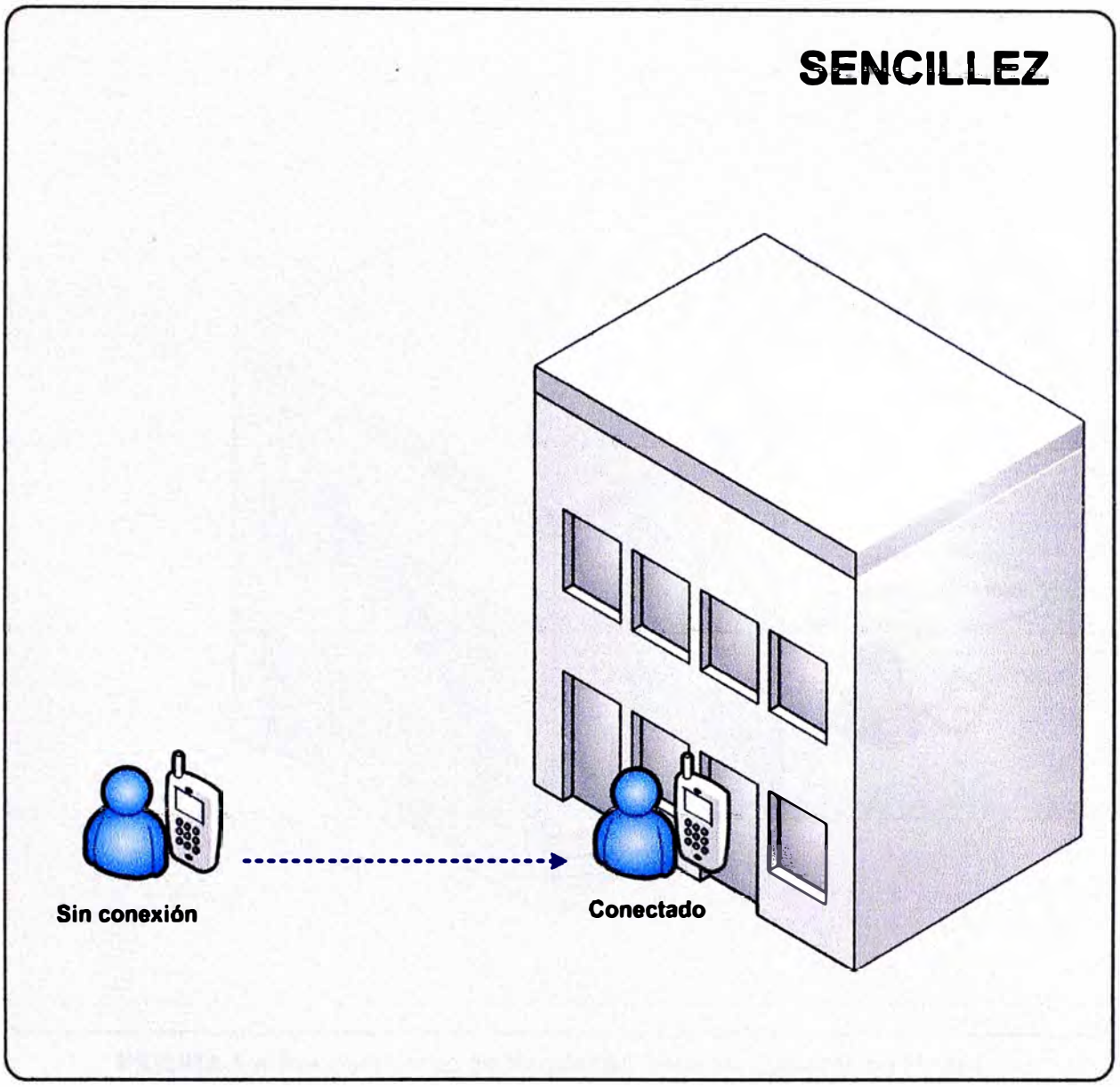

FIGURA 1.3 Requerimiento de Sencillez. Fuente: Elaboración Propia.

d) Seguridad

En los inicios de este tipo de redes se utilizaba un acceso abierto, debido a este motivo cualquier persona dentro del radio de alcance del equipo de acceso podía acceder a sus servicios libremente, y de esta manera podría realizar actos ilícitos como robo de información.

Al observar este problema las empresas comenzaron a utilizar el primer algoritmo de cifrado publicado por la IEEE, conocido como WEP (Wired Equivalent Privacy), para su tiempo este fue una solución viable, pero en la actualidad se ha desarrollado software que puede determinar la clave y por lo tanto este método no es seguro para una empresa. Sin embargo en la actualidad todavía se usa en los hogares, a pesar de ser un método obsoleto y no recomendable.

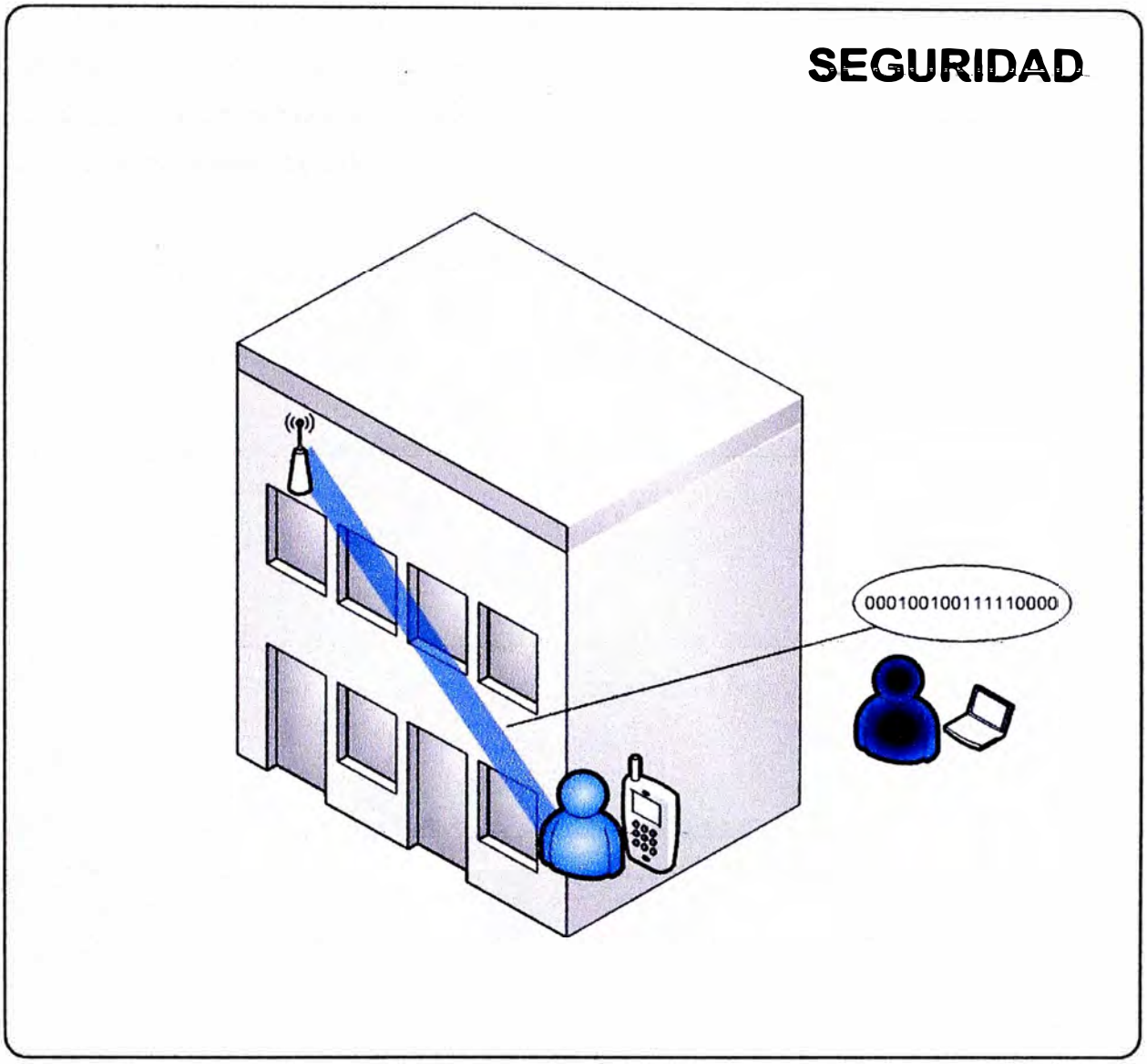

FIGURA 1.4 Requerimiento de Seguridad. Fuente: Elaboración Propia.

1.2 Evaluación del problema

1.2.1 Evaluación del problema de acceso inalámbrico

En función a los requerimientos establecidos en la sección anterior, se constituye el problema de brindar seguridad al acceso inalámbrico a la red de una empresa, la cual tiene tres locales ubicados en diferentes puntos del Perú. Para este propósito es posible utilizar los métodos de encriptación WEP, WPA-PSK, WPA-ENTERPRISE, WPA2-PSK y WPA2-ENTERPRISE.

Para esta propuesta de solución del problema, se plantea el escenario de comunicaciones donde se tiene un invitado que desea un acceso a la red de internet, al ser este un invitado podría contener algún tipo de virus electrónico en su equipo y se opto por brindarle un acceso inalámbrico restringido con solo acceso a internet pero sin acceso a la red corporativa.

Con la finalidad de brindar este acceso se establece una política de seguridad basada en técnicas de encriptamiento, tal como el AES (Advanced Encryptation Standard), el cual permite implementar redes seguras tanto para el usuario corporativo como para el usuario invitado.

CAPITULO II
MARCO TEÓRICO CONCEPTUAL

2.1 LAN Inalámbricas

La tecnología inalámbrica nace al ser los usuarios cada vez más móviles y al querer estos seguir accediendo a los recursos ofrecidos por sus centros de labores, en este sentido se crearon varias tecnologías inalámbricas que ofrecen estos servicios y se clasifican dependiendo del área de cobertura, estas pueden ser GSM, CDMA para áreas extensas, Wi-Max para áreas metropolitanas, Wi-Fi para área local y Bluetooth para área personal, como ilustra la Figura 2.1. Estas tecnologías ofrecen acceso móvil al usuario final, para nuestro caso explicaremos los fundamentos del acceso inalámbrico llamado Wi-Fi basándonos en el estándar de la IEEE 802.11.

Entre los principales estándares para redes inalámbricas se encuentran: IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11g y IEEE 802.11n (nuevo).

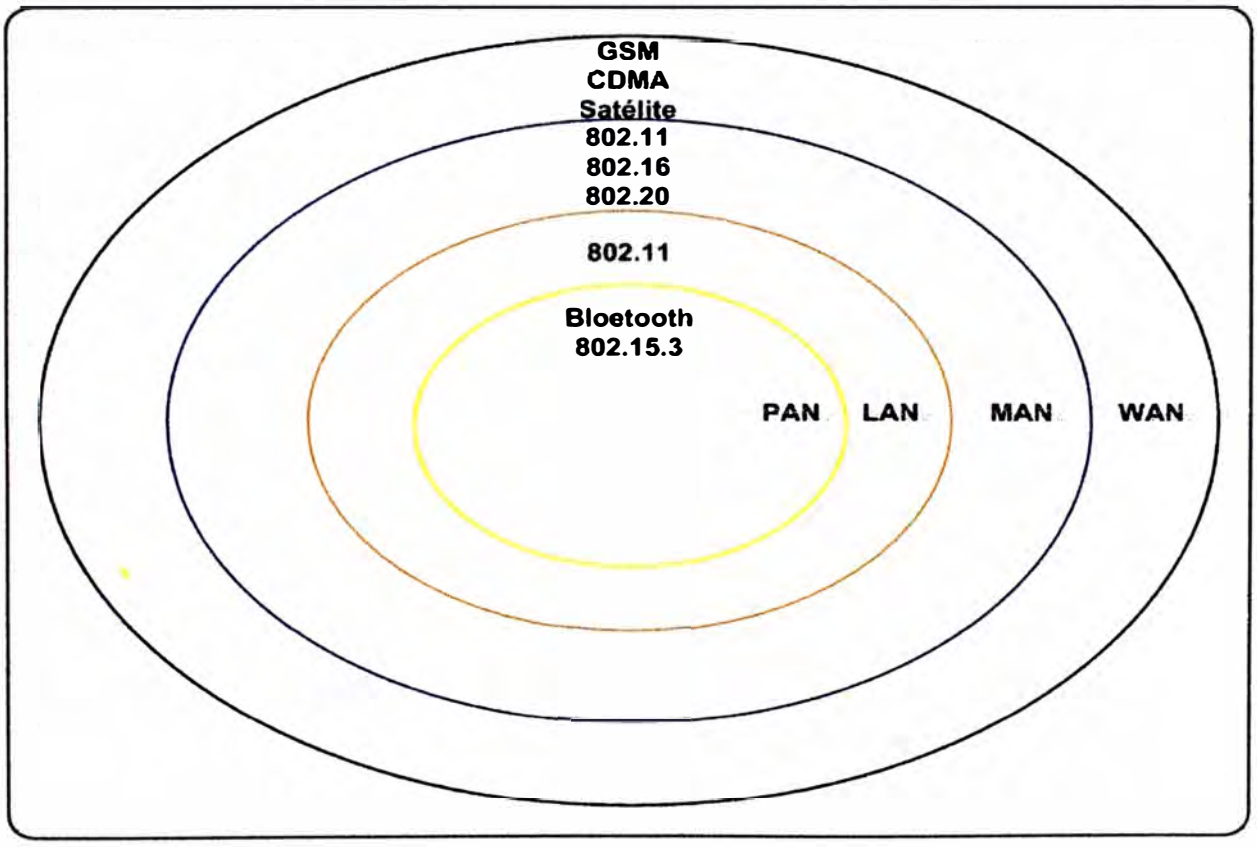

FIGURA 2.1 Tecnologías Inalámbricas. Fuente: Elaboración Propia.

2.1.1 Estándares publicados por la IEEE

Los estándares publicados por la IEEE han ido evolucionando para conseguir una mayor tasa de transferencia, menor interferencia y un mayor alcance. A continuación se explican los estándares publicados por la IEEE.

a) Estándar IEEE 802.11

Es el estándar original, publicado en 1997, especificaba dos tasas de transmisión a 1 y 2 Mbps utilizando señales infrarrojas o en la banda de frecuencia ISM (Industrial Scientic Medical) a 2.4 GHz, y utilizando los métodos de modulación FHSS y DSSS. Un problema de éste estándar es que ofrecía tantas opciones que hacía difícil garantizar la interoperabilidad, de manera que se dejaba bastante libertad a los fabricantes, por lo que fue rápidamente superado por el 802.11b.

b) Estándar IEEE 802.11b

El estándar 802.11b fue aprobado en 1999, permitiendo una tasa de transmisión máxima de 11 Mbps, utilizando el mismo método de acceso al medio que el 802.11. En la práctica no era posible superar los 6 Mbps con TCP (Transmission Control Protocol) y los 7 Mbps con UDP (User Datagrama Protocol). Los primeros equipos aparecieron muy rápidamente, ya que era una extensión a una modulación DSSS (Direct-Sequence Spread Spectrum) del estándar original. El aumento de velocidad y el reducido costo consiguieron un rápido crecimiento de la demanda y oferta. El protocolo se puede utilizar en topologías punto-a-multipunto (las más habituales) o punto-a-punto, con enlaces con distancias proporcionales a las características de las antenas y potencia utilizada. Además, si existen problemas de calidad de señal, es posible transmitir a 5.5, 2 y 1 Mbps, que utilizan métodos más redundantes de codificación de datos. El estándar divide el espectro en 14 canales que se traslapan, a una distancia de 5 Mhz cada uno de ellos, Esto provoca que cada canal interfiera con los dos adyacentes a cada lado, ya que el ancho de banda es 22 Mhz, a partir de donde la señal cae 30 dB como mínimo. Es por ello que se recomienda optar por los canales disjuntos (ej. canales 1,6 ó 11), que no representan traslapes especiales, produciéndose interferencias mínimas.

Los canales disponibles en cada país difieren de acuerdo a la reglamentación del mismo. Así, mientras en los Estados Unidos hay 11 canales disponibles, en Europa se disponen de 13 y en Japón 14, en Perú utilizamos 11 canales disponibles como se ilustra en la Figura 2.2. Este fue el estándar que recibió el nombre o denominación de Wi-Fi debido a su gran acogida en el mercado, siendo actualmente utilizado en conjunto con el estándar 802.11g.

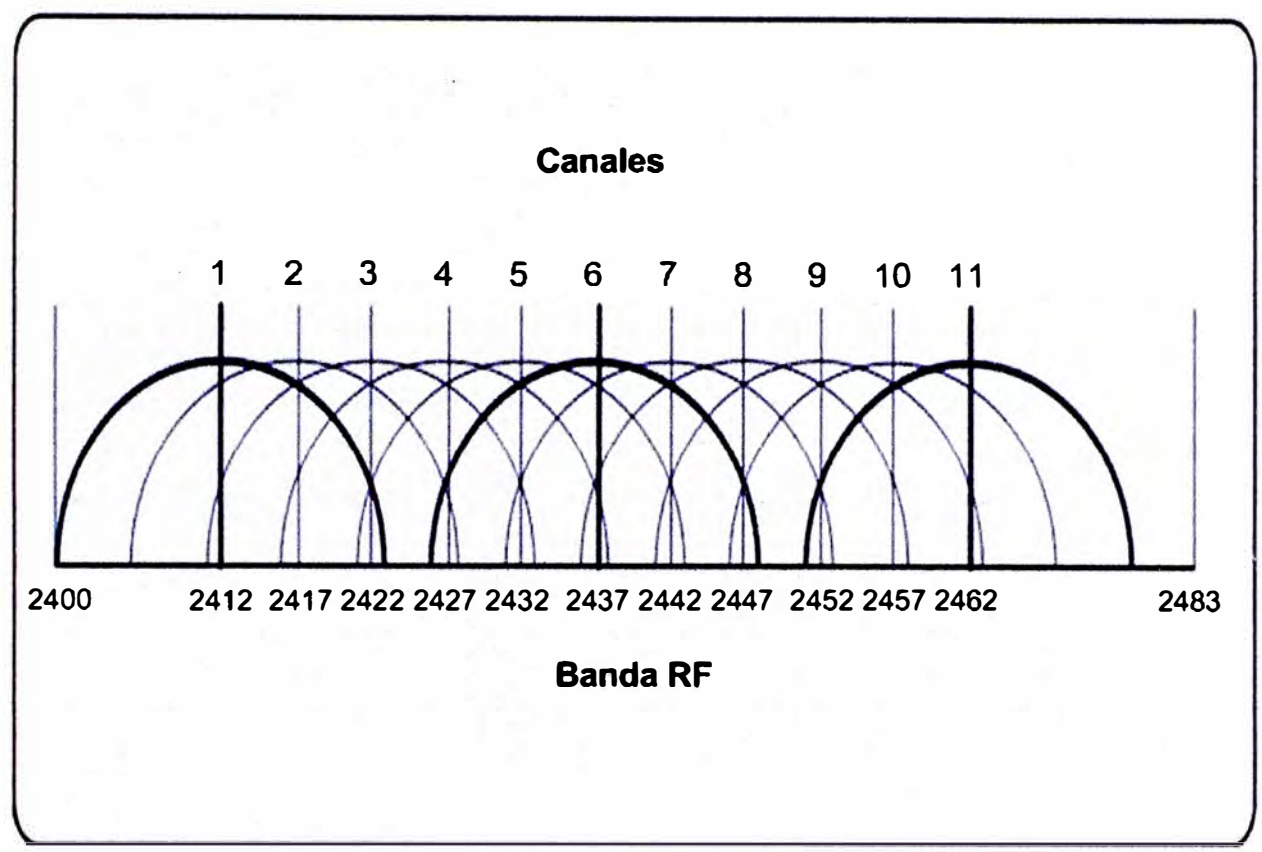

FIGURA 2.2 Banda RF de 2.4GHz. Fuente: Elaboración Propia.

c) Estándar IEEE 802.11a

El estándar fue aprobado en 1999. Se basa en el estándar original, operando en la banda de 5 Ghz, pero utilizando la técnica OFDM (Orthogonal Frequency Division Multiplexing) de modulación con 52 canales, alcanzando tasas de transmisión de hasta 54 Mbps, que se pueden corresponder con un rendimiento real de 20 Mbps. De forma similar al estándar 802.11b, la tasa se puede reducir a 48, 36, 24, 18, 12 , 9 y 6 Mbps. El estándar dispone de 12 canales no traslapados (ver Tabla 2.1). Utilizar la banda de 5 GHz permite disponer de menos interferencias, pero condiciona las instalaciones a disponer de línea de vista, además de tener una mayor absorción. En un primer momento fue utilizado en Estados Unidos y Japón, sin obtener licencia para operar en Europa, que en ese momento optaba por apostar por el estándar Hiperlan, hasta que en 2003 fue admitido. De las 52 subportadoras, 48 se utilizan para datos y cuatro actúan como pilotos, con una separación de 312.5 Khz. Cada subportadora puede ser BPSK (Binary Phase Shift Keying), QPSK (Quaternary Phase Shift Keying), 16 QAM (Quadrature Amplitud Modulation) o 64 QAM. La duración del símbolo es de 4 microsegundos, con un periodo de guardia de 0.8 microsegundos. Esta tecnología no fue tan adoptada como la basada en el 802.11b, ya que tenía un rango menor y estaba limitada en Europa. Hoy en día está ganando aceptación al existir intervalos duales.

Tabla 2.1 RF 802.11a. Fuente: Elaboración Propia.

Identificador de Canal	Frecuencia en MHz	Dominios Reguladores			
		América (-A)	EMEA (-E)	Israel (-I)	Japón (-J)
34	5170	–	–	–	–
36	5180	x	x	x	–
38	5190	–	–	–	–
40	5200	x	x	x	–
42	5210	–	–	–	–
44	5220	x	x	x	–
46	5230	–	–	–	–
48	5240	x	x	x	–
52	5260	x	–	–	x
56	5280	x	–	–	x
60	5300	x	–	–	x
64	5320	x	–	–	x
149	5745	–	–	–	–
153	5765	–	–	–	–
157	5785	–	–	–	–
161	5805	–	–	–	–

d) Estándar IEEE 802.11g

En Junio de 2003 se aprobó el tercer estándar, el 802.11g. Este estándar funciona en la banda de los 2.4 Ghz, como el 802.11b, pero con una tasa máxima de 54 Mbps (y efectiva de 24.7 Mbps). Es compatible con el 802.11b y utiliza las mismas frecuencias. El 802.11g logra tasas de datos superiores en esa banda mediante la técnica de modulación OFDM. IEEE 802.11g también especifica la utilización de DSSS para la compatibilidad retrospectiva de los sistemas IEEE 802.11b. El DSSS admite tasas de datos de 1; 2; 5,5 y 11 Mb/s, como también las tasas de datos OFDM de 6; 9; 12; 18; 24; 48 y 54 Mb/s.

Existen ventajas en la utilización de la banda de 2.4 GHz. Los dispositivos en la banda de 2.4 GHz tendrán mejor alcance que aquellos en la banda de 5 GHz. Además, las transmisiones en esta banda no se obstruyen fácilmente como en 802.11a.

Hay una desventaja importante al utilizar la banda de 2.4 GHz. Muchos dispositivos de clientes también utilizan la banda de 2.4 GHz y provocan que los dispositivos 802.11b y g tiendan a tener interferencia.

e) Estándar IEEE 802.11n

Este es el último estándar aprobado por la IEEE el 11 Setiembre del 2009 y fue creado para aumentar la capacidad de transmisión a más de 200 Mbps en el aire y 100 Mbps en la capa de acceso, el método de modulación utilizado en la capa física es el denominado MIMO (Multiple-Input Multiple-Output), la tecnología MIMO depende de

señales multiruta. Las señales multiruta son señales reflejadas que llegan al receptor un tiempo después de que la señal con línea de vista (LOS - line of sight) ha sido recibida. En una red no basada en MIMO, como son las redes 802.11a/b/g, las señales multiruta son percibidas como interferencia que degradan la habilidad del receptor de recobrar el mensaje en la señal. MIMO utiliza la diversidad de las señales multirutas para incrementar la habilidad de un receptor de recobrar los mensajes de la señal.

Para un mayor entendimiento de los estándares explicados en este capítulo se muestra un cuadro comparativo en la Tabla 2.2, el cual resume los métodos de modulación de la capa física, las tasas de transferencias y los años de publicación.

Tabla 2.2 Cuadro comparativo IEEE 802.11. Fuente: Elaboración Propia.

Estándar	Año ratificado	Banda RF	Modulación	Velocidad de Datos	Canal
802.11	1997	2.4GHz	FHSS o DSSS	1 o 2Mbps	20MHz
802.11a	1999	5GHz	OFDM	Hasta 54Mbps	20MHz
802.11b	1999	2.4GHz	HR-DSSS	Hasta 11Mbps	20MHZ
802.11g	2003	2.4GHz	OFDM y DSSS	Hasta 54Mbps	20MHZ
802.11n	2009	2.4GHz o 5GHz	MIMO	+ de 200Mbps	20 o 40MHZ

2.1.2 Componentes de la Arquitectura 802.11

En lo que se refiere a la arquitectura o topología en una red inalámbrica existen tres tipos la primera llamada IBSS (Independent Basic Service Set) o red Ad Hoc en la cual dos equipos se pueden comunicar sin necesitar un punto de acceso, la segunda llamada BSS (Basic Service Set) en la cual los equipos utilizan un punto de acceso para comunicarse y la tercera ESS (Extended Service Set) que es el agrupamiento de 2 o más BSS.

También se puede indicar que una LAN 802.11 está basada en una arquitectura celular, es decir, el sistema está dividido en celdas, donde cada celda denominada BSS es controlada por una Estación Base llamada Punto de Acceso (AP Access Point), aunque también puede funcionar sin la misma en el caso que las máquinas se comuniquen entre ellas. Los Puntos de Acceso de las distintas celdas están conectados a través de algún tipo de red troncal llamado Sistema de Distribución (DS Distribution System). La LAN inalámbrica completamente interconectada, incluyendo las distintas celdas, los Puntos de Acceso y el Sistema de Distribución son denominadas en el estándar como un Conjunto de Servicio Extendido (Extended Service Set, ESS).

Así también las denominaciones del área de cobertura son diferentes dependiendo del tipo de topología utilizada, en el caso de ser la topología IBSS o BSS el área de cobertura se denomina área de servicio básica o BSA (Basic Service Area) y para el

caso de ser la topología ESS se denomina área de servicio extendida o ESA (Extended Service Area), la Figura2.3 resume los términos utilizados.

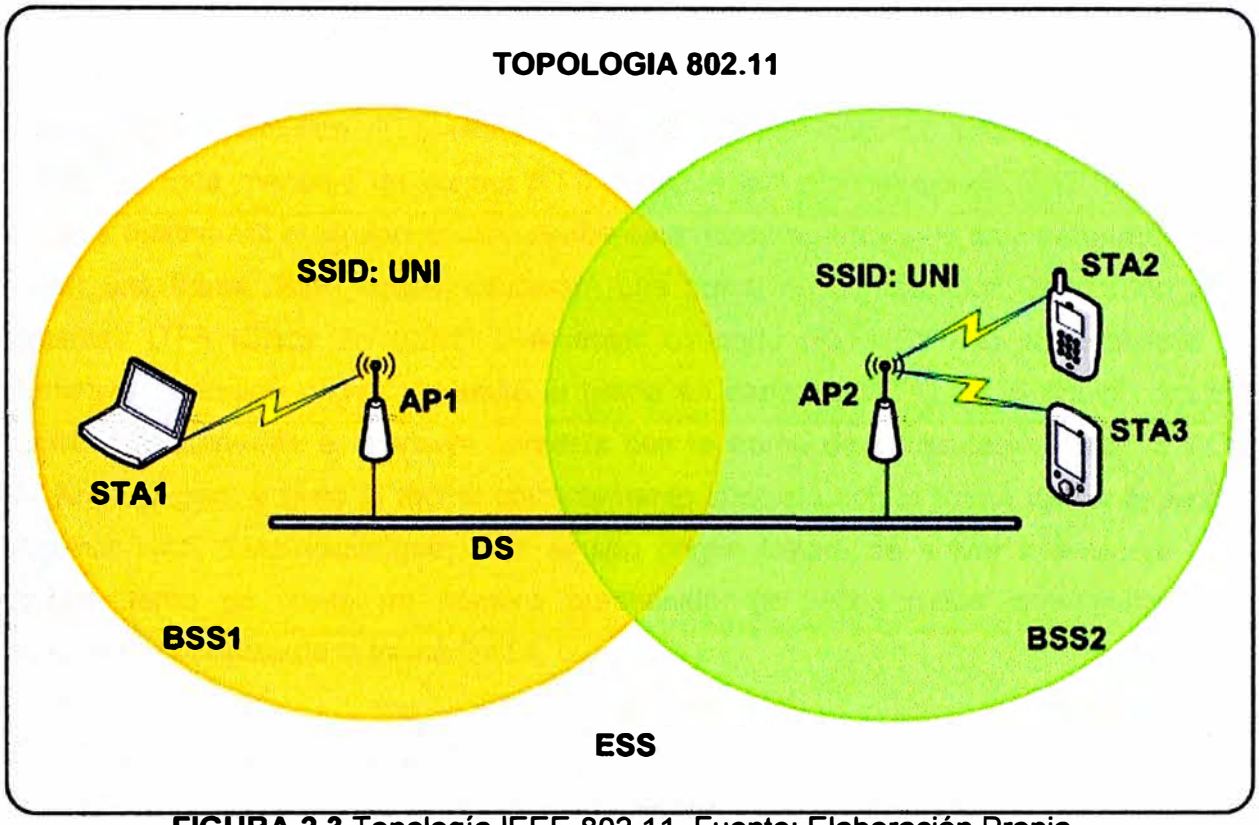

FIGURA 2.3 Topología IEEE 802.11. Fuente: Elaboración Propia.

2.1.3 Mecanismo de acceso al Medio

En wireless LAN el mecanismo utilizado es el conocido como Acceso Múltiple por Detección de Portadora con Evasión de Colisiones o CSMA/CA (Carrier Sense, Multiple Access, Collision Avoidance) es un protocolo de control de redes de capa 2 que permite que múltiples estaciones utilicen un mismo medio de transmisión. Cada equipo anuncia opcionalmente su intención de transmitir antes de hacerlo para evitar colisiones entre los paquetes de datos (comúnmente en redes inalámbricas, ya que estas no cuentan con un modo práctico para transmitir y recibir simultáneamente). De esta forma, el resto de equipos de la red sabrán cuando hay colisiones y en lugar de transmitir la trama en cuanto el medio está libre, se espera un tiempo aleatorio adicional corto y solamente si, tras ese corto intervalo el medio sigue libre, se procede a la transmisión reduciendo la probabilidad de colisiones en el canal. CSMA/CA es utilizada en canales en los que por su naturaleza no se puede usar CSMA/CD. CSMA/CA se utiliza en 802.11 basada en redes inalámbricas.

Aunque el CSMA/CD y CSMA/CA aseguren que un nodo va a obtener un acceso al medio no se asegura que el nodo destino esté en contacto con el nodo origen. Para

solucionar este problema se ha añadido un procedimiento de saludo adicional al protocolo de la capa MAC. Este procedimiento se ha denominado protocolo de MAC inalámbrico de fundamento distribuido (DFW MAC) con el objetivo de que sirva para los diferentes métodos de la capa MAC.

Para enviar una trama, el equipo origen primero envía una trama corta de control de solicitud de transmisión RTS (Request To Send) mediante el método CSMA/CD o CSMA/CA Este mensaje de control RTS contiene las direcciones de MAC del equipo origen y destino. Si el equipo destino recibe esta trama significa que está preparado para recibir una trama. Este equipo devolverá una trama de contestación: preparado para transmitir CTS (Clear To Send) o receptor ocupado (RxBUSY). Si la respuesta es afirmativa el equipo origen transmite la trama en espera (DATA). Si el equipo destino recibe correctamente el mensaje contesta con la trama de confirmación positiva ACK (ACKnowledged) y si no la recibe correctamente contesta con la trama de confirmación negativa NAK (NAKnowledged) y el equipo origen tratará de volver a enviarlo. Este procedimiento se repite un número predefinido de veces hasta conseguirse una transmisión correcta de la trama DATA.

a) Formato de la trama MAC

La subcapa MAC se encuentra en la capa de enlace del modelo OSI (ver Figura2.4), encima de ella se encuentra la subcapa LLC (Logical Link Control) y esta hace de intermediaria con las capas superiores, este documento solamente hará mención a la sub capa MAC.

Las tramas MAC se pueden clasificar según tres tipos:

- **Tramas de datos**
- **Tramas de control,**

Los ejemplos de tramas de este tipo son los reconocimientos ACKs, las tramas para multiacceso RTS y CTS, y las tramas libres de Contienda.

- **Tramas de gestión**

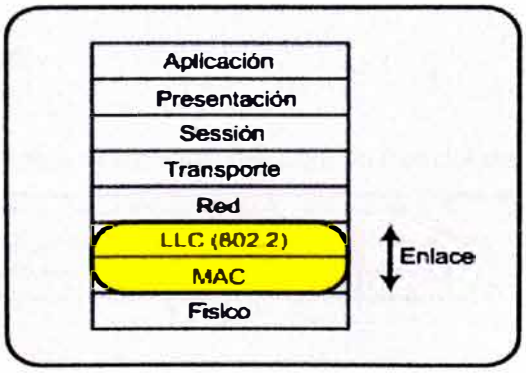

FIGURA 2.4 Modelo OSI. Fuente: Elaboración Propia

Como ejemplo podemos citar los diferentes servicios de distribución, como el servicio de Asociación, las tramas de Beacon o portadora y las tramas TIM o de tráfico pendiente en el punto de acceso.

En la Figura 2.5 se ilustra el formato y los capos de una trama MAC genérica.

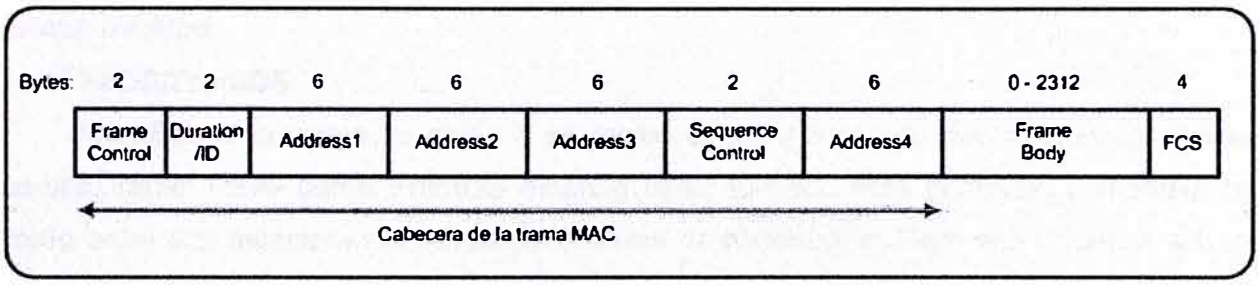

FIGURA 2.5 Trama MAC. Fuente: Elaboración Propia.

Los campos que componen esta trama son:

- **Frame Control**

  Es la trama de control se examinara más adelante con mayor detalle.

- **Duration/ID**

  En tramas del tipo PS o Power-Save para dispositivos con limitaciones de potencia, contiene el identificador o AID de estación. En el resto, se utiliza para indicar la duración del periodo que se ha reservado una estación.

- **Address1-4**

  Contiene direcciones de 48 bits donde se incluirán las direcciones de la estación que transmite, la que recibe, el punto de acceso origen y el punto de acceso destino.

- **Sequence Control**

  Es el Campo de control de Secuencia, contiene tanto el número de secuencia como el número de fragmento en la trama que se está enviando.

- **Frame Body**

  Es el cuerpo de la trama. Varía según el tipo de trama que se quiere enviar.

- **FCS**

  Contiene el checksum.

En la Figura 2.6 se ilustra el formato del campo control de trama.

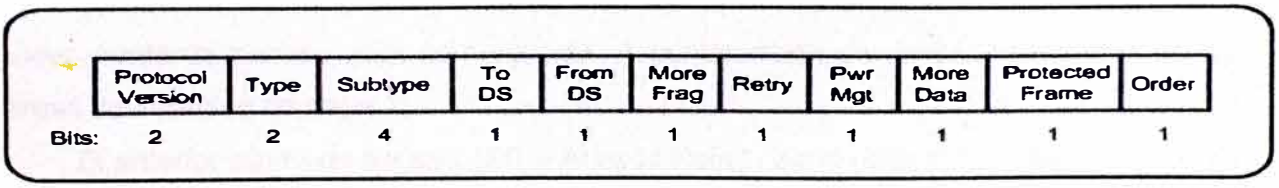

FIGURA 2.6 Campo Control de Trama. Fuente: Elaboración Propia.

- **Protocol Version**

  Es la versión del protocolo utilizado para este estándar el valor es 0.

- **Type/Subtype**

El Campo Type identifica uno de los tres tipos de trama, datos, control o gestión, y cada uno de estos tipos de trama tienen subtipos los cuales son identificados en el campo subtype.

- **ToDS/FromDS**

Identifica si la trama se envía o se recibe al/del sistema de distribución. En redes ad-hoc, tanto ToDS como FromDS están a cero. El caso más complejo contempla el envío entre dos estaciones a través del sistema de distribución. Para ello situamos a uno tanto ToDS como FromDS.

- **More Frag**

  Más fragmentos. Se activa si se usa fragmentación.

- **Retry**

  Se activa si la trama es una retransmisión.

- **Power Management**

  Se activa si la estación utiliza el modo de economía de potencia.

- **More Data**

  Se activa si la estación tiene tramas pendientes en un punto de acceso.

- **Protected Frame**

  Se activa si se usa el mecanismo de autenticación y encriptado.

- **Order**

  Se utiliza con el servicio de ordenamiento estricto.

2.2 Roaming de capa 2 en LANs Inalámbricas

El mecanismo para determinar cuándo realizan roaming no está definido por la especificación IEEE 802.11 y, por lo tanto, se ha dejado a los proveedores implementarlo. A pesar de este problema, que plantea un reto desde el principio de interoperabilidad, los proveedores han trabajado en conjunto para garantizar esta. El hecho de que estos mecanismos se deje a criterio de los proveedores hace que cada uno compita por el mejor algoritmo y por lo tanto los mantienen en forma confidencial.

El mecanismo de roaming incluye procesos que van más allá que solo encontrar un nuevo punto de acceso para comunicarse. A continuación se describen algunas de las tareas del roaming de capa 2:

- El anterior punto de acceso (AP – Access Point) debe determinar que el cliente se ha desplazado fuera de su alcance.

- El anterior punto de acceso debe almacenar temporalmente los datos destinados al cliente móvil en un búfer. [*]
- El nuevo AP debe indicar al anterior AP que el cliente móvil ha tenido éxito en su reconexión. Este paso suele ocurrir a través de un paquete unicast o multicast desde el nuevo AP al anterior AP con la dirección MAC de origen del cliente móvil. [*]
- El anterior AP debe enviar los datos almacenados en el búfer al nuevo punto de acceso.
- El nuevo AP debe actualizar las tablas de direcciones MAC en los switches de infraestructura para evitar la pérdida de datos al cliente móvil.

[*] Las tareas no son obligatorias, ya que no se especifican en el estándar 802.11.

Las Figuras 2.7 y 2.8 representan un cliente móvil que realiza roaming entre dos puntos de acceso. Los puntos de acceso están conectados a diferentes switches de Capa 2. En la Figura2.7, el servidor de aplicaciones envía datos al cliente con una dirección MAC A.B.C.D, el switch de capa 3 envía la trama con una dirección MAC de destino A.B.C.D al SW1 y este a su vez comprueba su tabla MAC y envía la trama al AP1.

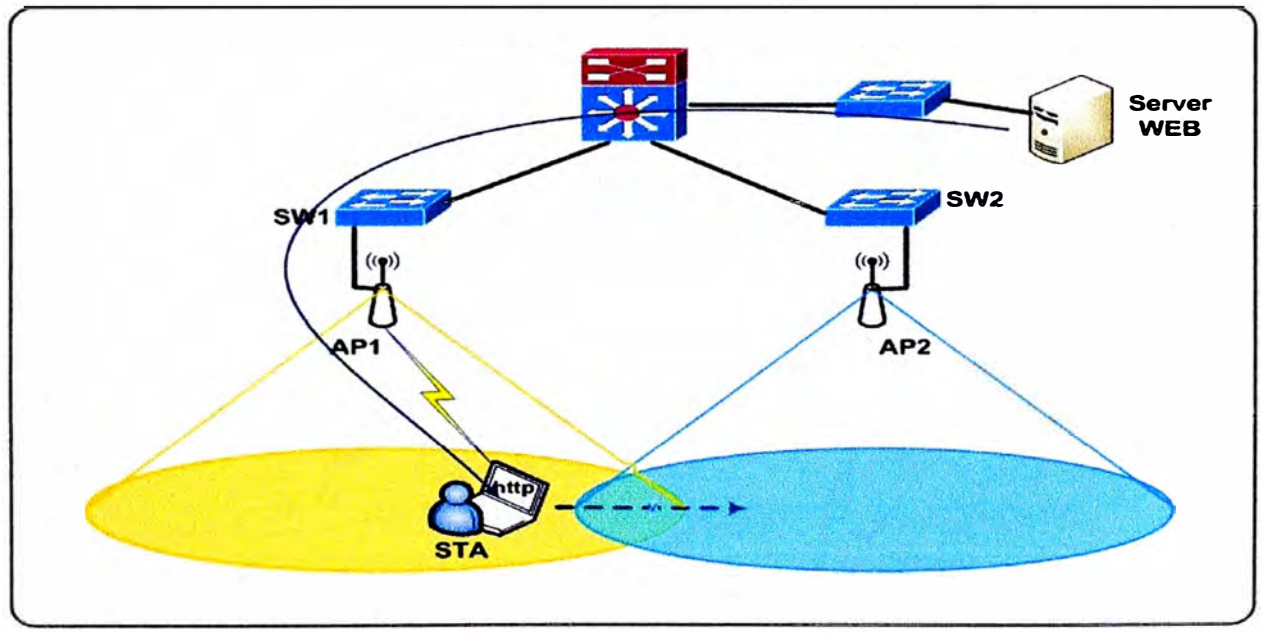

FIGURA 2.7 Ejemplo Roaming Capa 2. Fuente: Elaboración Propia.

En la Figura2.8, el cliente se ha desplazado al AP2 desde el AP1, pero el AP1 todavía no se ha enterado que el cliente se ha movido fuera de su alcance. El servidor de aplicaciones continúa enviando tramas a L3 (switch de capa 3) y este las sigue enviando al SW1, luego este último las envía al AP1 el cual intenta reenviárselas al cliente pero al

no recibir respuesta realiza el almacenamiento de las tramas en un búfer. El AP2 resuelve esta situación mediante el envío de un paquete al AP1 con la dirección MAC del cliente movil (STA), la Figura 2.9 ilustra cómo las actualizaciones de las tablas MAC en los switches de capa 2 hacen que el paquete se envíe al nuevo punto de acceso en este caso el AP2.

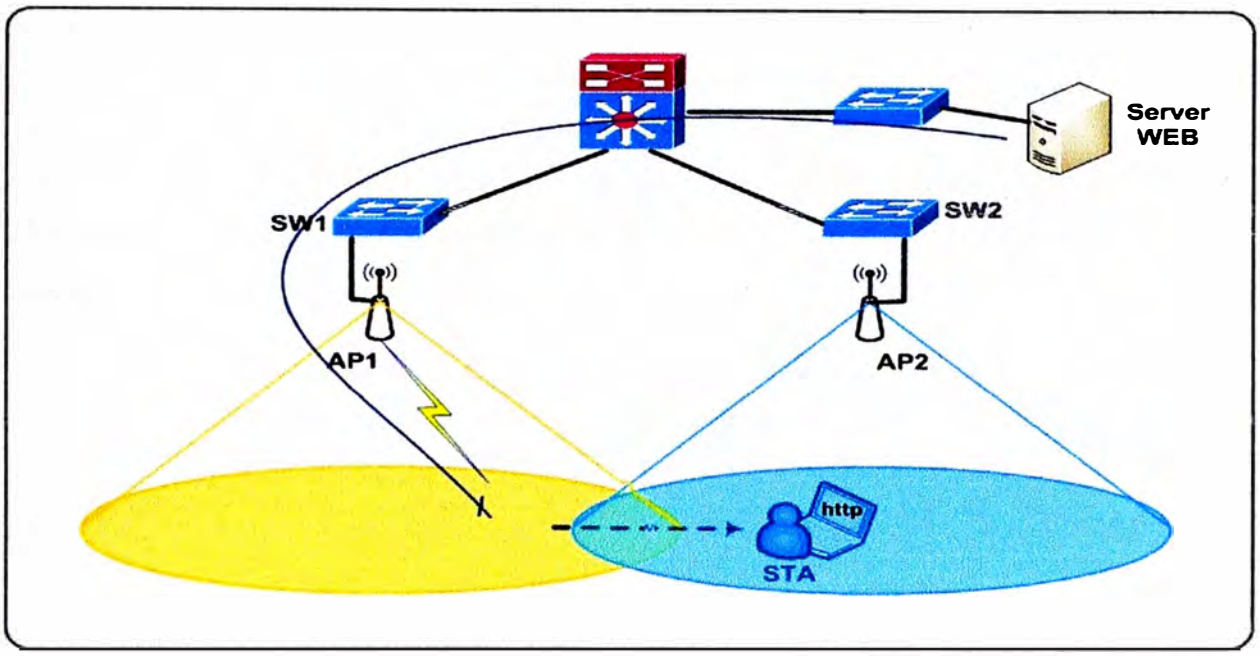

FIGURA 2.8 Ejemplo Roaming de Capa 2. Fuente: Elaboración Propia.

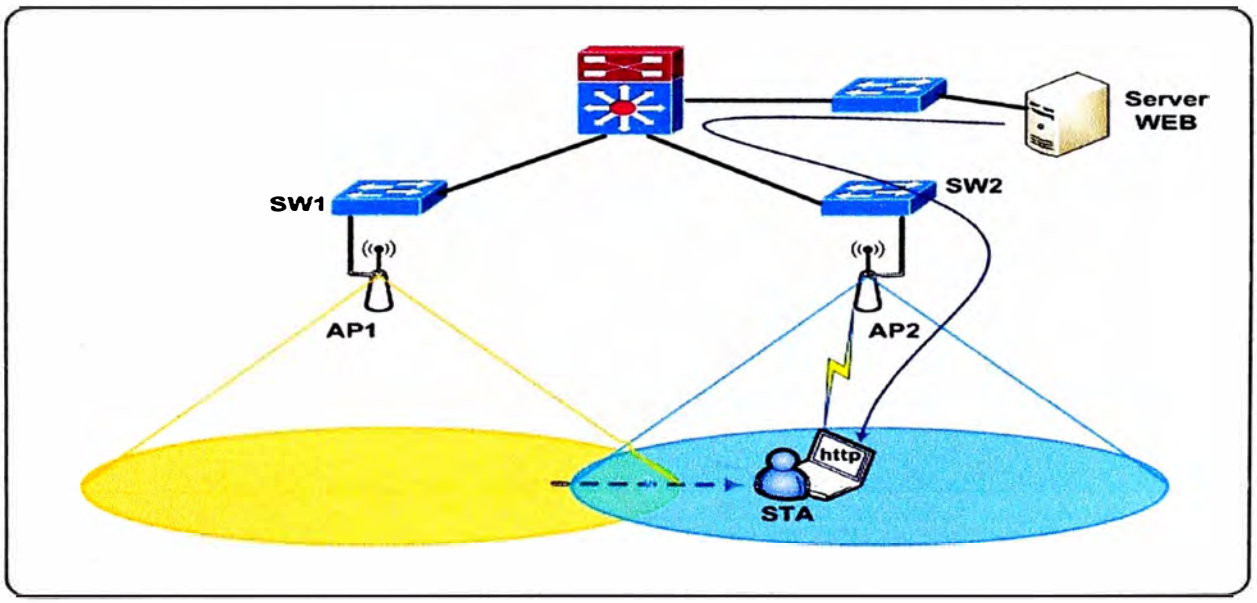

FIGURA 2.9 Ejemplo Roaming de Capa 2. Fuente: Elaboración Propia.

AP2 envía una trama con la dirección MAC del cliente al AP1. Se actualiza la tabla MAC del SW2, ya que ha recibido una nueva dirección MAC de un puerto de entrada. La

dirección de origen de la trama (la dirección MAC del cliente) se agrega a la tabla MAC y se asigna a la interfaz de entrada (es decir, la dirección MAC A.B.C.D se asigna al SW2). El conmutador L3 actualiza su tabla MAC para indicar que el destino es ahora accesible a través del SW2. El SW1 actualiza su tabla MAC de la misma manera. Las tramas de entrada para el cliente móvil son ahora correctamente transmitidas a través del SW2 y AP2. Debido a que el IEEE y el estándar 802.11 no se ocupa de la comunicación entre Access Point a través del sistema de distribución (las interfaces de cable en este caso), los proveedores de estos equipos aplican estos mecanismos por su cuenta. Dependiendo del proveedor, el mecanismo puede enviar una trama unicast o multicast con la MAC de origen la del cliente móvil y la MAC de destino la de los últimos AP, informando al anterior AP que el cliente se ha movido y de actualizar su tabla de direcciones MAC.

CAPITULO III
SEGURIDAD DE REDES INALAMBRICAS

Los métodos de seguridad en el Acceso inalámbrico son diversos desde el filtrado por MAC-address hasta el encriptamiento. En este trabajo, para la seguridad de acceso a una red inalámbrica se aplicara las técnicas de encriptamiento o cifrado basado en el estándar 802.11i, el cual hace uso del método de cifrado WPA2 basado en el algoritmo de encriptación AES.

Así También se analizara el método de autenticación basado en el estándar 802.1x, el cual hace uso del protocolo de autenticación PEAP (Protected Extensible Authentication Protocol).

3.1 Método de Encriptación AES

Rijndael es el método criptográfico que vino a substituir a DES (Data Encryption Standard) creado el 23 de noviembre de 1976, el cual era uno de los algoritmos más usados en el mundo, y que poco a poco fue desplazado por Rijndael. El surgimiento de Rijndael se da a inicios de 1997, cuando el National Institute of Standars and Technology (NIST) organiza un concurso para reemplazar al algoritmo de cifrado DES. Entre los requerimientos estaba que el nuevo algoritmo debería de soportar llaves de tamaño de 128, 192, y 256 bits, debería operar en bloques de 128 bits, también debería de poder trabajar en un gran variedad de hardware, por ejemplo, procesadores de 8-bits que puedan ser usados en tarjetas inteligentes (smart cards), en arquitecturas de 32 bits usadas comúnmente en computadoras personales, de igual manera fue importante la velocidad y la fortaleza criptográfica.

Los cinco finalistas resultantes fueron: MARS (IBM), RC6 (RSA), Rijndael (Joan Daemen y Vincent Rijmen),Serpent (Ross Anderson, Eli Biham, y Lars Knudsen), Twofish (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, y Niels Fergunson).

Finalmente, en octubre del 2002, NIST anuncio que el método criptográfico ganador de la competencia era Rijndael, a quien NIST lo renombro como AES (Advanced Encryption Standard).

3.1.1 Campos de Galoit

En esta sección se realiza una introducción a los campos de Gaoit o campos finitos en el cual se basa este algoritmo para realizar sus operaciones básicas como adición o suma y multiplicación. La ventaja de utilizar esta teoría es que se tiene un conjunto finito de números cuyo resultado de la suma y multiplicación también se encuentra en este campo finito de números. Para nuestro caso 256 números. Aquí también se puede realizar el inverso aditivo y el inverso multiplicativo y el resultado también se encontrara en este campo finito de números, logrando así el cifrado y descifrado.

3.1.2 Operaciones Matemáticas

Para implementar el algoritmo AES son utilizadas las operaciones básicas de suma y multiplicación sobre bytes.

Suma

La suma en el campo finito o Campo de Galoit GF(2^8) es definida a través del operador XOR (denotado por $\oplus$), es decir or exclusivo. A continuación se ilustra un ejemplo de la suma de 2 bytes 57 y 83:

$$\{01010111\} \oplus \{10000011\} = \{11010100\} \quad (3.1)$$

$$\{57\} \oplus \{83\} = \{d4\} \quad (3.2)$$

Multiplicación

La multiplicación (denotada por $\bullet$) en el campo finito o campo de Galoit GF(2^8) presenta una mayor complejidad matemática. A continuación se explicara la multiplicación de cualquier byte con el byte {02}. Para multiplicar el byte X por {02} se hace que este byte X se exprese en su forma binaria (8 bits) y se desplaza un bit a la izquierda, en seguida se agrega un cero a la derecha. Si el primer bit de la izquierda es 1 se realiza un XOR con el numero hexadecimal {01}{1B}, caso contrario este sería el resultado. A seguir, se presentan 2 ejemplos:

Ejemplo 1

$$\{57\}\bullet\{02\} = \{01010111\}\bullet\{00000010\} = \{0|10101110\} = \{ae\} \quad (3.3)$$

Ejemplo 2

$$\{83\}\bullet\{02\} = \{10000011\}\bullet\{00000010\} = \{1|00000110\} = \{01\}\{06\} \quad (3.4)$$

$$\{01\}\{06\} \oplus \{01\}\{1b\} = \{1|00000110\} \oplus \{1|00011011\} = \{0|00011101\} = \{1d\} \quad (3.5)$$

Una vez entendida la multiplicación por {02}, esta se convertirá en una función denominada "xtime(X)" donde X es un byte, utilizando el ejemplo 1, para realizar la operación de {57}•{02} es equivalente a usar la función xtime(57). Esta función se convertirá en la base para crear una función de multiplicación genérica tanto en software como en hardware. A continuación se realizara la operación de multiplicación {57}•{13} y se utiliza la propiedad distributiva del campo de galoit, tal como:

$$\{\mathbf{57}\}\bullet\{\mathbf{13}\} = \{\mathbf{57}\}\bullet(\{\mathbf{10}\}\oplus\{\mathbf{02}\}\oplus\{\mathbf{01}\}) \quad (3.6)$$

$$\{57\}\bullet\{13\} = (\{57\}\bullet\{10\}) \oplus (\{57\}\bullet\{02\})\oplus(\{57\}\bullet\{01\}) \quad (3.7)$$

Pero hay que tener en cuenta que:

$$\{02\}=\{02\} \quad (3.8)$$

$$\{04\}=\{02\}\bullet\{02\} \quad (3.9)$$

$$\{08\}=\{02\}\bullet\{02\}\bullet\{02\} \quad (3.10)$$

$$\{10\}=\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\} \quad (3.11)$$

$$\{20\}=\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\} \quad (3.12)$$

$$\{40\}=\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\} \quad (3.13)$$

$$\{80\}=\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\} \quad (3.14)$$

De esta manera se tiene:

$$\{57\}\bullet\{13\} = (\{57\}\bullet\{02\}\bullet\{02\}\bullet\{02\}\bullet\{02\}) \oplus (\{57\}\bullet\{02\}) \oplus \{57\} \quad (3.15)$$

A continuación se expresa la multiplicación en términos conocidos, por lo tanto se puede aplicar la función xtime() sucesivamente y obtenemos el resultado:

$$\{57\}\bullet\{13\} = \left(\text{xtime}\{\text{xtime}\left\{\text{xtime}\{\text{xtime}\{57\}\}\right\}\}\right) \oplus (\text{xtime}\{57\}) \oplus \{57\} \quad (3.16)$$

$$\{57\}\bullet\{13\} = \{07\} \oplus \{ae\} \oplus \{57\} \quad (3.17)$$

$$\{57\}\bullet\{13\}=\{fe\} \quad (3.18)$$

3.1.3 Algoritmo de Cifrado

Primeramente se debe decir que el método de cifrado AES es un caso particular del algoritmo de Rijndael, aquí analizaremos el método de cifrado para un texto plano de 128bits y claves de 128, 192 y 256 bits.

Siendo el objetivo de este algoritmo de cifrado codificar texto plano utilizando una clave y transformarlo a un texto cifrado (ver Figura 3.1), el análisis se centrara en explicar el funcionamiento del mismo utilizando técnicas matemáticas para la implementación en hardware y software.

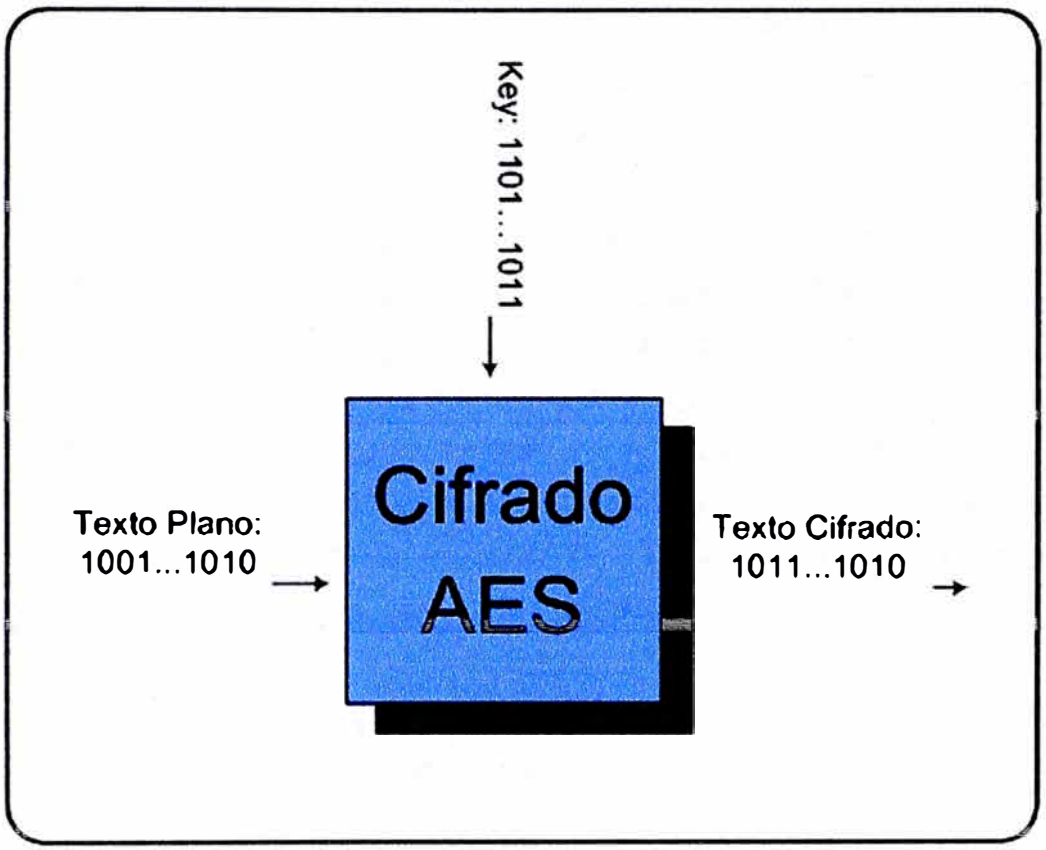

FIGURA 3.1 Modelo de Cifrado. Fuente: Elaboración Propia.

Inicialmente se da forma al texto de entrada al transformarlo en una matriz de bytes, los bloques de entrada están compuestos por 128bits de la siguiente manera:

$$input_0\, input_1\, input_2 \ldots input_{126}\, input_{127} \tag{3.19}$$

En seguida se definen bloques de 8 bits a las variables in_k:

$$in_0 = \{input_0, input_1, \ldots, Input_7\}; \tag{3.20}$$

$$in_1 = \{input_8, input_9, \ldots, Input_{15}\}; \tag{3.21}$$

$$\vdots$$

$$in_{15} = \{input_{120}, input_{121}, \ldots, Input_{127}\}. \tag{3.22}$$

En forma general:

$$in_n = \{input_{8n}, input_{8n+1}, \ldots, Input_{8n+7}\} \tag{3.23}$$

Luego se construye la matriz de entrada:

$$in = \begin{bmatrix} in_0 & in_4 & in_8 & in_{12} \\ in_1 & in_5 & in_9 & in_{13} \\ in_2 & in_6 & in_{10} & in_{14} \\ in_3 & in_7 & in_{11} & in_{15} \end{bmatrix} \quad (3.24)$$

Se debe indicar también que un conjunto de cuatro bytes se le conoce como una palabra de 32bits, este término se utilizara cuando se explique la clave extendida. A seguir se definen variables para el desarrollo del algoritmo:

Nb = Especifica la cantidad del bloque de entrada en grupos de 32bits.
Nk = Especifica la cantidad del bloque de la clave en grupos de 32bits.
Nr = Especifica la cantidad de rondas que realizara la matriz de estados.

Para el desarrollo del trabajo Nb es igual a 4 debido a que el bloque de entrada es de 128 bits, Nk varía entre 4, 6 y 8 para los bloques de key AES128, AES192 y AES256 respectivamente, Nr depende de los valores de Nb y Nk pero como Nb es constante solo depende de Nk, y estos son 10, 12 y 14 para AES128, AES192 y AES256 respectivamente.

A continuación se presenta el seudocódigo de cifrado:

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[0, Nb-1])
for round = 1 step 1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
end for
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
out = state
end
```

Este seudocódigo es bastante detallado, una forma más sencilla de representarlo es en diagrama de bloques como se ilustra en la Figura 3.2, en donde se encuentran las funciones o transformaciones SubBytes, ShiftRows, MixColumns y AddRoundKey, las

cuales representan parte importante en el cifrado del texto plano, estas serán explicadas a continuación.

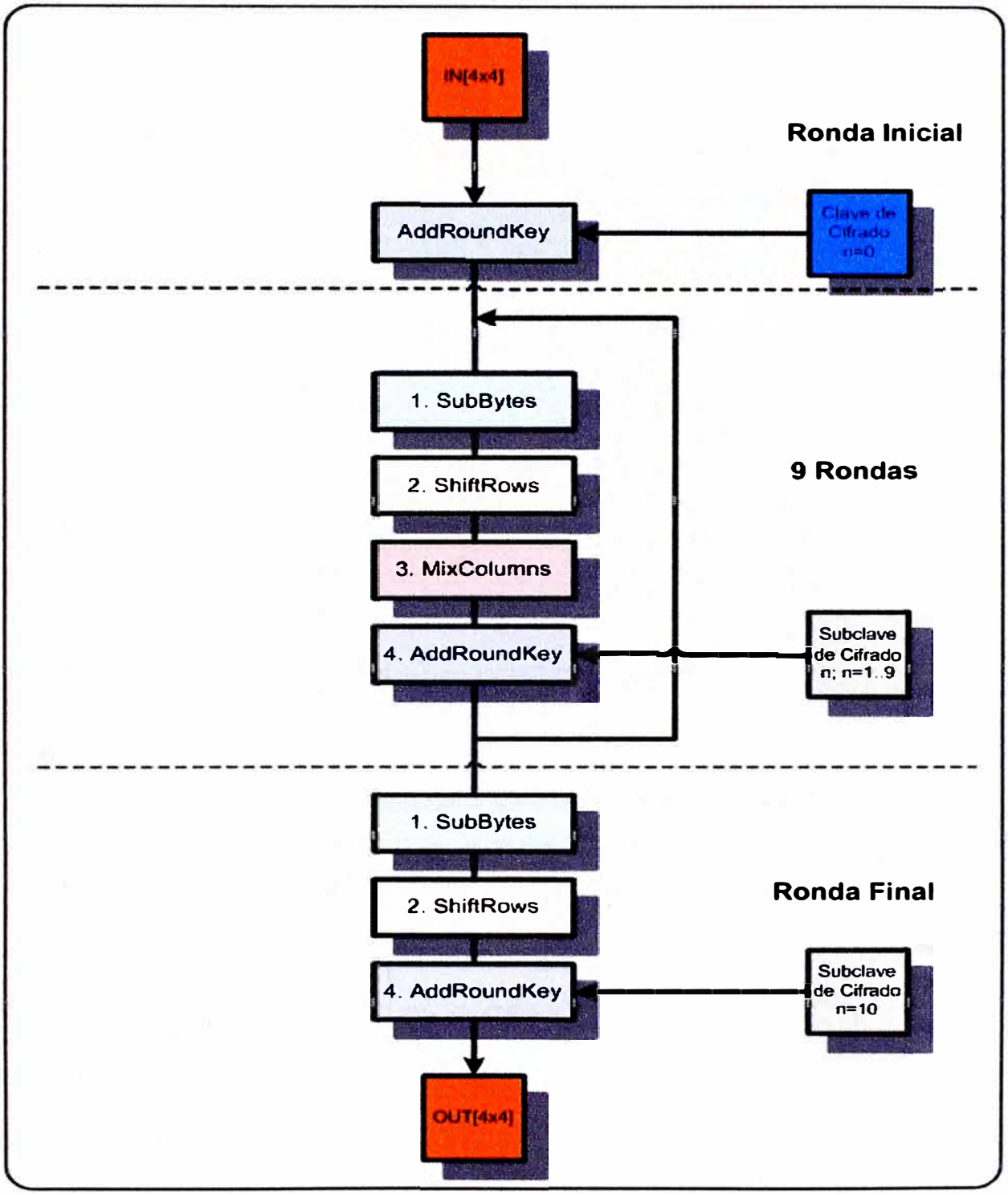

FIGURA 3.2 Diagrama de Bloques AES128. Fuente: Elaboración Propia.

SubBytes ()

Esta función o transformación consiste en sustituir todos los bytes de la matriz de estado (matriz de estado se le denomina a la matriz cuando se encuentra en proceso de cifrado) por su equivalente en la caja S-Box, podemos poner como ejemplo el reemplazar

el byte {53}, entonces buscamos en la caja de S-box la fila 5 y columna 3, y el resultado es {ed}.

Tabla 3.1 Caja S-Box. Fuente: Elaboración Propia.

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
	4	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

ShiftRows ()

Esta función consiste en desplazar la fila a la izquierda una cantidad de bytes igual al número de la fila, ejemplo la fila 0 no se mueve, la fila 1 se mueve un byte, la fila 2 se mueve 2 bytes y la fila 3 se mueve 3 bytes. El ejemplo siguiente muestra lo indicado.

$$\begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix} \equiv> ShiftRows \equiv> \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{11} & S_{12} & S_{13} & S_{10} \\ S_{22} & S_{23} & S_{20} & S_{21} \\ S_{33} & S_{30} & S_{31} & S_{32} \end{bmatrix} \quad (3.25)$$

MixColumns ()

Esta función multiplica la matriz de estados columna por columna por una matriz de 4x4, como se muestra a continuación:

$$\begin{bmatrix} S'_{0C} \\ S'_{1C} \\ S'_{2C} \\ S'_{3C} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} S_{0C} \\ S_{1C} \\ S_{2C} \\ S_{3C} \end{bmatrix} \quad (3.26)$$

La multiplicación matricial se resuelve aplicando las operaciones básicas del campo de Galoit GF(2^8) (sección 3.1.2), obteniéndose los siguientes resultados:

$$S'_{0C} = (\{02\} \bullet S_{0C}) \oplus (\{03\} \bullet S_{1C}) \oplus S_{2C} \oplus S_{3C} \quad (3.27)$$

$$S'_{1C} = S_{0C} \oplus (\{02\} \bullet S_{1C}) \oplus (\{03\} \bullet S_{2C}) \oplus S_{3C} \quad (3.28)$$

$$S_{2C} = S_{0C} \oplus S_{1C} \oplus (\{02\} \bullet S_{2C}) \oplus (\{03\} \bullet S_{3C}) \quad (3.29)$$

$$S'_{3C} = (\{03\} \bullet S_{0C}) \oplus S_{1C} \oplus S_{2C} \oplus (\{02\} \bullet S_{3C}) \quad (3.30)$$

AddRoundKey ()

Esta función o transformación consiste en adicionar la matriz de estado con la matriz de la clave que corresponde a la ronda, representado por:

$$[S'_{0C} \quad S'_{1C} \quad S'_{2C} \quad S'_{3C}] = [S_{0C} \quad S_{1C} \quad S_{2C} \quad S_{3C}] \oplus [W_{round*Nb+C}] \quad (3.31)$$

Donde Nb=4, round es el numero de ronda donde nos encontramos y C es la columna, W hace referencia a una palabra (Word) de 32 bits que representa una columna en la subclave de cifrado.

3.1.4 Clave Expandida

Uno de los componentes del algoritmo AES es la generación de subclaves (generadas a partir de la clave original) que se ingresan a la función AddRoundKey (), como se ilustro en la Figura 3.2. A continuación se muestra el seudocódigo que genera estas subclaves:

```
KeyExpansion(byte key[4*Nk], word w[Nb*(Nr+1)], Nk)
begin
word temp
i = 0
while (i < Nk)
w[i] = word(key[4*i], key[4*i+1], key[4*i+2], key[4*i+3])
i = i+1
end while
i = Nk
while (i < Nb * (Nr+1)]
temp = w[i-1]
if (i mod Nk = 0)
temp = SubWord(RotWord(temp)) xor Rcon[i/Nk]
else if (Nk > 6 and i mod Nk = 4)
temp = SubWord(temp)
end if
w[i] = w[i-Nk] xor temp
i = i + 1
end while
end
```

En este seudocódigo se tiene la función de **SubWord()**, que sustituye los 4 bytes de una palabra por su equivalente en la tabla S-Box, la función **RotWord()** desplaza a la izquierda en forma cíclica un byte, ejemplo si tenemos la palabra [a_{0C}, a_{1C}, a_{2C}, a_{4C}], luego aplicamos RotWord tenemos [a_{1C}, a_{2C}, a_{3C}, a_{0C}], y por último la palabra **Rcon[i]**, donde i es el numero de ronda, que se representa por [{02}$^{i-1}$, {00}, {00}, {00}], como ejemplo para Rcon[2] = [{02}•{02}, {00}, {00}, {00}] se tiene que Rcon[2]=[{04}, {00}, {00}, {00}].

3.1.5 Algoritmo de Cifrado Inverso

Al igual que el algoritmo de cifrado directo o simplemente algoritmo de cifrado este consiste en un conjunto de operaciones matemáticas que decodificara el texto cifrado en texto plano, el seudocódigo utilizado para este algoritmo es:

```
InvCipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
byte state[4,Nb]
state = in
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
for round = Nr-1 step -1 downto 1
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
InvMixColumns(state)
end for
InvShiftRows(state)
InvSubBytes(state)
AddRoundKey(state, w[0, Nb-1])
out = state
end
```

Para poder entender este seudocódigo se deben definir las funciones inversas.

InvShiftRows ()

Es el mismo procedimiento que ShiftRows pero esta vez no se desplaza a la izquierda sino a la derecha.

$$\begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{10} & S_{11} & S_{12} & S_{13} \\ S_{20} & S_{21} & S_{22} & S_{23} \\ S_{30} & S_{31} & S_{32} & S_{33} \end{bmatrix} \equiv > \text{InvShiftRows} \equiv > \begin{bmatrix} S_{00} & S_{01} & S_{02} & S_{03} \\ S_{13} & S_{10} & S_{11} & S_{12} \\ S_{22} & S_{23} & S_{20} & S_{21} \\ S_{31} & S_{32} & S_{33} & S_{30} \end{bmatrix} \quad (3.32)$$

InvSubBytes ()

Es el mismo procedimiento que SubBytes pero esta vez la caja S-Box cambia por una caja S-Box inversa.

Tabla 2.4 Caja S-Box inversa. Fuente: Elaboración Propia.

		y														
		0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
x	0	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
	1	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
	2	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
	3	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
	4	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
	5	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
	6	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
	7	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
	8	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
	9	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
	a	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
	b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
	c	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
	d	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
	e	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
	f	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

InvMixColumns ()

Es el mismo procedimiento que con MixColumns pero cambia la matriz de multiplicación.

$$\begin{bmatrix} S'_{0C} \\ S'_{1C} \\ S'_{2C} \\ S'_{3C} \end{bmatrix} = \begin{bmatrix} 0e & 0b & 0d & 09 \\ 09 & 0e & 0b & 0d \\ 0d & 09 & 0e & 0b \\ 0b & 0d & 09 & 0e \end{bmatrix} \begin{bmatrix} S_{0C} \\ S_{1C} \\ S_{2C} \\ S_{3C} \end{bmatrix} \quad (3.33)$$

Desarrollando se tiene:

$$S'_{0C} = (\{0e\} \bullet S_{0C}) \oplus (\{0b\} \bullet S_{1C}) \oplus (\{0d\} \bullet S_{2C}) \oplus (\{09\} \bullet S_{3C}) \quad (3.34)$$

$$S'_{1C} = (\{09\} \bullet S_{0C}) \oplus (\{0e\} \bullet S_{1C}) \oplus (\{0b\} \bullet S_{2C}) \oplus (\{0d\} \bullet S_{3C}) \quad (3.35)$$

$$S'_{2C} = (\{0d\} \bullet S_{0C}) \oplus (\{09\} \bullet S_{1C}) \oplus (\{0e\} \bullet S_{2C}) \oplus (\{0b\} \bullet S_{3C}) \quad (3.36)$$

$$S'_{3C} = (\{0b\} \bullet S_{0C}) \oplus (\{0d\} \bullet S_{1C}) \oplus (\{09\} \bullet S_{2C}) \oplus (\{0e\} \bullet S_{3C}) \quad (3.37)$$

Inversa de la función AddRoundKey

AddRoundKey es el inverso del mismo.

Con este último concepto concluye la teoría del Algoritmo AES, se puede adelantar indicando que el algoritmo AES128 es más rápido que el algoritmo AES192 y este a su vez más rápido que AES256. Algunos detalles de análisis se brindaran en el capítulo IV.

3.2 Método de Autenticación 802.1x

El estándar 802.11 provee un marco para varios protocolos de autenticación y gestión de claves. Existen distintos tipos de autenticación 802.1X y cada uno ofrece un método distinto de autenticación, pero todos emplean el mismo protocolo y marco 802.11 para la comunicación entre un cliente y un punto de acceso. En la mayoría de los protocolos, tras finalizar el proceso de autenticación 802.1X, el cliente recibe una clave que utiliza para la codificación de datos. Con la autenticación 802.1X, se utiliza un método de autenticación entre el cliente y el servidor (por ejemplo, un servidor de Servicio de usuario para el acceso telefónico de autenticación remoto (RADIUS)) conectado al punto de acceso. El proceso de autenticación utiliza credenciales, tal como la contraseña del usuario, las cuales *no se transmiten* a través de la red inalámbrica. La mayoría de los tipos 802.1X son compatibles con las claves dinámicas para cada usuario y cada sesión, lo cual fortalece la seguridad de las claves. La autenticación 802.1X se beneficia del uso del protocolo de autenticación existente conocido como Protocolo de autenticación ampliable (EAP). Cabe destacar que la autenticación 802.1x es independiente del proceso de cifrado.

La autenticación 802.1X para redes inalámbricas tiene tres componentes principales:

- El autenticador (el punto de acceso)
- El solicitante (el software cliente)
- El servidor de autenticación

La seguridad de autenticación 802.1X inicia una solicitud de autorización desde el cliente inalámbrico al punto de acceso, el cual autentica al cliente en un servidor RADIUS compatible con el Protocolo de autenticación ampliable (EAP). El servidor RADIUS puede autenticar ya sea a los usuarios (mediante contraseñas o certificados) o a los equipos (mediante direcciones MAC). En teoría, un cliente inalámbrico no puede conectarse a las redes hasta que se complete la transacción. (No todos los métodos de autenticación utilizan un servidor RADIUS. WPA-Personal y WPA2-Personal utilizan una contraseña común que debe introducirse en el punto de acceso y en todos los dispositivos que soliciten acceso a la red.) Existen varios algoritmos de autenticación utilizados con 802.1X. Algunos ejemplos son: EAP-TLS, EAP-TTLS, EAP Protegido (PEAP) y el

Protocolo de Autenticación ampliable ligero inalámbrico Cisco EAP (LEAP). Todos éstos son métodos que el cliente inalámbrico utiliza para identificarse a sí mismo ante el servidor RADIUS. Con la autenticación RADIUS, las identidades de los usuarios se verifican en las bases de datos. RADIUS constituye un conjunto de estándares que controla la autenticación, la autorización y la contabilidad (AAA). RADIUS incluye un proceso *proxy* para validar clientes en los entornos con varios servidores. El estándar IEEE 802.1X proporciona un mecanismo para controlar y autenticar el acceso a redes inalámbricas 802.11 basadas en puerto y a redes Ethernet cableadas. El control del acceso a redes basadas en puerto es similar a una infraestructura de red de área local (LAN) conmutada que autentica los dispositivos conectados a un puerto LAN y previene el acceso a dicho puerto si falla el proceso de autenticación.

Tipo de Autenticación PEAP

PEAP es un nuevo tipo de autenticación del Protocolo de autenticación ampliable (EAP) IEEE 802.1X diseñado para sacar provecho de la seguridad del nivel de transporte EAP (EAP-TLS) del lado del servidor y para admitir varios métodos de autenticación, los cuales incluyen las contraseñas de usuarios, las contraseñas temporales y las tarjetas de testigo genérico.

Protocolo de Autenticación MS-CHAP-V2

Introduce una función adicional que no está disponible con la autenticación MS-CHAP-V1 o CHAP estándar, la cual es la función de cambio de contraseña. Esta función permite que el cliente cambie la contraseña de cuenta si el servidor RADIUS informa que ha vencido la contraseña. Disponible para los tipos de autenticación TTLS y PEAP.

CAPITULO IV
ESTUDIO DE UN SISTEMA INALÁMBRICO SEGURO BASADO EN LA TÉCNICA DE ENCRIPTAMIENTO AES128

4.1 Seguridad en Sistemas Inalámbricos

Para proteger nuestro acceso inalámbrico se debe implementar métodos de encriptación y autenticación que hagan imposible que alguien externo a la empresa ingrese a la red.

4.1.1 Alternativas de seguridad y técnicas de encriptación

Los métodos de seguridad disponibles en el sector de las tecnologías de la información son:

a) Filtrado por MAC

Actualmente este método tiene problemas de seguridad ya que se ha encontrado la manera de rastrear (con un Sniffer) la red inalámbrica buscando una MAC autorizada y luego esta es duplicada, haciendo que el intruso pueda ingresar a la red.

b) Encriptación WEP

El "Wired Equivalent Privacy" o "Privacidad Equivalente a Cableado" es uno de los primeros método de encriptación que se utilizo para mejorar la seguridad en el acceso inalámbrico, pero lamentablemente a este método también se le ha encontrado falencias, y en la actualidad existe en internet software libre que pueden desencriptar este protocolo y por lo tanto también podrían ingresar a la red.

c) Encriptación WPA,

El "Wi-Fi Protected Access" o el "acceso protegido Wi-Fi", fue la mejora que se realizo al método de encriptación WEP hasta que saliera el estándar de la IEEE, al cual se le llamo WPA2 que es el más seguro en el campo de las TI.

d) Encriptación WPA2

El estándar definitivo denominado 802.11i fue ratificado en Junio de 2004, aquí se

define el método WPA2, este se basa en el algoritmo de encriptación AES, el cual ya se ha descrito en el capítulo II y es el método de encriptación que utilizaremos para nuestra red inalámbrica.

4.1.2 Métodos de autenticación

Una vez explicado el método de encriptación a utilizar se procede a buscar una forma de autenticación encontrándose dos métodos:

a) Clave compartida

b) 802.1x/PEAP (Este puede utilizar validación con el Active Directory)

Para el acceso a personal corporativo se utilizara el segundo método y para el acceso a personal externo, como visitas de clientes, vendedores y cualquier otro personal externo a la empresa se utilizara el primer método.

4.2 Diagrama y componentes del sistema inalámbrico

Como se indico en la sección anterior el método más seguro de encriptación es el WPA2 utilizando el algoritmo AES y el método de autenticación más seguro es el 802.1x/PEAP, ambos métodos en conjunto hacen que el acceso a la red corporativa de la empresa sea seguro, para este informe el nombre de la empresa será empresaX. A continuación se describe la solución brindada a los requerimientos solicitados en el capítulo I.

Movilidad, para este punto se utilizara el roaming de capa 2, para realizar esta tarea se necesita que las áreas de cobertura de cada punto de acceso o Access Point se traslapen por lo menos un 10%, también se deben utilizar rangos de frecuencia distintos para que no se genere interferencia, en este caso utilizaremos los canales 1, 6 y 11.

Flexibilidad, para este punto es suficiente con aplicar el mismo esquema de acceso en cada local de la empresa de esta manera al moverse de local en local el acceso inalámbrico será transparente para el usuario final y no afectara sus labores diarias.

Sencillez, para este punto es posible indicar que el método de autenticación será implícito para el usuario es decir no tendrá que ingresar un usuario y clave para que pueda tener acceso a la red, el método 802.1x/PEAP utilizara por defecto su usuario de dominio o de directorio activo con el cual ingreso a la maquina, de esta forma reutilizamos

el usuario para que se valide en el acceso inalámbrico, una de las ventajas de este método es que al utilizar el usuario de dominio también se adoptaran la seguridad de este, es decir la clave se cambiara cada 8 semanas, la clave tiene que ser diferente a las ultimas 10 claves utilizadas, se tiene que utilizar símbolos, números, letras minúsculas y mayúsculas o por lo menos 3 de estos 4 tipos de caracteres.

Seguridad, como se ha indicado anteriormente la seguridad está garantizada por el método de cifrado WPA2-AES y el método de autenticación 802.1x/PEAP.

Hasta ahora solo se ha explicado el acceso al personal corporativo, en lo referente al acceso del personal externo a la empresa (visitas), se les brindara un acceso similar pero solo tendrán salida a internet mas no acceso a la red corporativa, es decir se ubicaran en una red aislada con solo acceso a internet, sin embargo el personal corporativo si tendrá acceso al cliente de visita, esto se ilustra mejor en la Figura 4.1. En lo referente a la seguridad para los clientes de visita se utilizara el método de encriptación WPA2-AES con método de autenticación por clave compartida, una observación importante para poder realizar esta tarea se necesita que los Access Point tengan la capacidad de publicar dos BSS para que se asocien a dos vlan diferentes y así poderlos separar, este requisito fundamental lo cumplen los equipos wifi de cisco los cuales vamos a utilizar en esta implementación.

4.2.1 Diagrama de red de la Solución

En la Figura 4.1 se presenta el esquema de red que se va a utilizar en esta implementación para separar las redes utilizaremos un firewall de cisco, quien nos garantizara que la red de clientes se encuentre aislada de nuestra red corporativa.

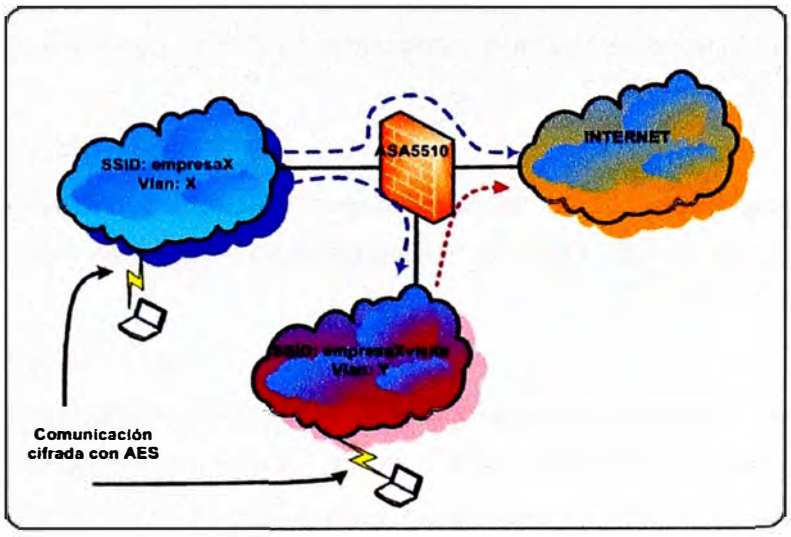

FIGURA 4.1 Esquema de Seguridad. Fuente: Elaboración Propia.

Para el método de autenticación utilizaremos un RADIUS utilizando la herramienta Cisco Secure ACS v4.2, este radius se integrara al Active Directory de la empresaX y le solicitara la validación del usuario y la clave, una vez validado el RADIUS enviara la orden de aceptación o negación al equipo de acceso en este caso el Access Point, también se debe recalcar que este método de autenticación solo se utilizara para los usuarios corporativos. Para los usuarios que son visitantes se utilizara una clave de acceso. En la Figura4.2 se ilustra el esquema de autenticación.

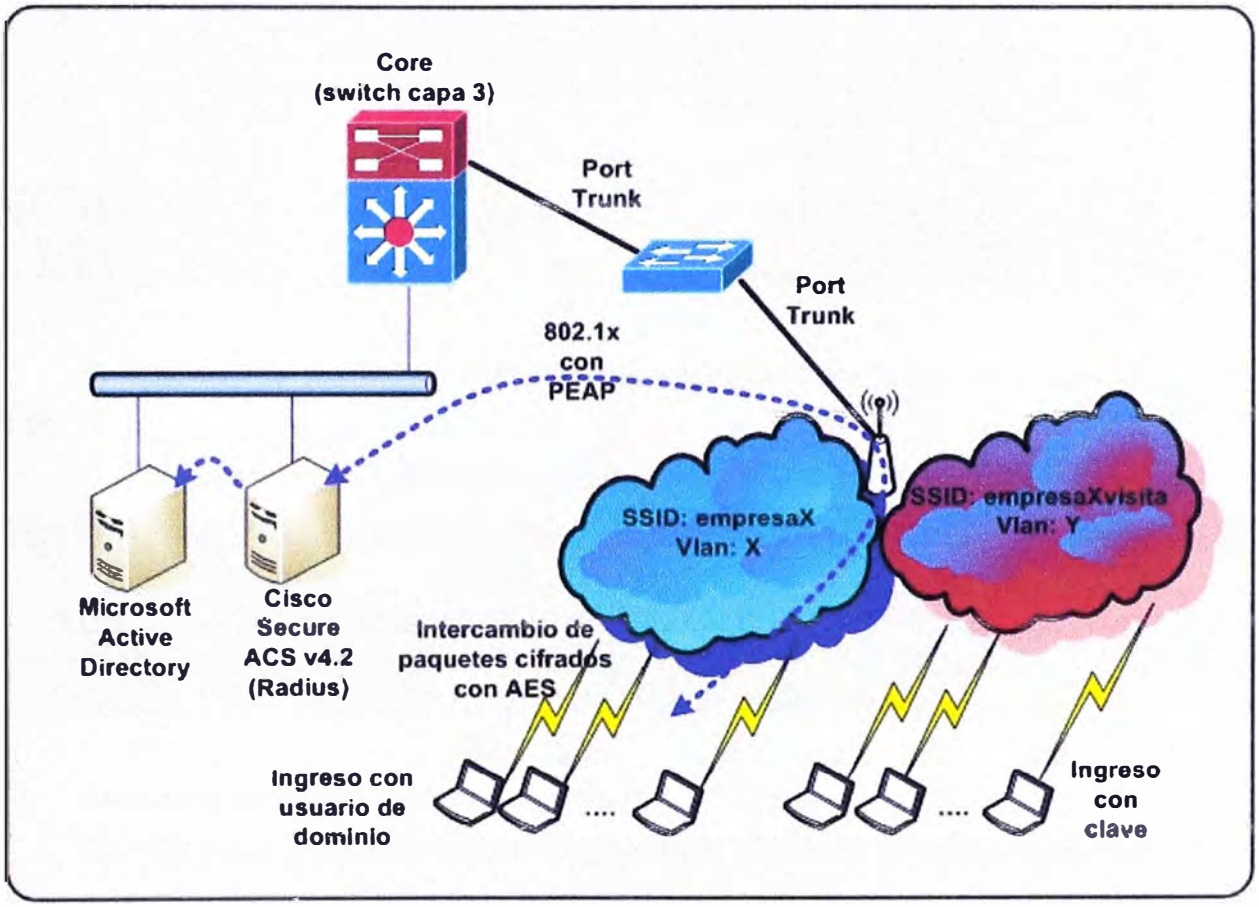

FIGURA 4.2 Esquema de Autenticación. Fuente: Elaboración Propia.

4.2.2 Diseño de la Red Corporativa

Para este informe, se inicia con el diseño del entorno que conlleva un acceso inalámbrico. Para este propósito las consideraciones para el diseño son las siguientes:

a) Segmentos y vlan de red a utilizar

Para la red de datos corporativa utilizaremos el segmento privado de clase A 10.0.0.0/8 y para las visitas o cualquier cliente utilizaremos un segmento privado de clase B 172.16.0.0/12. En la Tabla 4.1 se presentan los segmentos y vlan asociados que se utilizaran en este diseño.

Tabla 4.1 Cuadro de Segmentos de Red. Fuente: Elaboración Propia.

LOCAL	Vlan	Descripcion	Red	Mask	Cantidad de host
LOCAL1(10.101.0.0/18)	2	Equipos de Comunicaciones	10.101.0.0	255.255.255.0	254
		Reservado para Equipos de Comunicaciones	10.101.1.0	255.255.255.0	254
	3	Servidores de Datos	10.101.2.0	255.255.255.0	254
		Reservado para Servidores de Datos	10.101.3.0	255.255.255.0	254
	4	Servidores de Voz	10.101.4.0	255.255.255.0	254
		Reservado para servidores de Voz	10.101.5.0	255.255.255.0	254
	5	Camaras IP	10.101.6.0	255.255.255.0	254
		Reservado para Camaras IP	10.101.7.0	255.255.255.0	254
	6	Equipos de Datos (Desktop y Laptops)	10.101.8.0	255.255.248.0	2046
		Reservado para Equipos de Datos	10.101.16.0	255.255.248.0	2046
	7	Equipos de voz (Telefonos IP)	10.101.24.0	255.255.252.0	1022
		Reservado para Equipos de Voz	10.101.28.0	255.255.252.0	1022
		LIBRE	10.101.32.0	255.255.248.0	2046
		LIBRE	10.101.40.0	255.255.248.0	2046
		LIBRE	10.101.48.0	255.255.248.0	2046
		LIBRE	10.101.56.0	255.255.248.0	2046
LOCAL2		LOCAL2	10.101.64.0	255.255.192.0	16382
LOCAL3		LOCAL3	10.101.128.0	255.255.192.0	16382
LOCAL4		LOCAL4	10.101.192.0	255.255.192.0	16382

En seguida se presenta los segmentos utilizados para la red de visita (ver Tabla 4.2).

Tabla 4.2 Segmentos para la Red de Visita. Fuente: Elaboración Propia.

LOCAL	Vlan	Descripcion	Red	Mask	Cantidad de host
LOCAL1	100	Equipos de Datos de visita	172.16.0.0	255.255.255.0	254
LOCAL2	100	Equipos de Datos de visita	172.16.16.0	255.255.255.0	254
LOCAL3	100	Equipos de Datos de visita	172.16.32.0	255.255.255.0	254
LOCAL4	100	Equipos de Datos de visita	172.16.48.0	255.255.255.0	254

b) Esquema detallado y Asignación de IPs a equipos

En esta sección se procederá a esquematizar el diseño de red, se asignaran IPs a los servidores de dominio y Radius, equipos de comunicaciones como switches de capa 3, switches de capa 2, Firewall y por último a los Access Point. Así también, para el diseño se requiere un par de DHCPs quienes son los que asignaran de forma dinámica las IPs a los equipos móviles tanto corporativos como a los de visita.

Este diseño tomo en cuenta una red de voz tanto para servidores (ejemplo centrales telefónica IP) como para clientes como son los teléfonos IP, estos últimos no se esquematizan en la Figura 4.3 debido a que no son el objeto de estudio, pero también se podría asignar un SSID para equipos que deseen manejar exclusivamente voz como podrían ser los teléfonos inteligentes con un softphone IP instalado en el teléfono el cual mediante la red de datos podría conectarse a la central telefónica y ser un anexo mas de dicha central pudiendo recibir y realizar llamadas.

La Tabla 4.3 contiene las IPs asignadas a cada equipo:

Tabla 4.3 IPs asignadas a Equipos. Fuente: Elaboración Propia.

Equipo	IP	Mask
Core	10.101.0.1	255.255.255.0
Firewall	10.101.0.2	255.255.255.0
switches	10.101.0.3-10	255.255.255.0
Access Point	10.101.0.11-20	255.255.255.0
Server Active Directory	10.101.2.2	255.255.255.0
Server Radius (ACS v4.2)	10.101.2.3	255.255.255.0
Server DHCP Datos	10.101.8.2	255.255.248.0
Pool Posiciones de Datos	10.101.8.11 - 10.101.11.255	255.255.248.0
Server DHCP Visita	172.16.0.2	255.255.255.0
Pool Posiciones de los Visitantes	172.16.0.11-172.16.0.250	255.255.255.0

Para los otros locales el diseño es similar por lo que no habría necesidad de especificarlo. En la Figura 4.3 se ilustra un esquema detallado de la red a ser implementada.

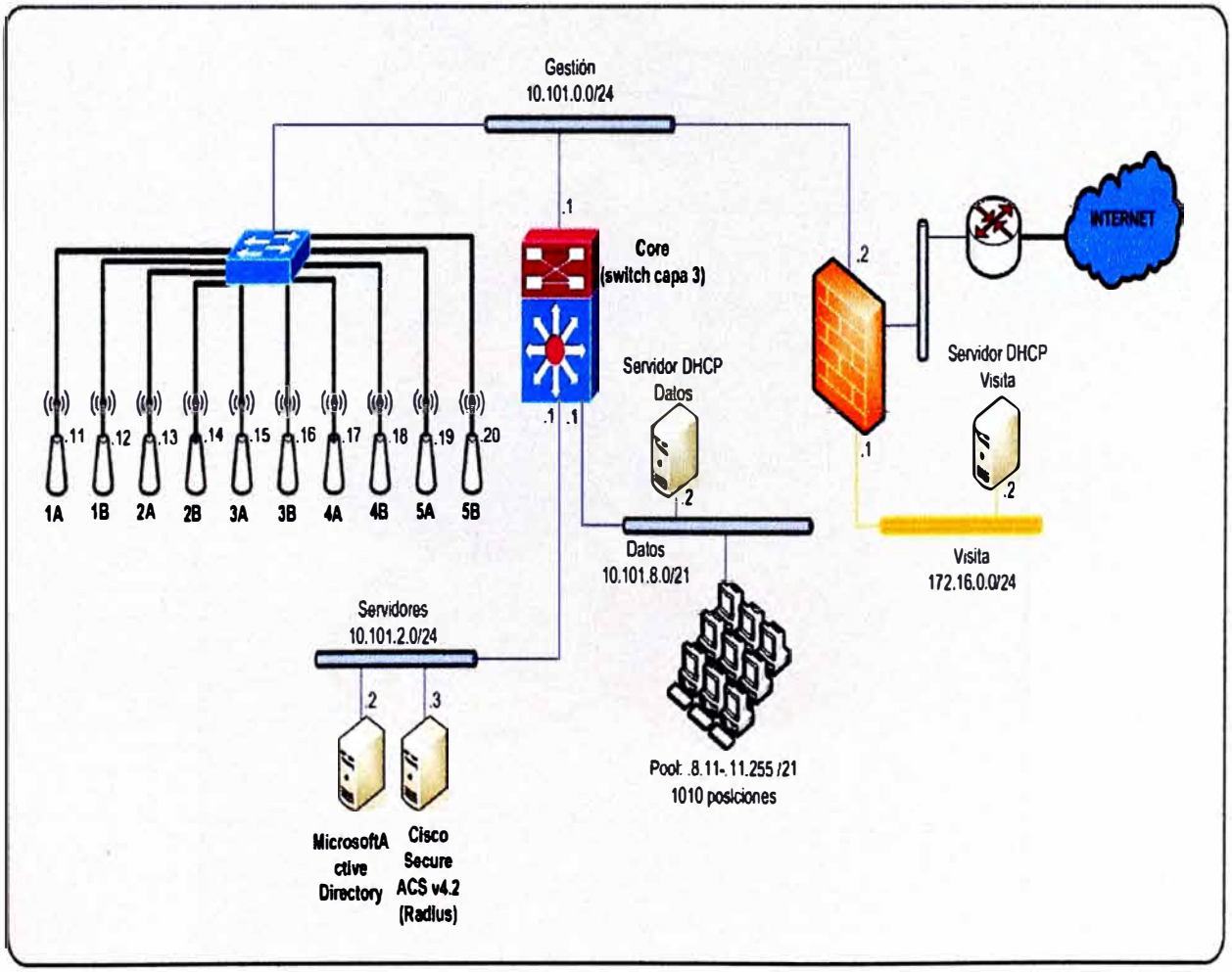

FIGURA 4.3 Esquema de Red Detallado. Fuente: Elaboración Propia.

4.2.3 Esquema de RF

El primer local es un edificio de 5 pisos, se dispuso la distribución de frecuencias como se ilustra en la Figura 4.4, el edificio está dividido como lado A y lado B, se han utilizado los canales 1,6 y 11 quienes son los únicos que no se traslapan entre sí, se ha distribuido de tal forma que se pueda realizar roaming de capa 2, es decir si un usuario se desplaza del primer piso hasta el 5to piso este no se desconectara de la Red.

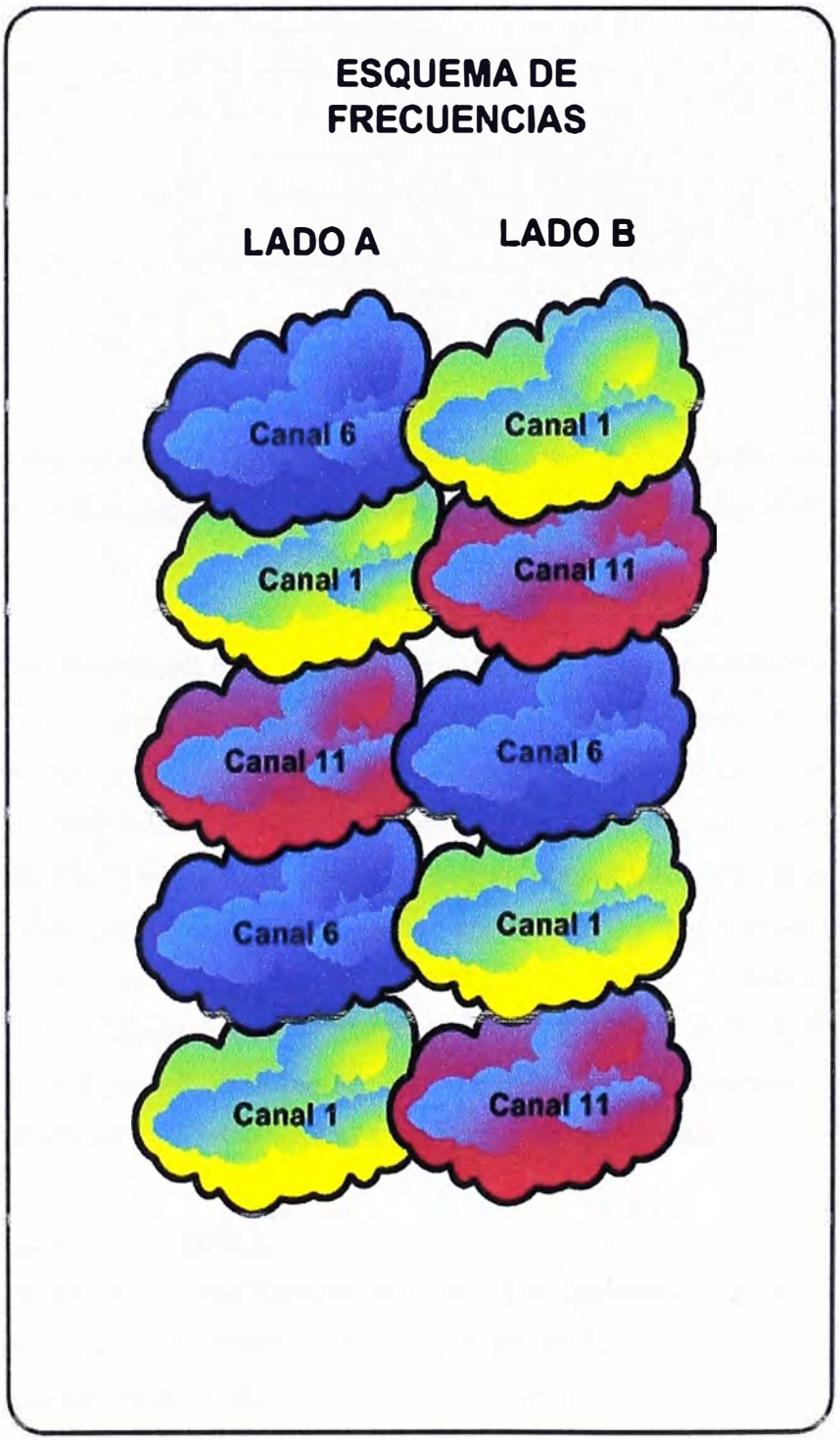

FIGURA 4.4 Esquema de Radiofrecuencia (RF). Fuente: Elaboración Propia.

4.2.4 Equipamiento

Los equipos que se utilizaran en esta implementación son los especificados en la Tabla 4.4.

Tabla 4.4 IPs asignadas a Equipos. Fuente: Elaboración Propia.

Equipo	Marca	Modelo	S.O.
Core	3com	5500G-EI 24-Port	3Com OS V3.02.04s56
Firewall	cisco	ASA5510	Cisco ASA Software Version 7.2(1)
switches	3com	4500 PWR 50-Port	3Com OS V3.03.00s56
Access Point	cisco	AIR-AP1131AG-A-K9	C1130 Software Version 12.4(21a)JA1
Server Active Directory	HP	HP ProLiant DL320 G6	Win2003 Server std Ed.
Server Radius (ACS v4.2)	HP	HP ProLiant DL320 G6	Win2003 Server std Ed.
Server DHCP Datos	HP	HP ProLiant DL320 G6	Win2003 Server std Ed.
Pool Posiciones de Datos	Diversas Marcas	No Aplica	WinXP SP3
Server DHCP Visita	HP	HP ProLiant DL320 G6	Win2003 Server std Ed.
Pool Posiciones de los Visitantes	Diversas Marcas	No Aplica	WinXP SP3

Para los Equipos que brindan servicios de Red (Servidores) se puede utilizar equipos más robustos y aplicar la virtualización para estos servicios, lográndose reducir los equipos a dos o a uno en el mejor de los casos.

4.3 Aplicación del Algoritmo AES para Cifrado y 802.1x para Autenticación

En lo que se refiere a la configuración que se realizara a los equipos de comunicaciones se hace referencia a las configuraciones que competen a este documento. Se inicia con una pequeña configuración en el core (switch de capa 3), enseguida se configura la interface Ethernet que se conectara a los Access Point siendo esta tipo trunk para que los equipos se puedan conectar a las vlan 6 (datos) y 100 (visita). A continuación se configura los Access Point, y por último el Radius. Luego de la configuración de los equipos de comunicaciones se procede a configurar los equipos móviles (laptops) que se conectaran a este acceso inalámbrico se brindara la configuración de las laptops corporativas y de las laptops de visita

4.3.1 Configuración del CORE

En el core se tienen que habilitar las vlan que brindara acceso a los equipos de comunicaciones, equipos de datos y los equipos de datos de los visitantes, la Figura 4.5 muestra un resumen de la configuración realizada, en la cual se configuran las IPs y las Vlans.

```
[CORE]
[CORE]
[CORE]display current-configuration vlan 2
#
vlan 2
 description Equipos de Comunicaciones
#
return
[CORE]display current-configuration vlan 6
#
vlan 6
 description Equipos de Datos
#
return
[CORE]display current-configuration vlan 100
#
vlan 100
 description Equipos de Datos de visita
#
return
[CORE]display current-configuration interface Vlan-interface 2
#
interface Vlan-interface2
 ip address 10.101.0.1 255.255.255.0
#
return
[CORE]display current-configuration interface Vlan-interface 6
#
interface Vlan-interface6
 ip address 10.101.8.1 255.255.248.0
#
return
[CORE]display current-configuration | i 172.16.0.0
 ip route-static 172.16.0.0 255.255.255.0 10.101.0.2 preference 60 description visita
[CORE]
[CORE]
[CORE]display current-configuration | i 0.0.0.0 0.0.0.0
 ip route-static 0.0.0.0 0.0.0.0 10.101.0.2 preference 60
[CORE]
[CORE]
```

FIGURA 4.5 Configuración del CORE. Fuente: Elaboración Propia.

4.3.2 Configuración del Switch de Acceso

Se configura la interface que se conectara al Access Point, la cual será en modo trunk (ver Figura 4.6).

```
[SWITCH-1A]display current-configuration interface Ethernet 2/0/43
#
interface Ethernet2/0/43
 poe enable
 stp edged-port enable
 port  in -type trun
 port trunk permit vlan all
 po t t unk pvid vlan 2
 broa cast-suppression pps  000
 packet-filter inbound link-group 4999 rule 0
 description WIFI1A(10.101.0.11)
#
return
[SWITCH-1A]
[SWITCH-1A]
[SWITCH-1A]
[SWITCH-1A]
```

FIGURA 4.6 Configuración Interface Ethernet. Fuente: Elaboración Propia.

4.3.3 Configuración del Access Point

Se configura los radios, la interface Ethernet, el método de encriptación y el método de autenticación. La configuración completa se encuentra en el anexo A.

Se inicia configurando primeramente la interface fastethernet y la IP que tendrá este Wi-Fi, así como también se configura la ruta por defecto, esta configuración se muestra en la Figura 4.7.

```
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
!
interface FastEthernet0.2
 encapsulation dot1Q 2 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.6
 encapsulation dot1Q 6
 no ip route-cache
 bridge-group 6
 no bridge-group 6 source-learning
 bridge-group 6 spanning-disabled
!
interface FastEthernet0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 no bridge-group 100 source-learning
 bridge-group 100 spanning-disabled
!
interface BVI1
 ip address 10.101.0.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.101.0.1
ip http server
no ip http secure-server
```

FIGURA 4.7 Configuración WIFI-1A Interface FastEthernet. Fuente: Elaboración Propia.

Como se observa de la Figura 4.7 se ha dividido la interface fastethernet en subinterfaces de tal forma que se pueda relacionar con las vlan 2, 6 y 100, y estas a su vez se relacionaran con los SSID que les corresponde (ver Tabla 4.5), a continuación se configurara los radios (interface de RF). Este equipo tiene capacidad para dos radios de los cuales uno trabaja con el estándar 802.1g y el otro con el estándar 802.1a, en este caso solamente se utilizara el estándar 802.1g y el otro radio se mantiene en estado de apagado o en modo shutdown. La Figura 4.8 muestra la configuración de la interface de radio.

```
!
interface Dot11Radio0.2
 encapsulation dot1Q 2 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.6
 encapsulation dot1Q 6
 no ip route-cache
 bridge-group 6
 bridge-group 6 subscriber-loop-control
 bridge-group 6 block-unknown-source
 no bridge-group 6 source-learning
 no bridge-group 6 unicast-flooding
 bridge-group 6 spanning-disabled
!
interface Dot11Radio0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 bridge-group 100 subscriber-loop-control
 bridge-group 100 block-unknown-source
 no bridge-group 100 source-learning
 no bridge-group 100 unicast-flooding
 bridge-group 100 spanning-disabled
```

FIGURA 4.8 Configuración WIFI-1A Interface Radio. Fuente: Elaboración Propia.

Como se observa de la Figura 4.8 se ha subdividido la interface del radio Dot11Radio0 de tal forma que se pueda relacionar con la subinterface fastethernet ya configurada.

Se continua con la configuración de los SSID (Service Set IDentifier), como nota resaltante de estos equipos se puede decir que tienen la capacidad para configurar hasta 16 SSID y asociarlo a una vlan diferente. Se inicia indicando los datos necesarios para configurar cada SSID tanto para los usuarios corporativos como para los visitantes, estos se resumen en la Tabla 4.5.

Tabla 4.5 Datos de Configuración de los SSID. Fuente: Elaboración Propia.

Característica	Acceso Corporativo	Acceso para Visitas
SSID	empresaX	empresaXvisita
Vlan	6	100
Cifrado	AES	AES
Autenticación	802.1x/PEAP	Clave Compartida
Clave	3mpr3saX	3mpr3saXv1s1ta

La característica de clave en la tabla anterior hace referencia en el caso del Acceso Corporativo a la clave que se utilizara entre el equipo wireless y el servidor Radius para

aplicar el método de autenticación 802.1x/PEAP y en el caso del Acceso para Visitas hace referencia a la clave que se utilizara entre los equipos de datos portátiles (ejemplo Laptops) y el equipo wireless o Access Point. La Figura 4.9 muestra la clave compartida cifrada.

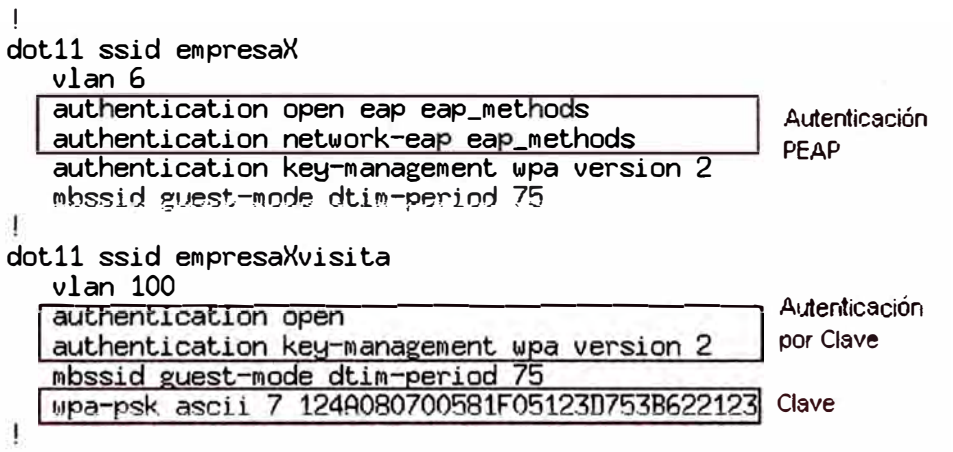

FIGURA 4.9 Configuración WIFI-1A SSID y autenticación. Fuente: Elaboración Propia.

La Figura 4.10 muestra las líneas de comando para el cifrado AES. Estas líneas indican que el método de encriptación que se utilizara para los SSID vinculados a las vlan 6 y 100 será el AES, estos SSID utilizaran este método de cifrado para intercambiar paquetes entre el Acess Point y el equipo cliente.

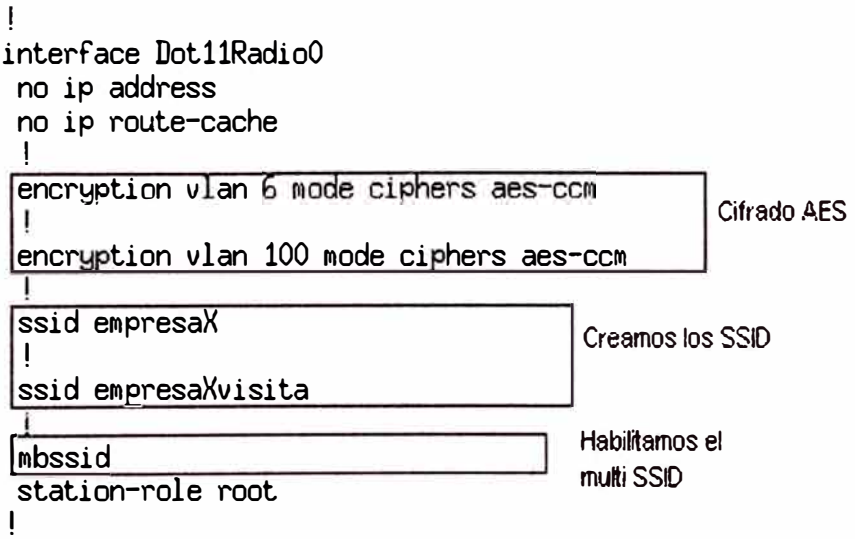

FIGURA 4.10 Configuración WIFI-1A Cifrado AES. Fuente: Elaboración Propia.

Finalmente se configura las líneas de comando que indiquen al Access Point cual es el radius que se utilizara para la validación de los usuarios corporativos (ver Figuras 4.11 y 4.12).

```
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.101.2.3  auth-port 1645 acct-port  1646
!
aaa authentication login eap_methods group rad_eap
!
aaa session-id common
!
!
dot11 syslog
```

Radius

FIGURA 4.11 Configuración WIFI-1A Radius. Fuente: Elaboración Propia.

```
interface BVI1
 ip address 10.101.0.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.101.0.1
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
radius-server host 10.168.145.52 auth-port 1645 acct-port 1646 key 7 101D04091744010A34
bridge 1 route ip
!
```

FIGURA 4.12 Configuración WIFI-1A Clave del Radius. Fuente: Elaboración Propia.

La línea de comando de la Figura 4.12 muestra la clave cifrada en este caso la clave es 3mpr3saX, la misma que se indico en la tabla 4.5

4.3.4 Configuración del Radius

En este apartado se configura el radius disponible en el software Cisco Secure ACS v4.2, como se muestra en la Figura 4.13.

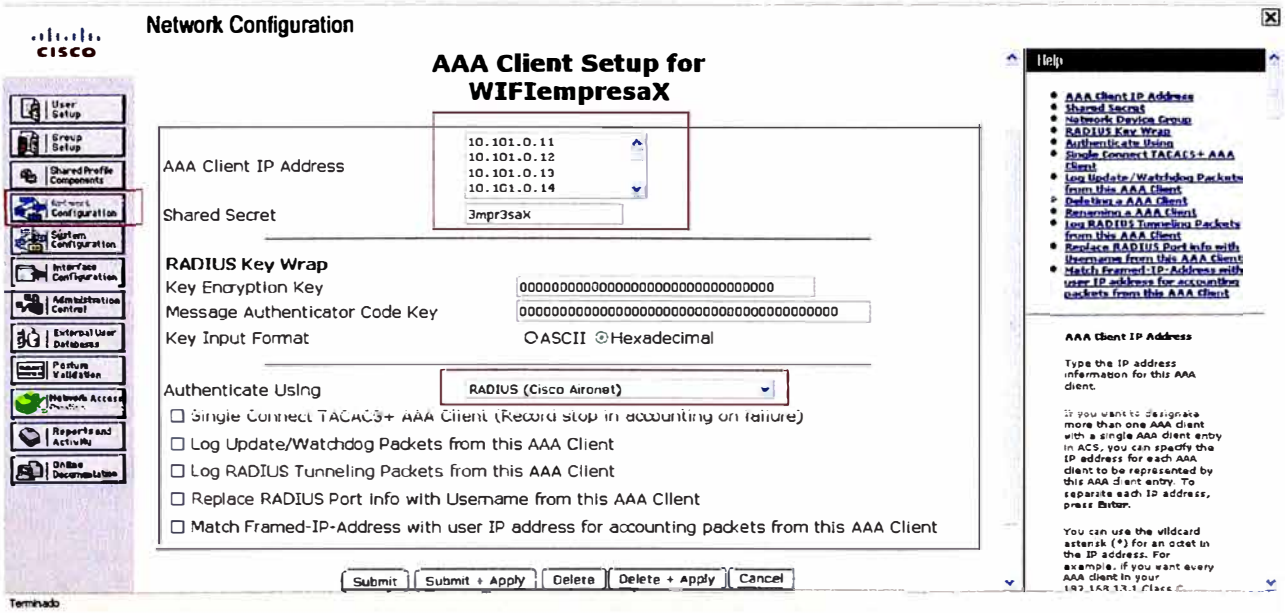

FIGURA 4.13 Configuración Cisco Secure ACS v4.2. Fuente: Elaboración Propia.

En la Figura 4.13 se presenta la interface del software para la configuración, la cual indica que se ha inscrito los 10 Access Point y se utilizara la autenticación vía Radius, aquí no se incluye la configuración del radius integrado al active directory.

4.3.5 Configuración de los Equipos de Datos

La configuración detallada se encuentra en el anexo B, pero se debe indicar que el requerimiento mínimo en lo que se refiere al sistema operativo de PCs portátiles es WinXP con SP3 (Service Pack 3), la configuración de los equipos corporativos es manual mientras que para los visitantes es automática.

4.4 Análisis de Resultados

En esta sección se mencionan resultados teóricos y prácticos.

4.4.1 Análisis teórico de AES

Como se indica en el Capítulo II dependiendo del tamaño de la clave el algoritmo de encriptamiento toma un mayor tiempo para procesar la información. En la Figura 4.14 se ilustra una comparación de los tiempos de procesamiento versus la cantidad de datos en bytes, como se observa el algoritmo AES128 es el más rápido y aunque la clave es más corta y por lo tanto menos seguro que los algoritmos AES192 y AES256, este tamaño de clave se recomienda para las implementaciones. Para el estudio de caso presentado en este trabajo el algoritmo de encriptamiento utilizado es el AES128.

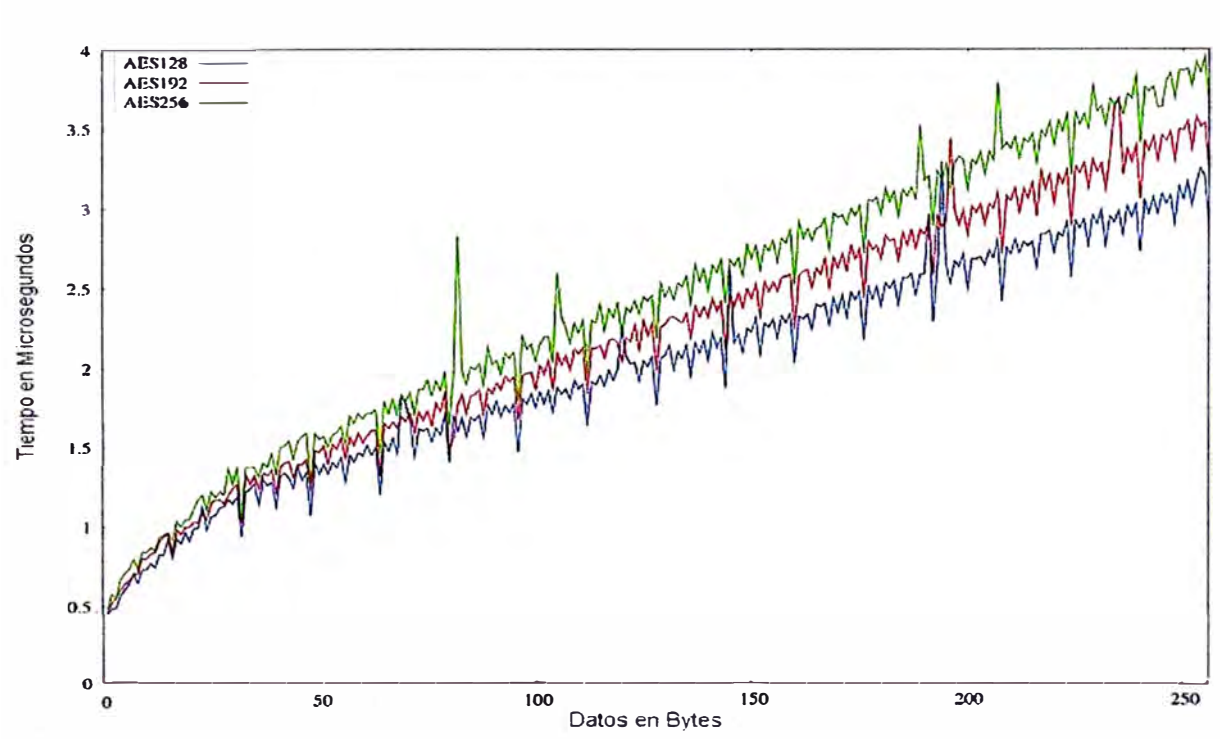

FIGURA 4.14 AES128 vs AES192 vs AES256. Fuente: Elaboración Propia.

4.4.2 Comparación de AES con otros algoritmos de Cifrado

La Figura 4.15 muestra un grafico de la velocidad de procesamiento en Mbytes/seg versus vs la cantidad de datos ingresados expresado en bytes, estos resultados se han conseguido aplicando los distintos métodos de cifrado a un mismo bloque de datos, y ejecutados en un misma máquina, los métodos de cifrado nombrados en la Figura son los que participaron en el concurso AES (sección 3.1), dos de los cuales son los más utilizados por los fabricantes, estos son Rijndael y 3DES, encontrándose que el Rijndael puede procesar la misma cantidad de información en menos tiempo, por tal motivo Rijndael es el algoritmo recomendado para nuestras implementaciones.

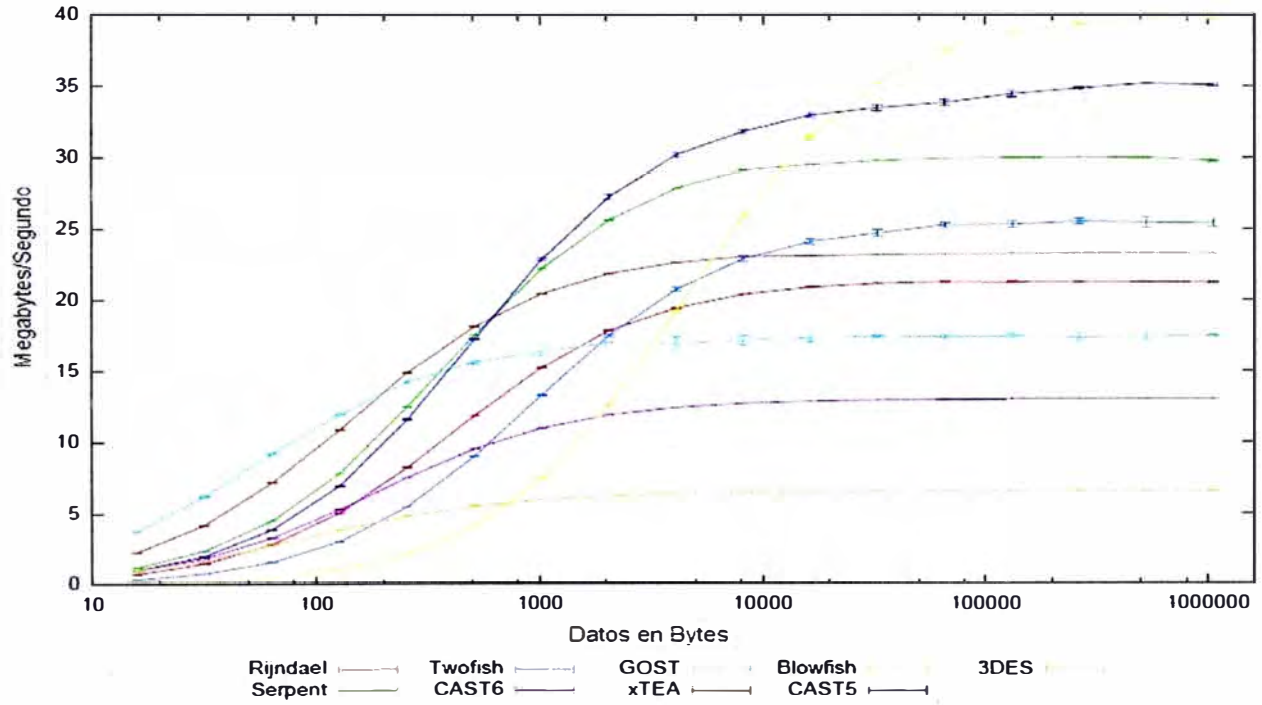

FIGURA 4.15 Comparación métodos de cifrado. Fuente: Elaboración Propia.

4.4.3 Presentación de Resultados de las velocidades de Acceso

La Tabla 4.6 contiene los resultados del análisis de comparación entre las velocidades de acceso versus la distancia al Access Point con línea de vista.

Tabla 4.6 Distancia vs Velocidad. Fuente: Elaboración Propia.

802.11g	
Disntancia(m)	**Velocidad(Mbits/seg)**
10	54
25	48
50	36
75	24
100	18

Como se muestra en la Tabla 4.6 cuanto más alejados nos encontremos del Access Point este asignara velocidades de acceso más bajas, este es el motivo por el cual se colocaron dos Access Point por piso.

4.4.4 Presentacion de Resultados de RF

En la Figura 4.16 se presenta el analisis de radiofrecuencia (RF), en donde se muestra el espectro de las antenas. Esta información fue obtenida por un software de RF llamada inSSIDer que es un analizador de espectros para redes inalambricas, realizando una analisis de radiofrecuencia en el lado A del piso 2. Los espectros de lineas naranja, roja y verde hacen referencia a los SSID de los pisos uno, dos y tres respectivamente, en donde se observa que se encuentran en los canales 1, 6 y 11 respectivamente de acuerdo a lo diseñado en la seccion 4.2.3, los espectros restantes hacen referencia a los SSID de los equipos vecinos como se observa son de menor potencia.

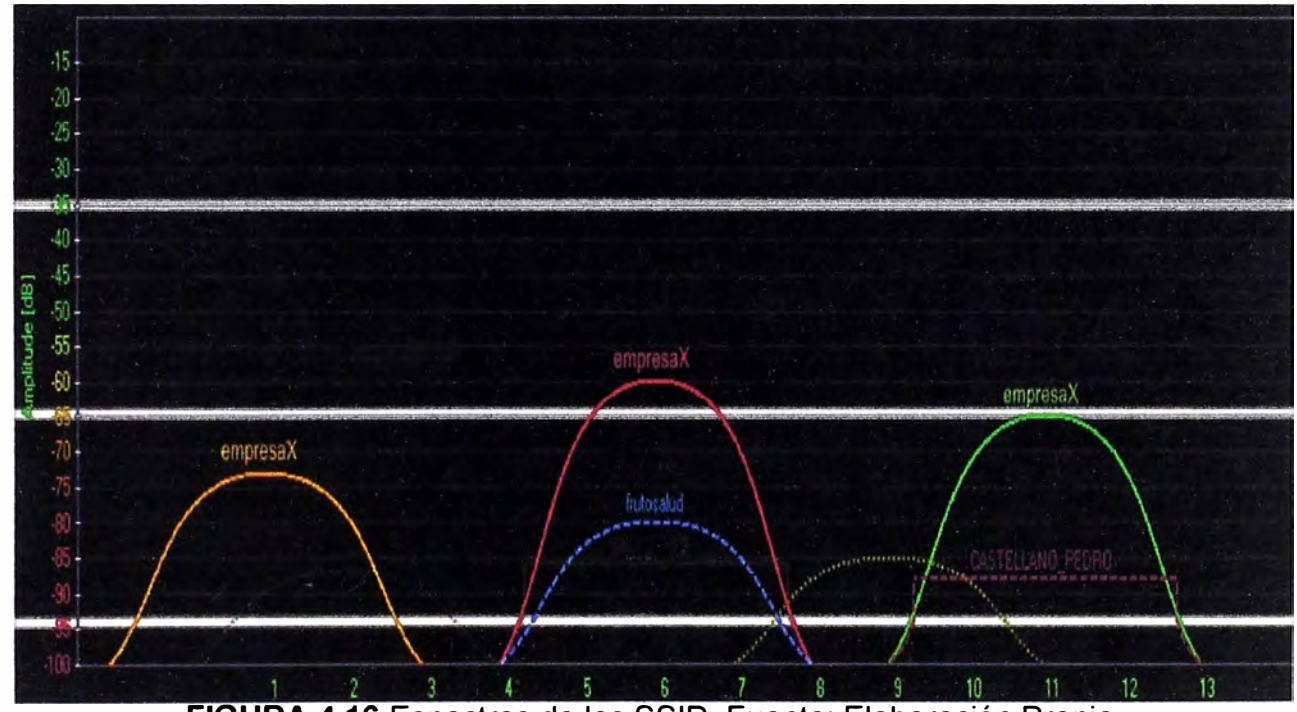

FIGURA 4.16 Espectros de los SSID. Fuente: Elaboración Propia.

4.4.5 Presupuesto y Tiempos de Ejecución

A continuación se describe el presupuesto y tiempos de implementación en la solución al acceso inalámbrico.

a) Presupuesto

El presupuesto requerido para la implementación de esta arquitectura de red descrita en las secciones 4.2.2 y 4.2.4, están contenidos en la Tabla 4.7.

Tabla 4.7 Tabla de Costos. Fuente: Elaboración Propia.

Descripcion	Marca	Modelo	Costo Unidad ($)	Catidad	Costo Total($)
Access Point	cisco	AIR-AP1131AG-A-K9	600	10	6000
Server Radius (ACS v4.2)	HP	HP ProLiant DL320 G6	1300	1	1300
Server DHCP Datos	HP	HP ProLiant DL320 G6	1300	1	1300
Server DHCP Visita	HP	HP ProLiant DL320 G6	1300	1	1300
Software ACS	cisco	version 4.2	5000	1	5000
Configuración	no aplica	no aplica	2000	1	2000
				TOTAL	16900

En esta tabla se supone que la arquitectura de red cableada mostrada en la Figura 4.3 se encuentra implementada, es decir se cuenta con un core (switch de capa3), switches de acceso y un firewall, por lo que solo se han cotizado los equipos que se adquirirían para la implementación como los Access Point y los Servidores. Los costos se pueden reducir si se utiliza un software libre para el Radius como FreeRadius (software con licencia GNU) y virtualización para los servidores lográndose reducir en 40% del costo total.

b) Tiempos de Ejecución

Los tiempos de ejecución para implementar el acceso inalámbrico seguro puede variar dependiendo principalmente del área de cobertura, es decir no es lo mismo implementar esta arquitectura de seguridad en un campus universitario que en un edificio, debido a la complejidad en su arquitectura física y el tamaño de la misma. Para nuestro caso de estudio el primer local es un edificio de 5 pisos, la implementación tomara un tiempo aproximado de 30 días cuya secuencia de procedimientos para la implementación se describen a continuación:

- Paso 1: Análisis y diseño de la arquitectura de acceso inalámbrico – 5 días
- Paso 2: Configuración en los equipos de Redes – 2 días
- Paso 3: Instalación física de los equipos – 2 días
- Paso 4: Configuración de la arquitectura inalámbrica – 5 días
- Paso 5: Configuración y pruebas en los equipos de acceso – 6 días

Todos estos pasos se reducen en un diagrama de Gantt como se muestra en la Tabla 4.8. En esta se supone que los equipos ya se encuentran disponibles, caso contrario la adquisición de los equipos podrían tomar entre uno o dos meses, debido al proceso de compra.

Tabla 4.8 Cronograma de Actividades. Fuente: Elaboración Propia.

Cronograma de Actividades	Semana 1					Semana 2					Semana 3					Semana 4				
	Dia1	Dia2	Dia3	Dia4	Dia5	Dia1	Dia2	Dia3	Dia4	Dia5	Dia1	Dia2	Dia3	Dia4	Dia5	Dia1	Dia2	Dia3	Dia4	Dia5
Análisis y diseño de la arquitectura de acceso Inalámbrica																				
Estudio de la arquitectura actual																				
Diseño de la arquitectura de acceso Inalámbrico																				
Configuración en los equipos de redes																				
Configuración en el Core y Switches																				
Configuración en el Firewall																				
Instalación física de los equipos																				
Análisis para la ubicación de los puntos de Acceso																				
Instalación de los Puntos de Acceso																				
Configuración de la Arquitectura Inalámbrica																				
Configuración de los Access Point																				
Configuración del Radius																				
Configuración DHCP																				
Configuración de los equipos de acceso																				
Pruebas de acceso en equipos móviles																				
Despliegue de la configuración a todos los equipos																				

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El método de encriptación AES es en la actualidad el algoritmo de cifrado más seguro en el sector de las tecnologías de la información, es utilizado en diversidad de aplicaciones.
2. Siendo AES un algoritmo público, varios han sido los intentos por burlar su seguridad, pero no se reconoce ninguno que pueda lograrlo.
3. El método de acceso inalámbrico se está haciendo cada vez más popular en los hogares y en las empresas, debido a la movilidad que brinda al usuario.
4. Los nuevos equipos portátiles obligan a los usuarios utilizar cada vez más los medios inalámbricos para acceder a su información, siendo cada vez de más importancia las velocidades de acceso y los métodos de seguridad.
5. El método de autenticación 802.1x/PEAP es un punto importante en la seguridad, para no tener que estar cambiando la clave de acceso cada vez que un usuario se retira de la empresa.

RECOMENDACIONES

1. Para el cifrado AES utilizar en lo posible claves de 128bits para que no consuma recursos memoria y CPU.
2. Para que el acceso inalámbrico funcione correctamente se necesita brindar un mantenimiento anual probando el área de cobertura, para este caso podemos utilizar un equipo portátil y movilizarse por todo el local revisando, conectividad, potencia de la señal y velocidad de acceso.
3. Si se utiliza este acceso inalámbrico para intercambiar paquetes de voz sería recomendable aplicar QoS.

ANEXO A
ARCHIVO DE CONFIGURACIÓN DEL ACCESS POINT

```
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname WIFI-1A
!
enable secret 5 $1$F2XZ$tLzOMCbVJJqNCMB0eixzu.
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.101.2.3 auth-port 1645 acct-port 1646
!
aaa authentication login eap_methods group rad_eap
!
aaa session-id common
!
!
dot11 syslog
!
dot11 ssid empresaX
   vlan 6
   authentication open eap eap_methods
   authentication network-eap eap_methods
   authentication key-management wpa version 2
   mbssid guest-mode dtim-period 75
!
dot11 ssid empresaXvisita
   vlan 100
   authentication open
   authentication key-management wpa version 2
   mbssid guest-mode dtim-period 75
   wpa-psk ascii 7 124A080700581F05123D753B622123


!
username Cisco password 7 123A0C041104
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 encryption vlan 6 mode ciphers aes-ccm
 !
 encryption vlan 100 mode ciphers aes-ccm
 !
```

```
 ssid empresaX
 !
 ssid empresaXvisita
 !
 mbssid
 station-role root
!
interface Dot11Radio0.2
 encapsulation dot1Q 2 native
 no ip route-cache
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio0.6
 encapsulation dot1Q 6
 no ip route-cache
 bridge-group 6
 bridge-group 6 subscriber-loop-control
 bridge-group 6 block-unknown-source
 no bridge-group 6 source-learning
 no bridge-group 6 unicast-flooding
 bridge-group 6 spanning-disabled
!
interface Dot11Radio0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 bridge-group 100 subscriber-loop-control
 bridge-group 100 block-unknown-source
 no bridge-group 100 source-learning
 no bridge-group 100 unicast-flooding
 bridge-group 100 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 dfs band 3 block
 channel dfs
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
```

```
 duplex auto
 speed auto
!
interface FastEthernet0.2
 encapsulation dot1Q 2 native
 no ip route-cache
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface FastEthernet0.6
 encapsulation dot1Q 6
 no ip route-cache
 bridge-group 6
 no bridge-group 6 source-learning
 bridge-group 6 spanning-disabled
!
interface FastEthernet0.100
 encapsulation dot1Q 100
 no ip route-cache
 bridge-group 100
 no bridge-group 100 source-learning
 bridge-group 100 spanning-disabled
!
interface BVI1
 ip address 10.101.0.11 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.101.0.1
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
radius-server host 10.101.2.3 auth-port 1645 acct-port 1646 key 7 101D04091744010A34
bridge 1 route ip
!
!
!
line con 0
line vty 0 4
!
end
```

ANEXO B
CONFIGURACION DE LOS EQUIPOS PORTATILES

B.1 Configuración de los Equipos de datos Corporativos

Primero debemos decir que la maquina al ser corporativa debe estar ingresada a dominio y debe contar como mínimo con WinXP with SP3 como sistema operativo, los pasos se muestran a continuación:

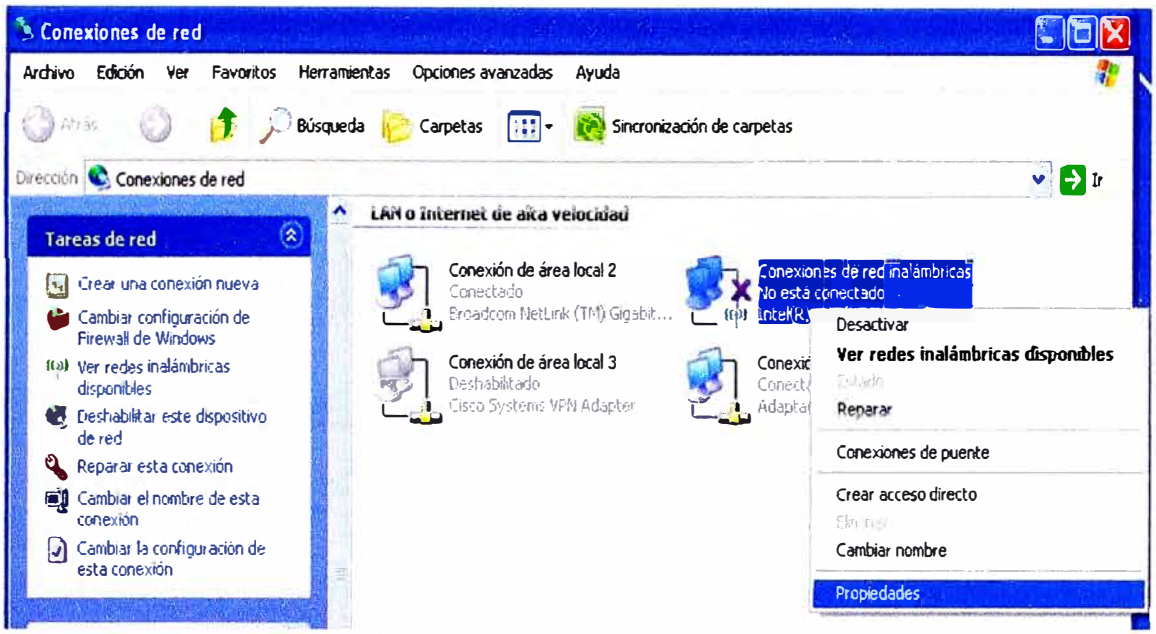

FIGURA B.1 Paso 1 Ingresar a Propiedades Inalámbricas. Fuente: Elaboración Propia.

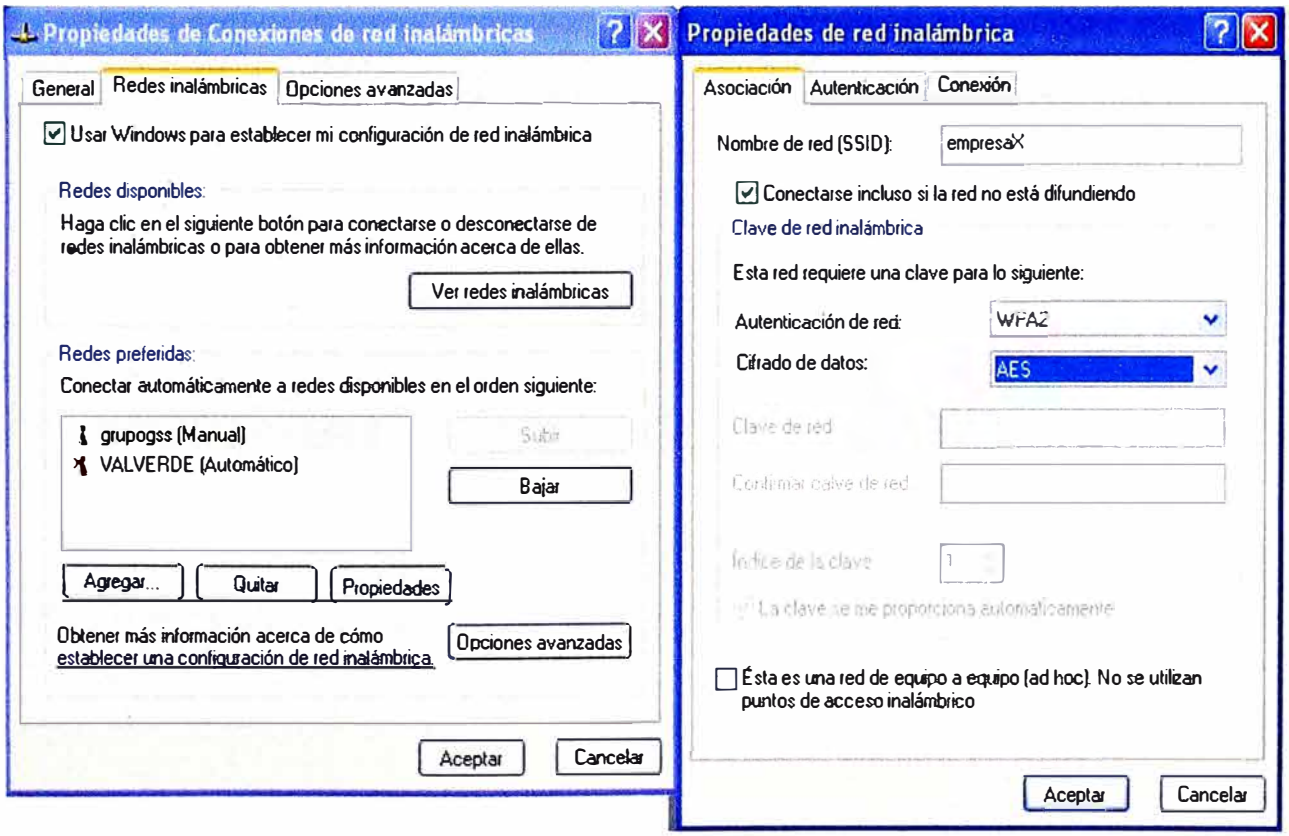

FIGURA B.2 Paso 2 Creación del SSID. Fuente: Elaboración Propia.

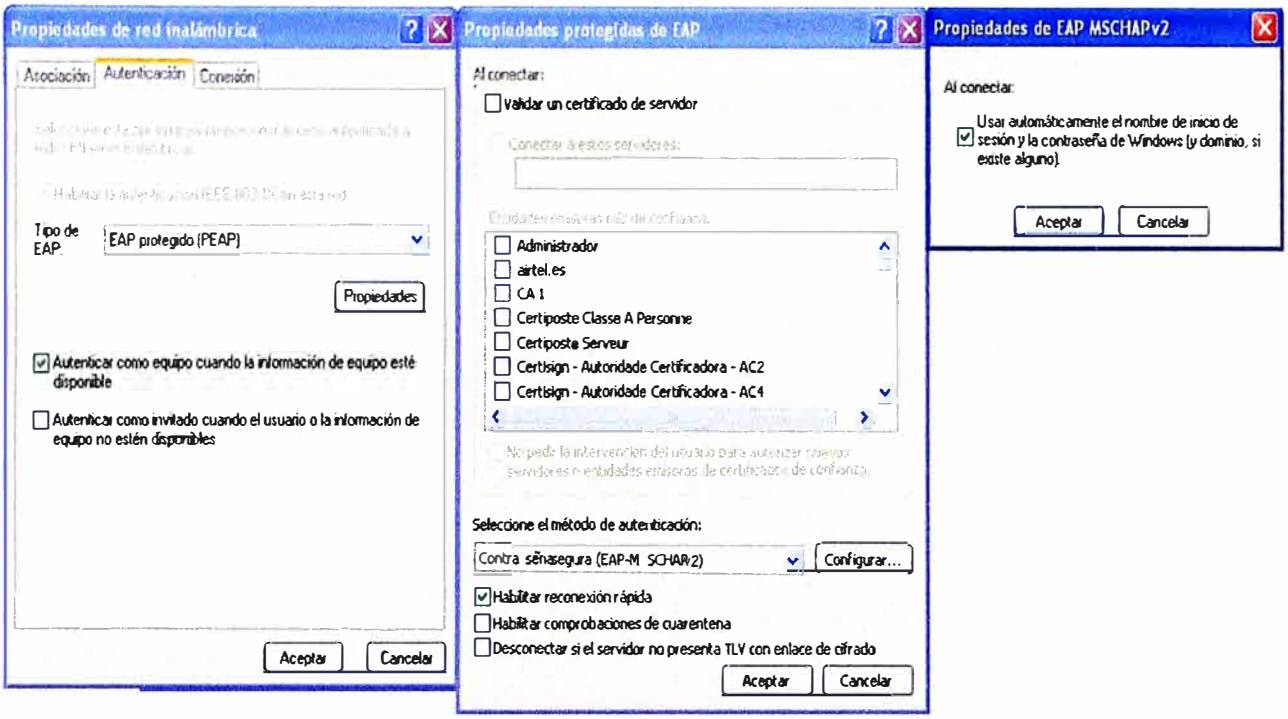

FIGURA B.3 Paso 3 Método de autenticación. Fuente: Elaboración Propia.

B.2 Configuración de los Equipos de Datos de los Visitantes

Para los visitantes la configuración es más sencilla, solo tienen que brindar doble click al SSID empresaXvisita y colocar la clave **3mpr3saXv1s1ta**, como se muestra en la Figura B.4.

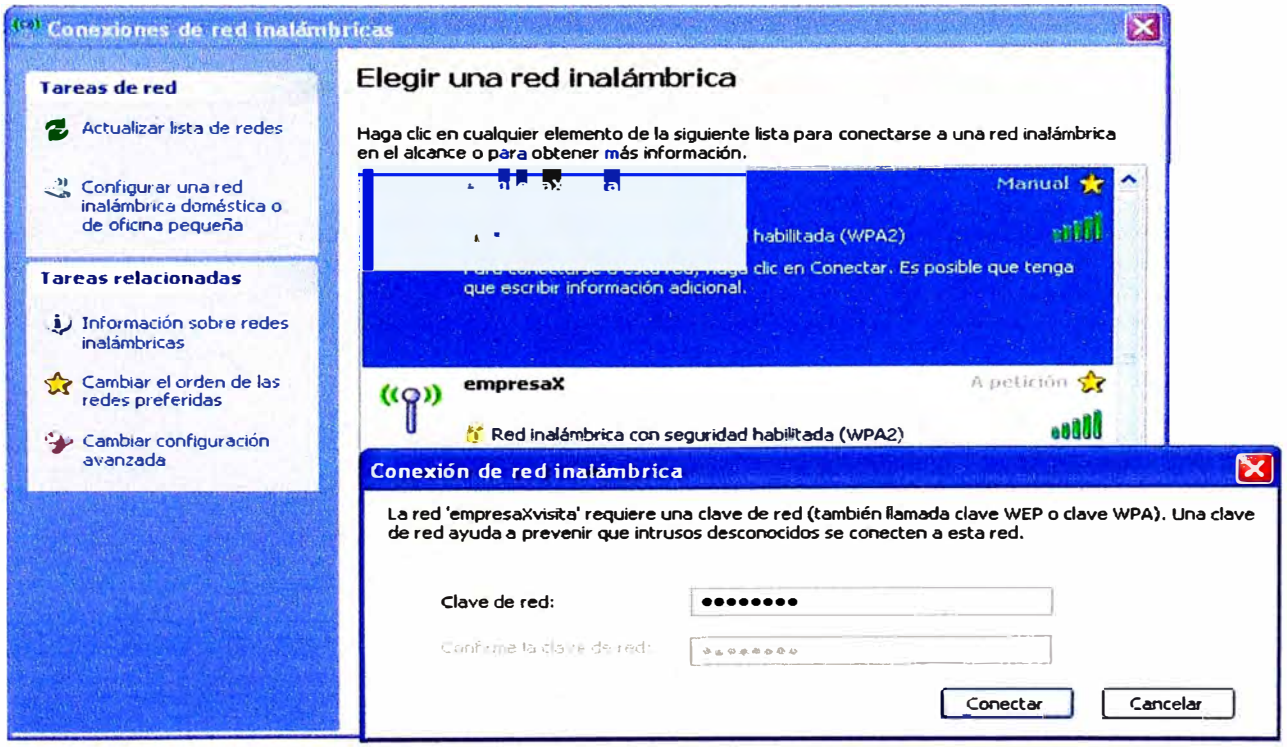

FIGURA B.4 Ingresando la clave para ingresar a la red visita. Fuente: Elaboración Propia.

ANEXO C
GLORARIO DE TERMINOS

- AES.- (Advanced Encryptation Standard) Es el nombre que se le brindo al método de encriptación ganador del concurso publicado por NIST.
- AP.- (Access Point) Es un punto de acceso inalámbrico.
- BSA.- (Basic Service Area) Es el área de cobertura básica, hace referencia al área de cobertura ofrecida por el servicio BSS.
- BSS.- (Basic Service Set) Es el servicio básico en una red inalámbrica, este está compuesto por un AP.
- CDMA.- (Code Division Multiple Access) Es un término genérico para varios métodos de multiplexación o control de acceso al medio basados en la tecnología de espectro expandido.
- CSMA/CA.- (Carrier Sense Multiple Access with Collision Avoidance) Es un protocolo de control de redes de bajo nivel que permite que múltiples estaciones utilicen un mismo medio de transmisión.
- DES.- (Data Encryption Standard) Es un algoritmo de cifrado, es decir un método para cifrar información, escogido por FIPS en los Estados Unidos en 1976.
- DS.- (Distribution System) Es un termino utilizado en redes inalambricas Wi-Fi, para hacer referencia a la estructura que conecta los AP.
- DSSS.- (Direct sequence spread spectrum) También conocido en comunicaciones móviles como DS-CDMA (acceso múltiple por división de código en secuencia directa), es uno de los métodos de modulación en espectro ensanchado para transmisión de señales digitales sobre ondas de radio que más se utilizan.
- EAP.- (Extensible Authentication Protocol) Es una metodo de autenticación usada habitualmente en redes WLAN Point-to-Point Protocol.
- ESA.- (Extended Service Area) Es el area de covertura extendida, hace referencia al area de covertura ofrecida por el servicio ESS.
- ESS.- (Extended service set) Es el servicio extendido en una red inalambrica, este esta compuesto por varios AP.
- FHSS.- (Frequency hopping spread spectrum) El espectro ensanchado por salto de frecuencia es una técnica de modulación en espectro ensanchado en el cual la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor.
- GSM.- (Global System for Mobile Communications) Es un estandar para sistemas de telefonia movil.
- IBSS.- (Independent BSS) Es un Independiente BSS, en donde la comunicación inalambrica entre dos equipos no pasa por un access point.

- IEEE.- (Institute of Electrical and Electronics Engineers) Es una asociación técnico-profesional mundial, dedicada a la estandarización, entre otras cosas.
- LAN.- (Local Area Network) Es una red de area local, generalmente compuesta por computadoras y otros perifericos.
- MAC.- (Media Access Control) En las redes de computadoras, la dirección MAC es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una tarjeta o dispositivo de red
- MAN.- (Metropolitan Area Network) Una red de área metropolitana es una red de alta velocidad que da cobertura en un área geográfica extensa.
- MIMO.- (Multiple-Input Multiple-Output) Se refiere específicamente a la forma como son manejadas las ondas de transmisión y recepción en antenas para dispositivos inalámbricos como enrutadores.
- NIST.- (National Institute of Standards and Technology) Es una agencia federal tecnologica que trabaja con la industria para desarrollar y aplicar tecnologias, estandares y medidas.
- OFDM.- (Orthogonal frequency division multiplexing) La Multiplexación por División de Frecuencias Ortogonales, consiste en enviar un conjunto de ondas portadoras de diferentes frecuencias, donde cada una transporta información, la cual es modulada en QAM o PSK.
- PAN.- (Personal Area Network) Es una red de area personal, esta puede ser un computador.
- PEAP.- (Protected Extensible Authentication Protocol) Es un protocolo que encapsula el EAP dentro de un tunel TLS (Transport Layer Security).
- RADIUS.- (Remote Authentication Dial-In User Server) Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red.
- ROAMING.- Desplazamiento de una zona de covertura a otra.
- SSID.- (Service Set IDentifier) Es el identificador o nombre que se le brinda a una red inalambrica.
- STA.- (station) Hace referencia a un equipo, este puede ser una PC, Laptop o un telefono 3G.
- TCP.- (Transmission Control Protocol) Es un protocolo de capa 4 según el modelo OSI, es un protocolo de comunicación orientado a conexión y fiable a nivel de transporte
- UDP.- (User Datagram Protocol) Es un protocolo de capa 4 según el modelo OSI, es un protocolo de comunicación no orientado a conexión.
- WAN.- (Wide Area Network) Es una red de área amplia.

- WEP.- (Wired Equivalent Privacy) Es un método de cifrado inalámbrico.
- Wi-Fi.- Es el nombre que se le brindo al estándar IEEE 802.11b.
- WiMAX.- (Worldwide Interoperability for Microwave Access) Es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,3 a 3,5 Ghz.
- WPA.- (Wi-Fi Protected Access) Es un sistema para proteger las redes inalámbricas, creado para corregir las deficiencias del sistema previo WEP.
- WPA2.- (Wi-Fi Protected Access 2) Es un sistema para proteger las redes inalámbricas, creado para corregir las vulnerabilidades detectadas en WPA.
- WPA2-ENTERPRISE.- Es el WPA2 con autenticación por 802.1x/EAP.
- WPA2-PSK.- Es el WPA2 con autenticación por clave pre-compartida.
- WPA-ENTERPRISE.- Es el WPA con autenticación por 802.1x/EAP.
- WPA-PSK.- Es el WPA con autenticación por clave pre-compartida.

BIBLIOGRAFÍA

[1].- National Institute of Standards and Technology (NIST) - FIPS-197
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2].- Daemen & Vincent Rijmen - A Specification for Rijndael, the AES Algorithm
http://www.comms.engg.susx.ac.uk/fft/crypto/aesspec.pdf

[3].- Pejman Roshan & Jonathan Leary - "802.11 Wireless LAN Fundamentals"
Cisco Press, USA 2003.

[4].- IEEE - IEEE Std 802.11–2007
http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[5].- IEEE - IEEE Std 802.11n–2009
http://standards.ieee.org/getieee802/download/802.11n-2009.pdf

[6].- IEEE - IEEE Std 802.11x
http://standards.ieee.org/getieee802/download/802.1X-2010.pdf

[7].- IEEE – IEEE Std 802.11i-2004
http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[8].- Lawrence C. Washington – "Introduction to Cryptography with Coding Theory"
Prentice Hall, 2002.

[9].- Cisco Systems Inc. – "Fundamentos de Seguridad de Redes"
Pearson Educación S.A., 2005