IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS DE SEGURIDAD INFORMÁTICA DEL ESTÁNDAR IEEE 802.16 BASADOS EN SOLUCIONES CRIPTOGRÁFICAS

JOSE IGNACIO CARDONA CAICEDO

JOHN JAMES PINO GOMEZ

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERIA ELECTRÓNICA Y TELECOMUNICACIONES

Departamento de Sistemas

Línea de investigación: Seguridad Informática

POPAYÁN

2008

IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS DE SEGURIDAD INFORMÁTICA DEL ESTÁNDAR IEEE 802.16 BASADOS EN SOLUCIONES CRIPTOGRÁFICAS

JOSE IGNACIO CARDONA CAICEDO

JOHN JAMES PINO GOMEZ

TRABAJO DE GRADO

DIRECTOR

ING. SILER AMADOR DONADO

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERIA ELECTRÓNICA Y TELECOMUNICACIONES

Departamento de Sistemas

Línea de investigación: Seguridad Informática

POPAYÁN

2008

Nota de aceptación

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Popayán ___ de ___ de 2008

LISTA DE ACRÓNIMOS

AES: Advanced Encription Standard (Estándar de Encriptación avanzada)

ARQ: Automatic Repeat Request (Solicitud de Repetición Automática)

AK: Authorization Key (Clave de Autorización)

BER: Bit Error Rate (Tasa de Errores de Bits)

BWA: Broadband Wireless Acces (Acceso Inalámbrico de Banda Ancha)

CBC: Cipher Block Chain (Cadena de Bloque Cifrado)

CCM: Counter With Cipher Block Chain MAC (Contador con Cadena de Bloque cifrado de la MAC)

CID: Channel Identifier (Identificador de Canal)

DES: Data Encrypytion Estandar (Estándar de Encriptación de Datos)

DSA: Dynamic Service Adition (Adición Dinámica de Servicio)

DSL: Digital Suscriber Line (Línea Digital de Abonado)

EAP: Extensible Authentication Protocol (Protocolo de Autenticación Extensible)

EB: Estación Base

ES: Estación Suscriptora

ISO: Organización internacional para la estandarización

KEK: Key Encription Key (Clave de Cifrado de Llave)

LOS: Line of Sight (Línea de Vista)

MAC: Médium Acces Control (Control de Acceso al Medio)

NLOS: Non Line of Sight (Sin Línea de Vista)

PDU: Protocol Data Unit (Unidad de Datos de Protocolo)

PHY: Physical (Capa Física)

PKM: Privacy Key Management (Gestión de clave Privada)

PTM: Point to Multipoint (Punto a Multipunto)

QoS: Quality of Service (Calidad de Servicio)

RSA: Rivest, Shamir y Adlerman (Algoritmo matemático para el cifrado y descifrado de llaves públicas y privadas)

SA: Security Associations (Asociaciones Seguras)

SAID: Security Association Identifier (identificador de Asociaciones Seguras)

SGSI: Sistema de Gestión de Seguridad de Información

SOM: System Operative Margin (Margen Operativo del Sistema)

TEK: Traffic Encryption Key (Claves de Cifrado de Trafico)

WiMAX: Worlwide Interoperability Microwave Access (Interoperabilidad Mundial para Acceso por Microondas)

WMAN: Wireless Metropolitan Area Network (Red de Area Metropolitana Inalámbrica)

X.509: Certificado que identifica a las partes comunicadas entre EB Y ES.

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

TABLA DE CONTENIDO

INTRODUCCIÓN

El estándar IEEE 802.16 conocido a nivel mundial como WiMAX se ha diseñado para brindar acceso inalámbrico de banda ancha global, con capacidad, robustez y desempeños altos dando soporte a tecnologías fijas, portátiles y móviles sobre coberturas extensas, trabaja tanto en bandas licenciadas como no licenciadas y tiene la posibilidad de desenvolverse en escenarios que no reúnen condiciones de línea de vista. La seguridad de esta clase de redes representa una necesidad dada las características del medio por donde se transporta la información, al igual que en las redes cableadas, las redes WiMAX pueden presentar las mismas vulnerabilidades en seguridad las cuales se basan en las debilidades y fallas que presenta el medio físico y los mecanismos de autenticación y cifrados presentes, siendo estos últimos los más comunes en los que se basan los métodos de ataques. Estos métodos de ataques pueden aprovechar la vulnerabilidad de la seguridad y los pocos conocimientos que pueden llegar a tener los administradores de la red, ya que como es sabido el desconocimiento favorece a todos los delincuentes informáticos deseosos de romper la seguridad de cualquier sistema. Es por esto que no hay que seguir únicamente mecanismos de protección de seguridad enmarcados dentro de políticas adecuadas y consistentes siguiendo listas de comprobación de seguridad y ciertas buenas prácticas, consiguiendo la defensa más básica, lo que se busca es preservar la seguridad en esta clase de redes analizando las diferentes situaciones y tomando decisiones basadas en la total comprensión del riesgo en función de amenazas, vulnerabilidades y exposiciones frente a cualquier clase de contramedida empleada, ya que el conocimiento del riesgo proporciona los medios necesarios para priorizar y asignar los recursos disponibles para llevar a la práctica ciertas contramedidas para lograr reducir al máximo los riesgos se seguridad informática de las redes WIMAX.

El objetivo principal que se quiso alcanzar con el presente trabajo de grado fue el de identificar y analizar los riesgos de seguridad informática del estándar IEEE 802.16 analizando los objetivos de cada protocolo de éste y comprobar si los algoritmos criptográficos que soportan los protocolos cumplen con el nivel de seguridad esperado, esto debido a la masificación de la banda ancha que están presentando las comunicaciones inalámbricas WiMAX en este momento, las cuales están teniendo un auge importante en el ámbito empresarial, comercial, doméstico y universitario, ya que su fácil instalación así como la movilidad que ofrecen con respecto a las redes cableadas, hacen de su principal ventaja un gran problema en lo que a seguridad se refiere.

El presente trabajo de grado está estructurado en cuatro capítulos dentro de los cuales se desarrollaron todos los objetivos del proyecto. El capítulo uno presenta los aspectos generales de la seguridad del estándar, aquí se explican algunas generalidades, su evolución, su arquitectura de seguridad analizando los mecanismo de seguridad que el 802.16 utiliza en su subcapa de seguridad de la capa MAC como son los procesos de autenticación, la administración de claves llevadas a cabo por el protocolo PKM, los procesos de confidencialidad e integridad de los datos. Se ve también la necesidad de utilizar estándares de seguridad de la información para poder llevar a cabo políticas de seguridad las cuales permitan regular la forma como una organización previene y enfrenta los riesgos informáticos siguiendo una serie de reglas y procedimientos identificando sucesos negativos del sistema y la posibilidad de su ocurrencia. Se identifican y estudian también de manera general los métodos de cifrado utilizados por el estándar dando una explicación de cómo criptoanálisis y algoritmos de cifrado están íntimamente ligados.

En el capítulo dos se presenta el estudio detallado de los posibles riesgos de seguridad a los que el estándar se puede ver expuesto como vulnerabilidades, amenazas y métodos de ataques; se hace un análisis de los algoritmos de seguridad (DES, AES y RSA) que el 802.16

utiliza en la subcapa de seguridad, analizando que tan seguros son estos algoritmos que el protocolo de cifrado de datos utiliza, y que tan seguro es el protocolo PKM al transportar claves entre Estaciones Base y Estaciones Suscriptoras respectivamente. Finalmente se dan algunas soluciones de seguridad propuestas para el estándar. En este capítulo se da solución al primer objetivo específico propuesto, Analizar los riesgos de seguridad informática de los protocolos de Encapsulamiento para el cifrado de datos y Gestión de clave privada, basándose en estrategias de criptoanálisis, dentro de los procesos de autenticación, confidencialidad e integridad de datos.

En el capitulo tres se estudian algunos estándares de seguridad de la información como el RFC 2196, el BS7799 y los pertenecientes al ISO 17799 y 27000; en este apartado se analiza cual de todos estos se adapta mejor a los objetivos del presente trabajo de grado dando solución al segundo objetivo especifico, Identificar el estándar de seguridad de información adecuado para garantizar un nivel de protección alto enmarcado dentro del ámbito de la realización del proyecto.

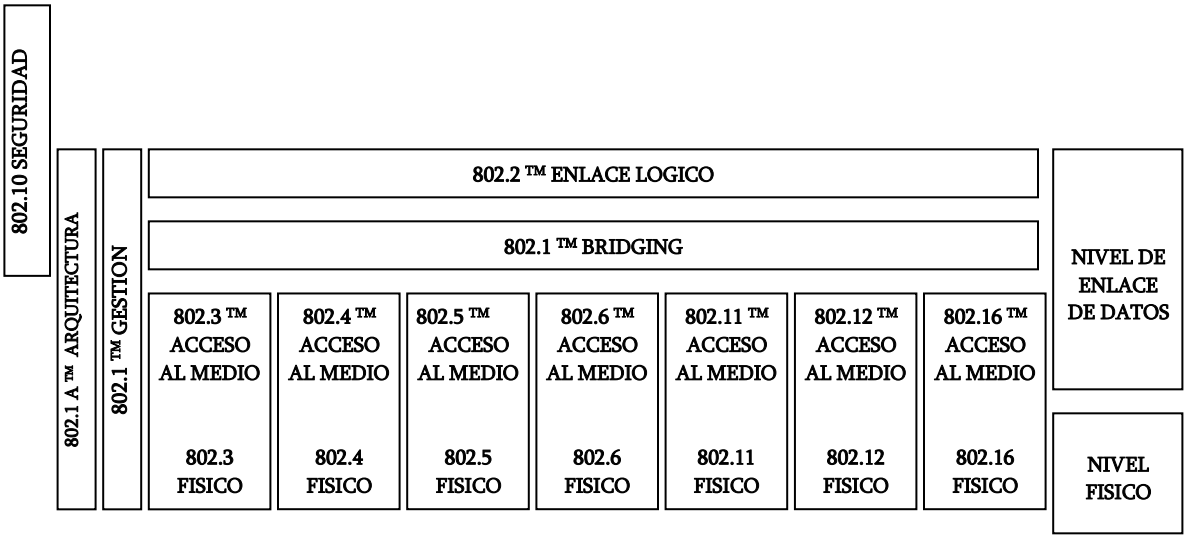
El capitulo cuatro describe como se realizó el diseño para la Red Universitaria de Popayán (RUP) bajo el estándar 802.16, siguiendo una estrategia para llevar a cabo el sistema de gestión de la información en el diseño propuesto de la red después de haber analizado de manera general la seguridad de cada sede que conforma la RUP y así ajustar el diseño de ésta al estándar de seguridad de la información escogido, en este capítulo se da solución al tercer y cuarto objetivo especifico, realizar un diseño para la Red Universitaria de Popayán bajo la norma IEEE 802.16 con un nivel de seguridad alto basado en soluciones criptográficas seguras y ajustar el diseño propuesto para la Red Universitaria de Popayán bajo la norma IEEE 802.16 al Estándar de Seguridad definido en el desarrollo del proyecto que disminuya sus amenazas y vulnerabilidades.

CAPÍTULO 1. ASPECTOS GENERALES DE SEGURIDAD

1.1 GENERALIDADES DEL ESTÁNDAR IEEE 802.16

El estándar IEEE 802.16 emerge como una de las tecnologías de Acceso Inalámbrico más prometedoras en el mundo de las redes MAN y dentro de la familia de estándares IEEE 802.x es una de las que mayor aceptación ha ganado en el mundo debido a las grandes ventajas que presenta además de la facilidad de utilización y mantenimiento. La figura 1 muestra la ubicación del estándar dentro de la jerarquía de estándares IEEE 802 [1].

Figura 1. Ubicación del Estándar IEEE 802.16 en la familia de estándares IEEE 802.x [1].



El estándar IEEE 802.16 permite la implementación de redes de Banda Ancha de Acceso Inalámbrico en grandes áreas, las cuales son capaces de proveer cualquier tipo de servicio debido a su gran capacidad de transportar información [1]. Estas redes han ganado gran acogida dentro de este mercado en los últimos años haciendo que cada vez más las grandes empresas proveedoras de equipos como Intel, Nokia, Samsung y Motorola las

cuales apoyan a este estándar lancen al mercado dispositivos que cumplan con las especificaciones del estándar y a su vez, muchas empresas adquieren esta tecnología como solución a sus necesidades de conexión como ETB, Telefónica Telecom y Orbitel que tienen autorización para ofrecer el servicio a nivel nacional, mientras que Telmex, Avantel, Comsat y Emcali, entre otras, lo pueden hacer regionalmente.

Sin embargo, la rápida penetración y expansión en el mercado y la utilización del aire como medio de transporte de datos, hacen que la seguridad sea un punto crítico para la integridad de la información que en ella fluye. Por esta razón la seguridad en la red ha sido un tema primordial en el diseño del estándar y se han tomado medidas como el cifrado de datos, protocolos de seguridad más robustos que en estándares anteriores como el IEEE 802.11, pero a pesar de estas medidas aun se presentan ataques y falencias a la hora de definir la arquitectura de seguridad del estándar, como la falta de definiciones explicitas de autorizaciones para las Asociaciones de Seguridad (SA), la necesidad de mutua autenticación, las vulnerabilidades de autenticación, la falla en la administración de claves, los errores en la protección de datos entre otros, los cuales se abordarán con más detalle en el capítulo dos [1].

1.2 EVOLUCIÓN DEL ESTÁNDAR IEEE 802.16

Desde su concepción en los años 90's, el estándar IEEE 802.16 ha tenido como objetivo primordial el de proveer diferentes tipos de servicios sobre una red de acceso inalámbrico de alta transferencia de bits. Para ello define unas especificaciones de interfaz incluyendo MAC (Medium Acces Control), la cual se describirá en detalle más adelante, y la PHY (Capa Física). Todo esto de acuerdo con el nivel de enlace de datos y el nivel físico del modelo de interconexión de sistemas abiertos (OSI) de ISO [1].

A pesar de tener estas especificaciones desde un principio para cumplir con los objetivos propuestos, se han visto algunas fallas principalmente en la capa MAC, donde la gestión en el envío de la información se realiza sin cifrar los datos para facilitar su funcionamiento adecuado, de este modo, en una escucha pasiva del canal de la red se podría acceder fácilmente a la información sin cifrar. Debido a esta situación se han realizado diferentes correcciones que han originado varias revisiones y adiciones a las especificaciones para las capas MAC y PHY agregando nuevas funciones a las mismas a través del tiempo. Estas correcciones se presentan en diferentes versiones del estándar [1]:

IEEE 802.16: 2001: Primera versión del estándar en la que se daban las primeras especificaciones para la capa MAC y PHY, proporciona acceso inalámbrico de banda ancha, configuración de red Punto a Punto (P2P) o Punto multipunto (PMP). Soporte para TDD (Multiplexación por División de Tiempo) y FDD (Multiplexación por División de Frecuencia). A diferencia de 802.11 o Wi-Fi que emplea CSMA/CD para transmitir, 802.16 emplea un paradigma totalmente diferente para realizar esta función controlado por las estaciones base (EB). Opera en la banda de los 10 – 66 GHz, al ser éstas altas frecuencias solo es funcional en ambientes LOS (Línea de Vista). Emplea modulación QPSK, QAM-16 y QAM-64 con la habilidad para cambiar entre modulaciones dependiendo de diferentes condiciones entre ellas las climáticas. Provee diferentes niveles de QoS (Calidad de servicio) controlando parámetros como la suma de retardos temporales dentro de la red (latencia) y la variación de algunos paquetes de datos recibidos debido a la latencia (jitter). El núcleo de la seguridad del estándar radica en la subcapa de privacidad perteneciente a la capa MAC utilizando para ello algoritmos de cifrado de datos en sus mensajes entre las Estaciones Base (EB) y las Estaciones Suscriptoras (ES) y haciendo uso de certificados digitales X.509 [1].

IEEE 802.16c:2002: Publicado en Diciembre de 2002, estándariza más detalladamente la tecnología inalámbrica, se corrigen algunos errores de la versión inicial definiendo un conjunto de prestaciones y funciones que son utilizadas en la implementación. Aumenta la interoperabilidad y consistencia entre equipos de diferentes fabricantes aumentando así la generalización y uso del estándar a futuro. Se agregan perfiles detallados para sistemas que operan en la banda de 10 – 66 GHz [1].

IEEE 802.16a: 2003: Publicado en Junio de 2003, introduce nuevas prestaciones como soporte para las bandas licenciadas de 2 – 11 GHz y de esta manera tener la capacidad de penetrar barreras por tratarse de frecuencias bajas y así ser viable su utilización en ambientes NLOS (Sin Línea de Vista). Nuevas especificaciones MAC y PHY para un mejor manejo de la interferencia producida por las multitrayectorias, además de utilizar un nuevo arreglo de antenas lo cual produce un mejor manejo de la potencia empleada por el sistema. Nuevo soporte de multiplexación por división de frecuencia ortogonal (OFDM) para evitar interferencias con otros sistemas de red que operan en el mismo rango de frecuencia 2 – 11 GHz. Se mejoró la seguridad al solicitar autenticación del emisor para algunos mensajes MAC. QoS específico para optimizar servicios de datos, voz y video así como también ARQ para mejorar el desempeño punto a punto. Soporte para redes en malla. Fue nombrada en un principio como Wireless HUMAN por Red de Área Metropolitana de Alta Velocidad no Licenciada [1].

IEEE 802.16: 2004: Publicación realizada en Junio de 2004, es la fusión entre IEEE 802.16: 2001 e IEEE 802.16c: 2002 integrando toda la familia de estándares existentes en ese momento bajo un mismo documento. Dio soporte a bandas licenciadas y no licenciadas pero para la banda de 10 – 66 GHz requiere de ambientes LOS, a su vez para frecuencias menores a 11 GHz soporta ambientes NLOS. La capa MAC soporta arquitectura PMP y en malla. Esta versión del estándar es la que se utiliza para dar la certificación de WiMAX [1].

IEEE 802.16e: 2005: provee funciones de transferencia de comunicación entre celdas mientras el usuario se mueve en el área de servicio (handover) entre Estaciones Base (EB), estas entidades proveen funcionalidad sobre el enlace controlando la admisión y la gestión de recursos de radio en los enlaces de subida y de bajada, dando la posibilidad de tener Estaciones suscriptoras (ES) móviles, estas ES son las entidades que permiten la recepción de información en el lado del cliente y la transmisión desde este hacia la EB[1].

IEEE 802.16f: 2005: Define la MIB (Base para la Gestión de la Información) para las capas MAC y PHY. Define además un procedimiento para crear un estándar de Gestión de Red para sistemas basados en IEEE 802.16 [1].

Con todas estas revisiones y mejoras adoptadas por el estándar se pueden determinar algunas ventajas o beneficios que este tipo de red provee a sus usuarios [1]:

Gran cobertura: En ambientes LOS hasta 50Km; para ambientes NLOS hasta 8KM

Alta capacidad de transferencia de bits: Idealmente la red es capaz de transferir datos a 70Mbps

Soporte para ambientes NLOS: En las frecuencias indicadas es posible implantar una red bajo el estándar sin tener línea de vista.

Tamaño flexible de canales: Esta es una prestación muy importante ya que se puede configurar el ancho de los canales de comunicación optimizando así su uso y evitando el desperdicio de recursos de red.

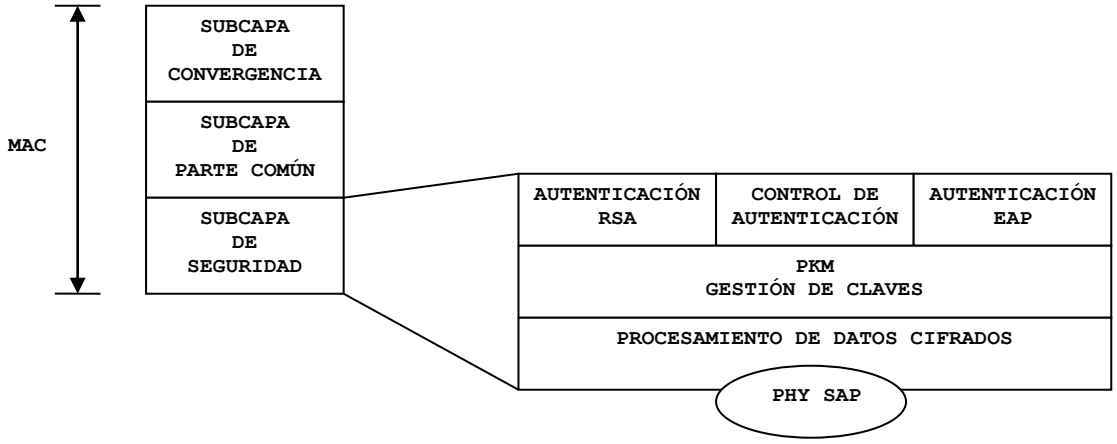
Soporte para redes en malla: Esta opción permite a las ES hacer enrutamiento entre unas y otras sin pasar por la EB haciendo esta función transparente a ella.

Soporte para usuarios móviles: Una ES puede tener acceso a la red moviéndose a una velocidad vehicular. Esto da a la ES la posibilidad de tener servicio usando dispositivos móviles.

1.3 ARQUITECTURA DE SEGURIDAD DEL ESTÁNDAR IEEE 802.16

A continuación se analizarán los mecanismos de seguridad que utiliza el estándar 802.16. Los servicios de seguridad están ubicados en la capa de control de acceso al medio MAC, esta capa está dividida en tres subcapas que se muestran en la figura 2 [9].

Figura 2. Subcapa de seguridad de la capa MAC.



Subcapa de Convergencia: Esta subcapa es una interfaz lógica; se encarga del tratamiento de protocolos de capas superiores y se utiliza para mapear tráfico específico de la capa de transporte hacia la capa MAC a través de características como supresión de cabeceras,

empaquetado y fragmentación de tramas. Esta subcapa y la MAC proveen eficiencia en el transporte de tráfico [24].

S*ubcapa de Parte Común*: Se localiza en la parte central, maneja los canales de acceso, el establecimiento y mantenimiento de la conexión y calidad de servicio QoS, se encarga de funciones de adaptación del enlace y solicitud de repetición automática ARQ para mantener las tasas de errores de bits BER dentro de los niveles fijados mientras maximiza el rendimiento en la transmisión de la información, especialmente en el trabajo en bandas de 2-11GHz en topologías algo más complejas que las Punto Punto (PTP) y Punto Multipunto (PTM), como lo son las mallas [24].

Subcapa de seguridad: Especifica métodos de autenticación, control de autorizaciones, administración de llaves y el cifrado / descifrado de datos [24].

1.3.1 SUBCAPA DE SEGURIDAD. La componen Los protocolos de Encapsulamiento para el cifrado de datos, que define un conjunto de series criptográficas soportadas (grupos de algoritmos de cifrado de datos y autenticación) y las reglas para aplicarlas a la carga útil (payload), de la MAC; y el de Gestión de Clave Privada PKM, que describe como la EB distribuye claves a las ES clientes y a través del cual las EBs y ESs sincronizan sus llaves. Esta subcapa busca proveer control de acceso y confidencialidad sobre el enlace de datos [24].

1.3.2 PROCESOS DE AUTENTICACION 802.16. Dado que el estándar se diseñó para aplicaciones de red pública, virtualmente todas las transmisiones se cifran entre las EBs y las ESs brindando seguridad a los diferentes operadores con una profunda protección del servicio. La EB protege en contra de acceso no autorizado a estos servicios de transporte de datos mediante el cifrado permitiendo a los servicios asociados que fluyen a través de

la red. La privacidad se garantiza empleando el protocolo de autenticación PKM cliente/servidor en el cual la EB, el servidor, controla la distribución de material clave al cliente, la ES. Adicionalmente, los mecanismos de privacidad básica son reforzados agregando al control de protocolo autenticación de la ES basada en certificados digitales. Si durante la negociación de capacidades, la ES específica no soporta seguridad 802.16, los pasos de autorización e intercambio de llaves serán ignorados. Está previsto dentro del estándar que la EB debe considerar a la ES como auténtica, de otra manera la ES no será atendida [9].

A continuación se verá como estas entidades se autentican utilizando diferentes algoritmos de cifrado de clave privada como el DES y el AES; y de cifrado de clave pública asimétrica como el RSA, así como el protocolo de autenticación PKM. Los protocolos de seguridad y los algoritmos que estos utilizan se explican en detalle en el Anexo A, B, C y D.

- **AUTENTICACIÓN BASADA EN RSA.** Esta forma de autenticación utiliza el algoritmo criptográfico de clave pública RSA para autenticar la ES y la EB, utilizando claves diferentes para el cifrado y el descifrado de los datos, la ES envía una respuesta de autorización a la EB, esta verifica la identidad de la ES basado en un certificado proporcionado que después es contestado con los parámetros de seguridad usados para la conexión de estas entidades. En una configuración de Punto Multipunto PMP la EB es la entidad proveedora y es vista como el dispositivo de confianza por defecto, de esta forma el protocolo PKM no define el proceso de autorización para la EB en dirección a la ES. Este proceso de autenticación consta de tres mensajes: Mensaje de información de autenticación, Mensaje de autorización y mensaje de autorización de respuesta [9].

    - **Mensaje de Información de Autenticación:** La ES envía el mensaje de información de autenticación hacia la EB, este mensaje contiene el

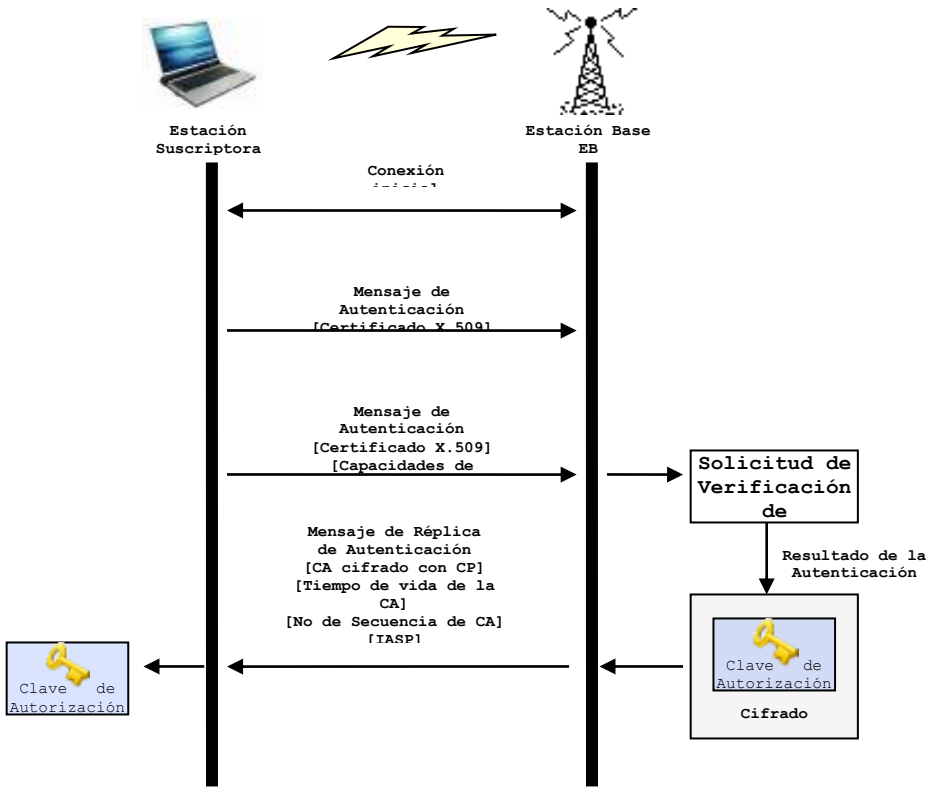
certificado de fabricante X. 509 el cual es utilizado por este o algún grupo de autoridades de la ES mostrando que la ES es un dispositivo de confianza. El mensaje de información de autenticación es utilizado para propósitos de información ya que el estándar permite que la EB ignore este mensaje y que su política de seguridad permita acceso solo a dispositivos conocidos con anterioridad [9].

- **Mensaje de Autorización:** La ES envía el mensaje de autorización hacia la EB, la ES pide los parámetros de seguridad para la conexión. El mensaje de autorización consiste de tres parámetros, el primero es el certificado digital X. 509 del fabricante para identificar la ES, este certificado contiene una llave pública propia la cual es utilizada por la EB para cifrar los parámetros de seguridad importantes y evaluar la respuesta. El cifrado es posible gracias a una llave privada la cual es propia del certificado. Otro de los parámetros del mensaje de autorización es una lista de algoritmos criptográficos soportados por la ES, esta lista tiene un formato definido el cual soporta métodos de seguridad que se presentan en la identificación entre la EB y la ES. La EB decide, basada en esta lista el uso de métodos de seguridad en la conexión. El tercer parámetro en el mensaje de autorización es el identificador de conexión CID. La ES posee múltiples conexiones lógicas con los niveles de la capa MAC que son reconocidos por el CID, esta petición de parámetros de seguridad son validos únicamente para el primer CID llamado el identificador básico de conexión [9].

- **Mensaje de Autorización de respuesta:** El mensaje de autorización de respuesta se envía desde la EB hacia la ES después de la verificación satisfactoria dada por el certificado X. 509. Este mensaje consiste en

múltiples parámetros, el primero es una llave de autorizaron AK de 160 bits la cual es utilizada como información de seguridad básica, otras claves como la de cifrado KEK y las de mensajes de autorización son heredadas de la llave de autorización AK. Este proceso de herencia de llaves es desempeñado por la ES y la EB independientemente, el contenido de las llaves simétricas no se envía por la interfaz de aire. Esta es una mejora de seguridad, de este modo la información de seguridad básica AK tiene que ser enviada por un medio más seguro. La ES cifra la llave de autorización AK con la llave publica que la ES le envió. Una parte importante en el esquema de seguridad es el refresco de llaves, haciendo limitado el tiempo de vida de éstas. La clave de autorización AK tiene un parámetro de tiempo de vida el cual es dado en el mensaje de autorización de respuesta, cuando el tiempo de vida termina la llave usada después de este tiempo ya no es válida dando como resultado que la EB genere múltiples AK para mantener la conexión. El mensaje de autorización de respuesta incluye un número de secuencia el cual es identificado en el momento de la conexión utilizando AK, el tiempo de vida de AK y el número de secuencia no es la única información importante en el mensaje de autorización de respuesta, ya que esta conexión se caracteriza por un conjunto de métodos y algoritmos de seguridad utilizados, la cual está representada como un identificador de asociaciones seguras SAID para el mensaje de autorización de respuestas. El proceso completo de autenticación se muestra en la figura 3 [9].

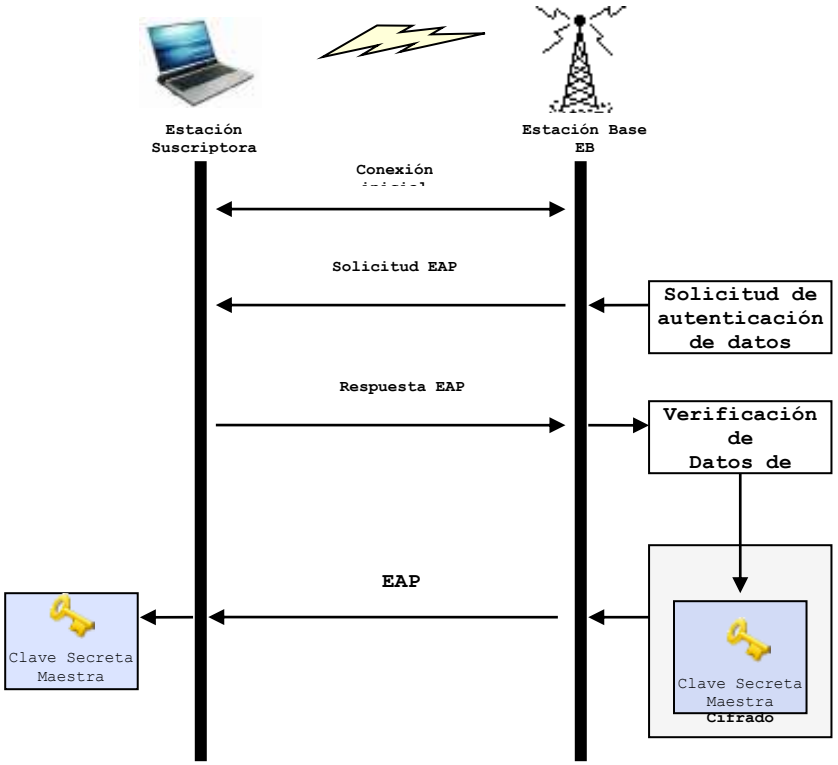
Figura 3. Proceso de autenticación 802.16 de la ES.



- **AUTENTICACION BASADA EN EAP.** Este método no es específico en su forma de autenticar la EB y la ES, en una petición de la EB se espera una respuesta satisfactoria por parte de la ES, el resultado de la comunicación entre estas entidades depende en su totalidad de los métodos con los cuales se encapsula el mensaje EAP cuando hay solicitud/respuesta entre la EB y la ES. Por otro lado, el estándar 802.16e introduce una alternativa para la autenticación basada en los certificados X.509, este nuevo esquema es considerado más flexible y está basado en este protocolo de autenticación EAP, el cual es cifrado directamente dentro del manejo de la información. Dos mensajes PKM adicionales para realizar solicitudes y enviar respuestas EAP, PKM EAP petición y PKM EAP respuesta

fueron introducidos en el transporte de datos EAP. Este proceso de autenticación se muestra en la figura 4 [9].

Figura 4. Autenticación EAP.

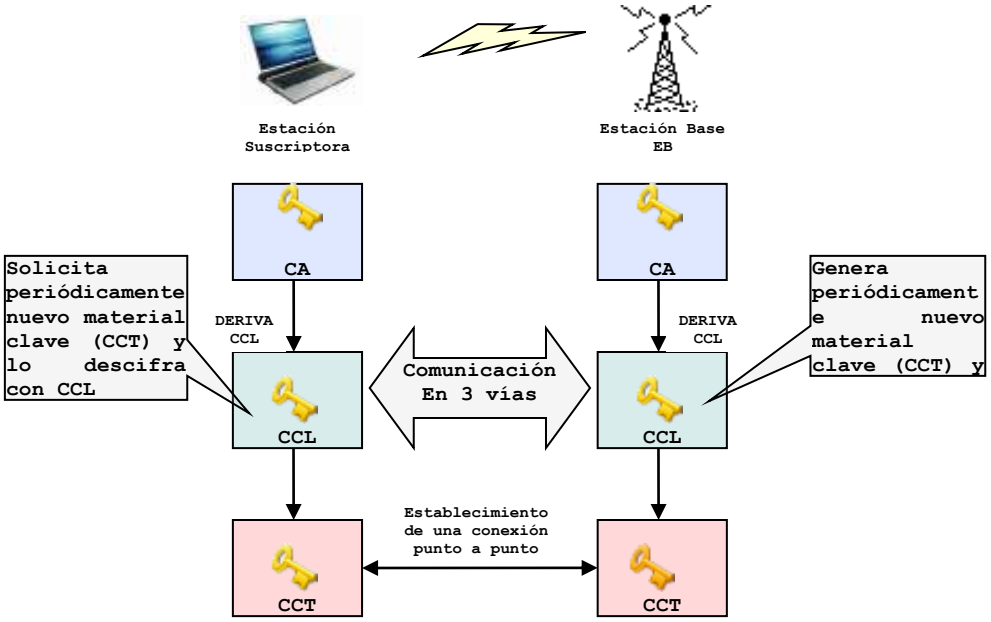


1.3.3 ADMINISTRACION DE LLAVES PKM. La administración de llaves se hace utilizando el protocolo PKM, este protocolo es el responsable de la sincronización y actualización de llaves entre la EB y la ES. El protocolo opera con múltiples llaves para realizar operaciones específicas, estas son organizadas jerárquicamente y la raíz de esta estructura es la clave de autorización AK, la cual se genera por la EB y es la encargada de llevar a cabo el proceso de autenticación. Esta AK es transmitida de manera segura hacia la ES siendo utilizada en la autorización e identificación. El proceso de cifrado/descifrado de datos requiere un cambio dinámico de llaves utilizando la clave de autorización AK. El proceso de cifrado de datos se lleva a cabo por la Llave de Cifrado de Trafico TEK esta es generada

en la EB la cual se asegura de que sea transmitida hacia la ES. El protocolo PKM define una llave extra para el transporte seguro de TEK a la ES llamada la Clave de cifrado KEK la cual es derivada desde la AK con un carácter estático también. Todo el proceso completo comienza generando una clave de autorización AK derivando todo hacia una KEK y finalmente se generan las llaves de administración y seguridad TEK's. El proceso completo de sincronización se muestra en la figura 5 [9].

1.3.4 CONFIDENCIALIDAD E INTEGRIDAD DE DATOS 802.16. El estándar IEEE 802.16 utiliza diferentes métodos para asegurar la confidencialidad y la integridad de los datos tanto de control como de carga útil en sus protocolos, muchos de ellos están basados en métodos criptográficos desde la autenticación, identificación y acceso a la red, tales como el DES y el AES, los cuales están definidos en una suite de capacidades o suite criptográfica la cual es utilizada por un dispositivo para autenticar y cifrar datos utilizando algoritmos criptográficos, esta suite criptográfica está definida por el fabricante del dispositivo y está basada en software o hardware criptográfico instalado en este. Esta información de cifrado está localizada en el formato de encabezado MAC genérico. El valor 0x01 indica el uso del algoritmo DES y el valor 0x02 indica el uso del algoritmo AES respectivamente [9].

Figura 5. Proceso de Operación del protocolo PKM.



1.4 ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

Debido a que la seguridad en los sistemas informáticos es un tema muy extenso no es necesario solamente abarcar la seguridad de las redes y la información que ella transporta. La seguridad de un sistema de información también depende de factores que influyen en el correcto funcionamiento de todo un complejo sistema de intercambio de información entre diferentes dependencias, ya sean internas o también externas como en el caso de empresas que tienen diferentes sucursales.

A lo largo del desarrollo de la informática y de sus aplicaciones en muchas áreas de la productividad del hombre se han venido creando necesidades más complejas, esto lleva a que las empresas adopten sistemas que sean capaces de manipular un inmenso flujo de información que se genera. Pero esta gran cantidad de información, en muchos casos es

crítica para la institución, también atrae a otro grupo de personas los cuales intentan "robar" esta pieza clave en el funcionamiento de ésta. Para evitar, minimizar y reaccionar ante esta clase de sucesos se han desarrollado desde hace un tiempo mecanismos que ofrecen pautas a seguir para fortalecer la seguridad integral de un sistema de información. Muchos de ellos se han convertido en estándares adoptados por las Instituciones que tienen a su cargo elaborar protocolos y políticas de diferente naturaleza a nivel mundial.

Las necesidades de protección frente a distintos tipos de ataques que se puedan ocasionar en un sistema de información pueden ser de diferentes características dependiendo del medio, es por eso que muchos países han desarrollado sus propios métodos, estándares y mecanismos de protección según sus propias necesidades. Muchos de estos estándares regionales han sido adoptados por otros países y se han convertido gradualmente en estándares aceptados a nivel mundial, es el caso del estándar británico BS7799, el cual ha sido adoptado por la ISO y convertido en el ISO 27000 [30].

En el capítulo tres se analizarán los estándares reconocidos mundialmente y se escogerá el más adecuado a las necesidades del desarrollo del trabajo de grado: ***RFC 2196***, desarrollado por la IETF como guía práctica para asegurar servicios e información. ***BS7799***, desarrollado por el British Estándar Institute (BSI), ha tenido una gran aceptación en todo el mundo dando origen a otros estándares de seguridad de la información. En la actualidad existen 3 partes del estándar. ***ISO 17799***, Es una familia de estándares adoptados por la ISO y que están basados principalmente en la serie BS7799 británica [30].

1.5 CRIPTOGRAFÍA MODERNA

La criptología, del griego *criptos* = oculto y *logos* = tratado, es el nombre con el cual se designa la unión de dos disciplinas: *Criptografía* y *Criptoanálisis*. La criptografía es la encargada de crear métodos o procedimientos para ocultar la información empleando diferentes técnicas y algoritmos. El criptoanálisis, es el encargado de romper esos métodos de ocultamiento de la información para recuperar el mensaje original. El desarrollo de las dos disciplinas ha sido paralelo ya que para cada método de cifrado existe su correspondiente método de descifrado [12].

El mensaje original o también llamado *texto plano,* sufre diferentes transformaciones en el emisor para tratar de hacerlo no entendible, a través de la aplicación de diferentes técnicas que han venido creciendo en complejidad a lo largo del tiempo para adaptarse a la creciente necesidad de proteger la información. Luego de esta transformación, el mensaje original cifrado, ahora llamado, *criptograma,* es transmitido por un canal que generalmente es inseguro. En recepción este criptograma llega a su destino, el cual con conocimiento de la clave *K*, es idealmente el único capaz de convertirlo nuevamente en el mensaje original [12].

1.5.1 CLASIFICACIÓN. A partir que algunos factores importantes volvieron más complejos los algoritmos criptográficos, como la gran capacidad de procesamiento que tienen actualmente los equipos de cómputo lo cual hace que se disponga de una potencia de cálculo mucho mayor, también, el avance en las matemáticas, las cuales permitieron encontrar y definir con claridad sistemas criptográficos estables y seguros, y del mismo modo, aparecían necesidades de seguridad debido al surgimiento de actividades que requerían el ocultamiento de datos, con lo cual la criptografía experimentó un fuerte

avance, apareciendo nuevos y complejos sistemas criptográficos los cuales utilizan técnicas de cifrado según el tratamiento del mensaje [12].

El estándar 802.16 trabaja con el Cifrado en bloque, ya que los algoritmos criptográficos que el estándar soporta trabajan la información dividiéndola en bloques y cifrándola por separado utilizando la misma clave.

A continuación se hace una clasificación de los sistemas que utiliza el estándar para manejar sus claves:

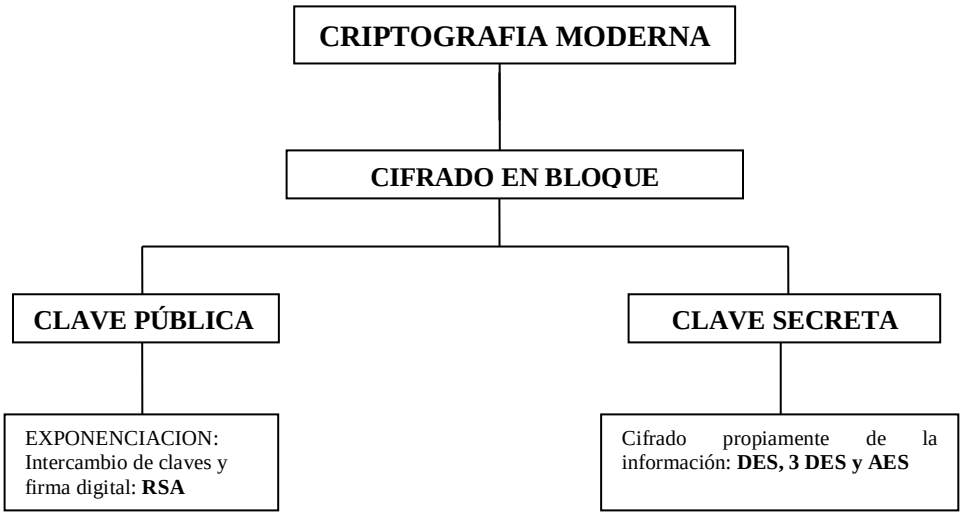
- **Sistemas de clave privada:** La clave que se utiliza para cifrar y descifrar el mensaje original es la misma, es decir, que la EB y la ES hacen uso de la misma clave para cifrar y descifrar respectivamente el mensaje. Los algoritmos criptográficos que utilizan este sistema de claves en el estándar 802.16 son el DES, 3-DES y el AES [24].

- **Sistema de clave pública**: La clave empleada para cifrar el mensaje difiere de la clave que la ES utiliza para descifrar dicho mensaje. Generalmente la clave de cifrado usada por la EB es de dominio público, mientras que la clave que emplea la ES es conocida exclusivamente por ésta. El estándar 802.16 utiliza el algoritmo RSA para el intercambio de claves entre estas entidades [24].

Los sistemas de clave privada son rápidos, frente a los de clave pública que son más lentos, pero carecen de firma digital, los primeros son utilizados para el cifrado de la información y los segundos para el intercambio de las claves de cifrado y la firma digital [24].

A continuación se muestra en la figura 6 los métodos de cifrado utilizados en el estándar IEEE 802.16 para cifrar la información e intercambiar claves entre Estación Base y Estación Suscriptora.

Figura 6. Métodos de cifrado usados por el estándar 802.16.



1.5.2 CRIPTOANÁLISIS. El criptoanálisis está íntimamente ligado a cada algoritmo de cifrado. Cuando alguien diseña un criptosistema, tiene que tener en mente todos los posibles ataques que éste puede sufrir, y cada mecanismo de ocultación que implementa está respondiendo a su hipotético procedimiento de criptoanálisis. No se puede hablar de un procedimiento general de criptoanálisis, cada algoritmo ha de ser atacado mediante un procedimiento adecuado a su estructura, no obstante, el usuario de un sistema criptográfico ha de tener presente que la robustez del algoritmo de cifrado no es el elemento definitivo en la seguridad; hay otros aspectos a tener en cuenta, principalmente la utilización del algoritmo y los protocolos con que se usa. Los algoritmos de cifrado utilizados actualmente resultan tan robustos y su rotura exige tal esfuerzo computacional, que resulta mucho más práctico para un posible oponente el atacar al protocolo o

simplemente emplear ingeniería social, la cual se utiliza para ayudar de manera involuntaria al atacante y así permitir el acceso a la información que el delincuente informático busca. Un criptosistema se puede atacar de muchas formas, la más directa sería la que hace uso únicamente del análisis del mensaje cifrado o criptograma. Se trata de un análisis pasivo pero en la realidad se pueden producir más ataques, apoyados en cierto conocimiento adicional o bien en cierto grado de intervención, en cuyo caso se estará frente a un ataque activo [5].

A la hora de realizar un criptoanálisis, se puede disponer de información diversa, cuanta más información se posea, más fácil será su realización. A continuación se presenta una lista, en orden de facilidad creciente, de las situaciones más frecuentes [12]:

1. Solo se conoce el criptograma.

2. Solo se conoce el criptograma, pero éste deja ver textos claros sin cifrar.

3. Se conocen varios criptogramas diferentes correspondientes al mismo texto claro, cifrado con claves diferentes o vectores de inicialización.

4. Se conoce el criptograma y el texto claro correspondiente.

5. Se conoce el criptograma correspondiente a un texto claro escogido por el criptoanalista.

6. Se conoce el texto descifrado correspondiente a un criptograma elegido de forma adaptativa por el criptoanalista en función de análisis previos.

7. Se conoce la clave o al menos se puede limitar el espacio de claves posibles.

Todos estos casos pueden estar modulados por el hecho de que se conozca o no el criptosistema en uso, cuando el algoritmo es conocido, hay un ataque posible denominado *fuerza bruta,* y que consiste en probar todas las claves [12].

Estas formas de ataque obligan a varias precauciones por parte del usuario para no dar facilidades al oponente [12]:

- Cuando sea necesario repetir la transmisión de un mensaje cifrado, se hará con la clave original, para evitar el ataque número 3.

- No se cifrará la información que ya es pública, para evitar el ataque número 4.

- No se enviará la misma información en claro y en cifrado, aunque se haga por canales diferentes, para evitar el ataque numero 4.

- No se enviarán en una misma comunicación partes en claro y en cifrado, para evitar los ataques números 2 y 4.

- Se evitarán enviar mensajes cifrados, referentes a mensajes en claro recibidos del oponente para evitar el ataque número 5.

- Se elegirán las claves de forma aleatoria y carecerán de sentido, para no facilitar un ataque por fuerza bruta mediante diccionario evitando así el ataque numero 7.

- Se incorporará de alguna forma la fecha y hora de producción de un mensaje a la clave, lo que asegura de cierta forma el cambio de clave con cada mensaje.

- Las claves y algoritmos de cifrado, a ser posible, han de ser secretos y conocidos por un número reducido de personas, para evitar un ataque por fuerza bruta.

- Se cambiarán las claves con la mayor frecuencia posible y se tratará de evitar el uso de la misma clave con mensajes diferentes, para obligar al oponente que es capaz de romper el algoritmo recuperando la clave, a repetir el proceso de ataque con cada nuevo mensaje.

CAPÍTULO 2. RIESGOS DE SEGURIDAD DEL ESTÁNDAR IEEE 802.16

Durante el diseño y desarrollo del estándar IEEE 802.16 la seguridad tuvo un lugar preponderante en la cual se desarrollaron y aplicaron técnicas de cifrado de datos, protocolos de encapsulamiento, firmas electrónicas, certificados digitales, autenticación y gestión de claves entre otros. Dadas estas condiciones, el estándar se fortalece en muchos aspectos y se hace muy atractivo para la implementación de servicios como Internet de alta velocidad, servicios multimediales, VoIP, entre otros.

No obstante, debido a que la tecnología del 802.16 es relativamente nueva, se pueden presentar en ésta clase de redes vulnerabilidades que explotan las debilidades de la tecnología como autenticación débil de Estaciones suscriptoras, cifrado de datos débil donde se ha probado que la utilización del algoritmo DES es ineficiente como medio para cifrar datos, y ausencia en algunos casos de integridad de mensajes.

Existen también amenazas a las que se ven expuesta esta clase de redes, estas son las amenazas externas aquellas en donde las personas no tienen acceso autorizado a la red inalámbrica y acceden a ésta desde el exterior, las amenazas internas que se presentan cuando alguien tiene acceso autorizado a la red por medio de una cuenta de servidor o un acceso físico al cableado, las amenazas estructuradas que vienen de personas técnicamente competentes que conocen las vulnerabilidades de la tecnología y pueden comprender y desarrollar explotación de códigos, programas, scripts etc. y las amenazas no estructuradas las cuales se dan por acción de personas inexpertas que hacen uso de herramientas de hacking disponibles de manera gratuita.

Los métodos de ataque según su categoría son los ataques de reconocimiento los que generalmente preceden a un acceso real o ataque de negación del servicio, los cuales se pueden evitar si se utiliza un esquema de cifrado de datos fuerte y la no utilización de protocolos que pueden ser fácilmente escuchados, los ataques de acceso al sistema, donde la capacidad para que un intruso no autorizado logre acceder a un dispositivo para el cual no tiene una cuenta, se puede llevar a cabo ejecutando alguna herramienta que explote una vulnerabilidad conocida del sistema o aplicación, como cuentas débiles o no existentes, servicios HTTP, FTP, Telnet, etc.

El uso también de la ingeniería social, la cual no comprende ninguna habilidad informática en donde un intruso puede engañar a un miembro de una organización para que le dé información valiosa como ubicaciones de archivos y servidores o passwords, entonces aquí el ataque resulta mucho más sencillo, también se puede presentar el robo de EB haciendo que la mayoría de las ES se asocien a esta EB con la señal más fuerte, si una EB no autorizada hace que las ES se asocien a este dispositivo, la EB robada tendrá acceso al tráfico de red de todos las ESs asociadas, Por lo tanto, la EB puede ser usada para realizar ataques como el de hombre en el medio contra tráfico cifrado como SSL o SSH. Esta EB furtiva también puede usar spoofing de ARP e IP para engañar a las ESs para que envíen contraseñas e información confidencial. Finalmente, se presenta el ataque de negación del servicio, el cual ocurre cuando un atacante desactiva o corrompe las redes, sistemas o servicios inalámbricos, con la intención de negar el servicio a usuarios autorizados. El atacante no necesita acceder previamente al objetivo, porque todo lo que se necesita normalmente es una forma de acceder a él. Por estas razones y a causa del gran daño potencial, esta clase de ataques son los más temidos, ya que son los más difíciles de evitar, de hecho, cualquier dispositivo que opere a 5 GHz puede ser usado como una herramienta DoS, ya que el estándar trabaja en esa banda de frecuencia sin licencia, se

puede ver afectado por herramientas que falsifiquen paquetes que parezcan que hayan sido generadas por una EB y que se dirijan a todas las ES de la red diciéndole a estas que se desconecten, esta clase de herramientas pueden ser por ejemplo la suite denominada Air-Jack que a pesar de ser utilizada para ataques de negación de servicio en redes WLAN (802.11a) debe tenerse en cuenta ya que este estándar también trabaja en las banda de frecuencias de los 5GHz.

Todos estos aspectos de seguridad presentes en el estándar 802.16 hacen que este deba cumplir con una tecnología de seguridad la cual busca implementar contramedidas que funcionen para prevenir y afrontar estos tipos de amenazas, vulnerabilidades y riesgos de seguridad, es por eso que la implementación de un sistema de seguridad informática basado en prácticas y técnicas encaminadas a proveer un buen ambiente contribuye a la seguridad del 802.16.

2.1 ANALISIS DE LOS ALGORITMOS CRIPTOGRAFÍCOS UTILIZADOS EN EL ESTÁNDAR 802.16

La criptografía moderna tiene como objetivo ocultar información para quienes no estén autorizados a poseerla o que si de alguna manera la poseen no sean capaces de interpretarla utilizando complejas estructuras matemáticas para generar algoritmos que combinan sustituciones, permutaciones y desplazamientos de caracteres además de claves para descifrar los textos. A continuación se estudiarán los métodos de cifrado y los algoritmos utilizados por el estándar en sus protocolos de seguridad [12].

Los algoritmos criptográficos usados en la capa de seguridad del estándar utilizan el método de cifrado en bloque, en este método, los caracteres se agrupan en conjuntos de dos o más elementos para minimizar el riesgo de ataque estadístico al que puede estar expuesta la información, existiendo una dependencia de caracteres adyacentes para originar el correspondiente texto cifrado. Están presentes en diferentes procesos de seguridad como: técnicas de autenticación de mensajes, mecanismos de integridad de datos, protocolos de autenticación de entidades, esquemas de firma digital [11]. Por su relevancia en estos aspectos se hará un estudio de los diferentes métodos utilizados en el estándar IEEE 802.16 como son el DES y el AES.

2.1.1 DES. El funcionamiento de DES está regido por diferentes normas del gobierno de EEUU, entre las cuales está la implementación del sistema en un chip que no se puede exportar sin un permiso especial; tampoco se permite la comercialización dentro del país de chips fabricados fuera de USA. Todo esto encaminado a la protección del sistema y la seguridad nacional. Sin embargo, en 1981 el ANSI (American National Standards Institute) adoptó el DES bajo el nombre de DEA (Data Encryption Algorithm) para poder ser programado no necesariamente en un chip sino en un computador [12].

El funcionamiento del DES se puede resumir como una serie de funciones que pretenden ocultar el mensaje original haciendo uso de teorías matemáticas complejas que van más allá del alcance del presente trabajo de grado, conmutaciones, diversas funciones para hacer que el algoritmo sea lo suficientemente seguro a los diferentes tipos de ataques, sin embargo, la seguridad del DES ha sido fuertemente cuestionada debido a las debilidades que presenta en algunos aspectos, como se presentará más adelante, el avance en la

tecnología computacional de décadas recientes ha hecho que el DES no sea la mejor opción para el cifrado de datos importantes en cualquier sistema.

En el anexo A se muestra una completa descripción del funcionamiento del algoritmo DES.

Propiedades del DES

Las principales propiedades del DES se pueden resumir como sigue [12]:

- *Dependencia entre símbolos:* Cada bit del texto cifrado es una función compleja de TODOS los bits de la clave y TODOS los bits del texto original.

- *Cambio de los bits de entrada:* Un cambio de un bit en el texto original produce un cambio dramático en los bits del bloque cifrado, aproximadamente del 50%.

- *Cambio de los bits de la clave:* Un cambio en un bit de la clave produce, aproximadamente, el cambio de la mitad de los bits del bloque cifrado.

- *Claves débiles:* Existen 4 claves "débiles", las cuales originan que las 16 subclaves sean iguales. Existen 12 claves "semidébiles" que originan que solo 2 o 4 subclaves sean diferentes. En conjunto, estas 18 claves producen un texto cifrado fácil de descifrar, es preciso asegurarse de no escoger ninguna de ellas.

- *Error acumulativo:* Un error en la transmisión de un texto cifrado se propaga a todo el bloque del que forma parte, produciendo un conjunto de errores después del descifrado de 64 bits.

Estas propiedades dan una idea de la seguridad del DES contra ataques de tipo estadístico, los cuales se basan en realizar un estudio de frecuencia de repeticiones de series de bits

presentes en los textos cifrados ya que la dependencia de todos los bits de la clave y los bits del mensaje original con los bits de salida es muy fuerte, esto hace que las frecuencias de repeticiones en los bits de salida sean muy bajas.

La principal debilidad del algoritmo DES radica en su tamaño de clave, el cual en teoría es de 64 bits, pero de los cuales solo 56 son utilizados en el cifrado ya que el último byte es utilizado para paridad. Esto hace que otro tipo de ataque sea el más adecuado para quebrar la seguridad del DES. Este ataque llamado "por fuerza bruta", realiza una búsqueda exhaustiva de todas las posibles claves dentro del espacio de claves que el DES puede utilizar. Adicional a esto, la existencia de claves débiles y semidébiles reducen este espacio, no de forma dramática, sino de manera tal que es indispensable evitar usarlas de manera accidental.

Ataques a DES

Se dice que ningún algoritmo es completamente seguro, debido a que todos los algoritmos presentan cierto grado de inseguridad ya sea en el espacio de claves o debido a los múltiples ataques a los que están expuestos. En DES la debilidad más grande se presenta en su espacio de claves que, a raíz del gran avance en hardware de la computación actual, es considerado pequeño [12].

A lo largo de la historia de DES se han intentado realizar ataques al espacio de claves con máquinas que resultan siendo demasiado costosas. En 1988 se demostró que un ataque por fuerza bruta al espacio de claves del DES era posible; tal máquina fue analizada por W. Diffie y E. Hellman, tenía la capacidad de encontrar la clave utilizada en 12 horas partiendo de un texto claro y su correspondiente texto cifrado, su costo: 20 millones de dólares.

En 1988 una empresa sin ánimo de lucro construyó una máquina capaz de descifrar mensajes DES en menos de 3 días con un costo de 40 millones de euros actuales. La NSA, declaró en ese entonces, que DES era seguro porque el costo para descifrarlo era muy elevado inclusive para el gobierno.

En 1997 los laboratorios RSA sugirió un concurso con un premio de US$ 10.000 a quien encontrara la clave utilizada para cifrar mediante DES un texto plano. Un consultor independiente diseñó un sistema de ataque distribuido, el cual hacia uso de Internet logrando unir más de 70.000 sistemas en todo el mundo y de esta manera, 96 días más tarde del inicio del proyecto, logró encontrar la clave correcta luego de probar aproximadamente un cuarto del total de las claves posibles.

En el año de 1998 la Electronic Frontier Foundation creó una máquina capaz de probar todas las claves del DES en 9 días, lo que da un tiempo medio de 4 días y medio para encontrar una clave. Este dispositivo, combinación de hardware y software, ensaya un total de 92.160.000.000 claves por segundo y tuvo un costo de 210.000 dólares. Bajo esta perspectiva descifrar DES no estaría al alcance de un particular pero si de cualquier gobierno, es por esto que según [11] DES ya no es seguro.

Los anteriores ejemplos sugieren que el algoritmo DES es cada vez más vulnerable a este tipo de ataques, esto debido a que los avances en tecnología computacional hacen que se puedan hacer mas operaciones en menos tiempo lo que supone un ahorro tanto de recursos computacionales como recursos económicos en la construcción de dispositivos capaces de realizar la búsqueda de claves utilizadas en DES. Haciendo una proyección hacia el futuro, DES no se hará más fuerte, al contrario, llegará un día en que quebrar la seguridad del DES será tan rápido de lograr como los límites de la tecnología lo permitan. Como se mencionó anteriormente, existe un número de claves que se deben evitar ya que

ellas producen un criptograma "fácil" de descifrar. Estas claves débiles y semidébiles son presentadas en la tabla 1 y tabla 2 respectivamente [24].

Tabla 1. Claves débiles para el algoritmo DES (64 bits).

Clave	Clave después de la 1ª permutación
0101010101010101	0000000 0000000
1F1F1F1F0E0E0E0E	0000000 FFFFFFF
E0E0E0E0F1F1F1F1	FFFFFFF 0000000
FEFEFEFEFEFEFEFE	FFFFFFF FFFFFFF

Tabla 2. Claves semidébiles para el algoritmo DES (64 bits), expresadas en hexadecimal.

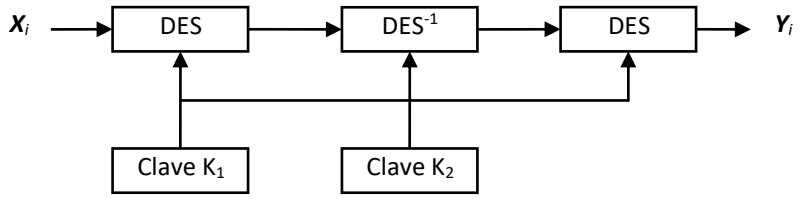
Clave	Clave después de la 1ª permutación
01FE01FE01FE01FE	AAAAAAA AAAAAAA
FE01FE01FE01FE01	5555555 5555555
1FE01FE01FE01FE0	AAAAAAA 5555555
EO1FEO1FEO1FEO1F	5555555 AAAAAAA
01E001E001E001E0	AAAAAAA 0000000
E001E001E001E001	5555555 0000000
1FFE1FFE1FFE1FFE	AAAAAAA FFFFFFF
FE1FFE1FFE1FFE1F	5555555 FFFFFFF
011F011F011F011F	0000000 AAAAAAA
1F011F011F011F01	0000000 5555555
E0FEE0FEE0FEE0FE	FFFFFFF AAAAAAA
FEE0FEE0FEE0FEE0	FFFFFFF 5555555

Cifrado Triple

Existe una variación de cifrado múltiple que se aplica en especial al DES, la cual consiste en emplear 3 etapas de cifrado pero con claves que no son independientes, es inmune al ataque por encuentro a medio camino, doblando la longitud efectiva de la clave pero a cambio de triplicar las operaciones de cifrado. En este método se utiliza una clave K_1 en la primera etapa para cifrar el texto, en la segunda etapa se utiliza una clave K_2 para descifrar el texto obtenido en la primera etapa y por último se emplea la clave K_1 para

cifrar el texto nuevamente siendo el resultado final del proceso. Este proceso se muestra en la figura 7 [12].

Figura 7 Triple DES.



Este tipo de cifrado ofrece mejores garantías en cuanto a seguridad debido a que el tamaño de clave utilizado puede ser mayor que el de DES; adicionalmente no existe una sola clave sino que se utilizan 2 claves en el proceso de cifrado y descifrado agregando mayor dificultad para realizar ataques por fuerza bruta. El 3-DES o triple DES se presenta como una muy buena opción para ser utilizado en sistemas que aun utilicen DES otorgando un mayor nivel de seguridad sin causar muchos inconvenientes en su implementación ya que ésta es relativamente sencilla.

2.1.2 AES y Rijndael. Debido a que el espacio de claves en el DES se hacía cada vez mas insuficiente para garantizar la seguridad del algoritmo gracias a los avances en tecnología que se presentaron a finales de la década de los 90, NIST organizó una convocatoria abierta a nivel mundial para encontrar el reemplazo a DES y Triple DES. La búsqueda del nuevo estándar llamado AES (Advanced Encrytpion Standard) se inició en 1997 con las premisas de que fuera un algoritmo simétrico, debería ser de dominio público, por consiguiente no estar patentado, permitir que el tamaño de la clave pudiera ser

manipulado según las necesidades del usuario, de fácil implementación tanto en software como en hardware [10].

En octubre de 2000, NIST anunció oficialmente la adopción de Rijndael como nuevo estándar de cifrado de datos sucesor de DES. La palabra Rijndael es un acrónimo de sus creadores, dos belgas llamados Joan Daemen y Vincent Rijmen y que de ahora en adelante se nombrara solamente como AES [24].

La estructura completa del algoritmo AES se presenta en el anexo B.

CRIPTOANÁLISIS DEL AES

Los primeros ataques al sistema se realizaron en el año de 1998, pero éste solo alcanzaba a romper la seguridad del sistema de 6 vueltas. Dos años después Gilbert y Miner publicaron un ataque que lograba penetrar la seguridad de un sistema con 7 vueltas [6].

En general todos los métodos aplicados para lograr quebrar la seguridad del AES tales como: Suma parcial, Ataque cuadrado y ataques empíricos solo han logrado descifrar, en el mejor de los casos, 8 vueltas del algoritmo AES. Recordemos que AES puede trabajar hasta con 14 ciclos o vueltas, lo cual lo hace prácticamente inmune a estos ataques.

Teniendo en cuenta que para atacar la seguridad del AES, es necesario poseer una gran cantidad de parejas texto plano – texto cifrado, esta tarea se vuelve más compleja aun. Por ejemplo, para encontrar la clave de un sistema AES de 6 vueltas con el tamaño de clave máximo es necesario un tiempo igual a 2^{72} segundos, lo cual equivale a 149.745.258.842.898 años.

Otros tipos de criptoanálisis especializados como el diferencial o el lineal, no han logrado romper la seguridad del algoritmo AES debido a que éste tiene una estructura que elimina la simetría de las claves, punto de partida de este tipo de ataques. Por esta razón, el método más eficiente conocido hasta el momento es el de recuperar la clave a partir de parejas de texto plano – texto cifrado mediante búsqueda exhaustiva lo cual lo convierte en uno de los sistemas de cifrado más seguros que existen [27].

Por todas estas razones AES es la mejor opción existente en la actualidad para ser usado en sistemas de protección de datos. El elevado número de rondas y la capacidad de variar el tamaño de la clave, hacen que los ataques realizados a este algoritmo sean infructuosos.

Los criptosistemas presentados anteriormente, llamados de clave secreta o clave simétrica, tienen como característica principal que tanto el emisor como el receptor comparten la misma clave para cifrar y descifrar los mensajes. Dadas estas condiciones la mayor parte de la seguridad del sistema recae en mantener en secreto dicha clave y adicionalmente, este tipo de criptosistema presenta el inconveniente de distribuir de forma segura la clave por canales inseguros [26].

En una red de n usuarios, se debe disponer de una clave para cada pareja de comunicación en particular, es decir, se tendría un total de $n(n - 1)/2$ para garantizar todas las comunicaciones posibles dentro de usuarios de la red. No existe la posibilidad de asegurar que el emisor de un mensaje sea efectivamente quien dice ser, es decir, no se puede utilizar una firma digital en los mensajes que confirme la identidad del emisor [12].

Este tipo de criptosistemas se basan en las llamadas "F*unciones Unilaterales Tramposas*" que tienen las siguientes características:

- Son funciones que se pueden calcular fácilmente en una dirección pero que el cálculo de su inversa es muy difícil [26].

- El conocimiento de una información adicional que hace que el cálculo de la función inversa de dichas funciones unidireccionales sea fácil, se conoce con el nombre de *trampa* [12].

- La *trampa*, es la clave privada utilizada para descifrar los mensajes previamente cifrados con su clave pública [12].

Aunque aún no se ha demostrado que este tipo de funciones existan, si se supone que existen 2 firmes candidatas a serlo, la primera de ellas es el producto de números enteros: dado un número *n*, es difícil encontrar sus factores primos; este tipo de función se emplea en el algoritmo RSA, y la segunda es la exponenciación discreta, cuya inversa es el algoritmo discreto: dados *a* y *b*, es difícil calcular *x* tal que $a^x = b$; principio que se emplea en el algoritmo de Diffie – Hellman [12] [26].

2.1.3 CRIPTOSISTEMA RSA. El algoritmo más utilizado dentro de la familia de algoritmos de clave pública es el RSA. El cual hace uso del producto de factores primos de más de 200 dígitos para calcular las claves públicas y privadas. Este algoritmo emplea una serie de teoremas matemáticos complejos para generar de manera extremadamente segura las dos claves anteriormente mencionadas, de esta forma es casi imposible (o con un nivel extremo de dificultad, basado en la teoría matemática de la factorización de un número)

encontrar la clave privada de un ente teniendo su clave pública. La descripción detallada del funcionamiento del criptosistema RSA se presenta en el anexo C.

ATAQUE AL CRIPTOSISTEMA RSA

La seguridad del criptosistema RSA se basa en el problema de la factorización. Se trata de determinar mediante algún medio el valor del número *d* conociendo *n* y *e*. De esta manera es posible localizar la clave privada en un tiempo factible. Ya es sabido que *n* es el producto de dos primos, entonces, es conveniente hacer que su factorización sea difícil de realizar (ver anexo C). Esto se logra escogiendo los números primos ***p*** y ***q*** muy grandes, actualmente de alrededor de 200 dígitos. Y adicional a eso es recomendable elegir los números según las siguientes condiciones que hacen que su factorización sea aun más dificultosa [12]:

1. *p* y *q* sólo deben diferir en unos pocos dígitos, aunque no deben ser demasiado cercanos.

2. (*p* - 1) y (*q* - 1) deben contener factores primos grandes.

3. El mcd(*p* – 1,*q* - 1) debe ser pequeño

Otra manera de romper el criptosistema sería calcular $\phi(n)$ = (p-1) (q-1) directamente o intentar un ataque por fuerza bruta para encontrar la clave privada. Afortunadamente estos procedimientos son más costosos computacionalmente hablando que la propia factorización [24].

Otra situación importante en la seguridad del RSA es que existe el problema de tener la certeza de que los números escogidos son primos, *problema de la primalidad*, y más aún si deseamos que los dos números sean grandes [12].

Existen métodos para probar si un número es primo, como por ejemplo el algoritmo de Rabin-Miller, el cual nos da una probabilidad de $1/2^{60}$ cuando se prueba un número realizando 30 pasadas del mismo [24].

VULNERABILIDADES DEL RSA

Aunque en teoría el algoritmo es bastante seguro, existen varias falencias que pueden ser aprovechadas por un atacante, ellas son [24]:

Claves débiles: Es posible demostrar matemáticamente que existen claves para las que el mensaje original queda inalterado.

Claves demasiado cortas: Una clave de RSA de al menos 768 bits se considera segura, pero se recomienda usar claves no inferiores a 1024 bits aunque este valor también depende del tiempo que se quiera tener en secreto la información codificada, se supone que una clave de 1024 bits mantiene la confidencialidad por unos pocos años.

Ataques de texto claro escogido: Cuando un usuario codifica y firma el mensaje con un mismo par de claves, entonces se puede presentar un ataque sobre el mensaje codificado. Por ello se recomienda que la firma digital del mensaje se haga no sobre el mensaje en si sino sobre su signatura.

Ataques de módulo común: Se podría pensar que es más fácil generar claves diferentes a partir de un par de números *p* y *q*, pero esto haría que un atacante pudiera descifrar los mensajes sin necesidad de la clave privada. Por lo tanto se recomienda generar *p* y *q* para cada clave que se utilice.

Ataques de exponente bajo: Por razones de eficiencia, en varias aplicaciones de RSA se utiliza un exponente de cifrado bajo, *e* = 3, es un valor característico. Pero este valor bajo puede hacer que un atacante rompa el sistema.

Firmar y Codificar: Se debe firmar primero un mensaje y luego codificarlo para evitar ataques que permiten manipular exitosamente mensajes que no siguen este proceso aún empleando funciones Hash o resumen.

La firma digital y los certificados digitales que hacen uso del criptosistema RSA se presentan en el anexo D.

A pesar de estas debilidades, se puede decir que el RSA es muy seguro. La razón de tanta seguridad radica en la escogencia de los números primos grandes y de asegurarse de que en efecto sean primos. Como se mencionó anteriormente, esto no es problema ya que existen pruebas matemáticas para saber si un número de tales características es primo.

Esto a su vez es una razón adicional para confiar en el criptosistema RSA debido a que, contrario a lo que se pueda pensar, el incremento de la capacidad de cómputo debido al avance de la tecnología hace que se puedan utilizar números cada vez mayores haciendo aun más difícil la tarea de tratar de factorizarlos. Así pues, el RSA presenta las mejores condiciones de seguridad para sistemas de clave pública.

2.2 VULNERABILIDADES DE LOS ALGORITMOS DE CIFRADO UTILIZADOS EN EL ESTÁNDAR IEEE 802.16

El estándar IEEE 802.16 utiliza diferentes algoritmos de cifrado en sus protocolos de autenticación, identificación y PKM, éstos algoritmos son: el DES con una extensión clave de 56 bits lo que lo hace muy vulnerable a los ataques descritos anteriormente, todo esto adicional a que en la actualidad no es recomendable la utilización del algoritmo DES ya que debido a los avances en tecnología es inseguro [11].

Es recomendable entonces que se revise la utilización del algoritmo de cifrado DES en el estándar IEEE 802.16 ya que actualmente este método de cifrado no ofrece las garantías de seguridad necesarias para que el estándar tenga una base de seguridad sólida desde sus cimientos, es decir, desde su primera línea de defensa que es el uso de algoritmos y sistemas de cifrado.

IEEE 802.16 emplea el algoritmo AES para cifrar datos, en el algoritmo de autenticación de datos y en el algoritmo de cifrado de TEK con una extensión de clave de 128 bits, lo cual lo hace muy resistente a cualquier tipo de ataque, haciendo que las funciones anteriormente descritas se lleven a cabo de una manera muy segura.

Por su parte, el algoritmo RSA es utilizado por IEEE 802.16 en el algoritmo de cifrado de TEK con una extensión de clave de 1024 bits. Por esta razón el RSA proporciona las condiciones de seguridad suficientes para afirmar que no existe una amenaza real sobre las operaciones que se llevan a cabo mediante este algoritmo.

La seguridad en general del estándar IEEE 802.16 está soportada en un alto porcentaje en la seguridad proporcionada por los algoritmos de cifrado de datos. Cada algoritmo tiene sus características en cuanto a seguridad y prestaciones que los hacen útiles en diferentes partes del estándar y que además proporcionan herramientas para contrarrestar posibles ataques a sistemas que implementen el estándar.

2.3 ATAQUES Y FALENCIAS DE SEGURIDAD DEL ESTÁNDAR 802.16

En el estándar los riesgos en la seguridad se presentan en la capa física y la capa MAC. Un ataque presente a nivel físico es el que logra introducir una fuente de ruido suficiente para reducir la capacidad del canal causando negación en el servicio en todas las estaciones (jamming), otro riesgo de ataque es el envío de una serie de tramas en corto tiempo para agotar las baterías en el receptor (scrambling), en general las técnicas disponibles para defender la capa física de los ataques son insuficientes y pocas centrándose mejor en la protección de la capa MAC, a pesar que esta capa nunca cifra los mensajes y casi nunca los autentica abriendo la puerta a riesgos de ataques como el de hombre en el medio, ataques activos como la adivinación de contraseñas por fuerza bruta y ataques pasivos como el automatizado mediante diccionario el cual se realiza sin necesidad de conexión, entre otros, dándose estos en versiones anteriores a la 802.16e [24] [25].

Una vulnerabilidad presente en la autenticación se da al suplantar la identidad de la EB debido a que el protocolo PKM encargado que las Estaciones suscriptoras obtengan la autorización y el material para intercambiar claves desde estas y que administran las Asociaciones de seguridad SA, que son un conjunto de reglas de información de seguridad que una o más ESs comparten para soportar comunicaciones seguras a través de la red WiMAX, presenta vulnerabilidades, permitiendo los ataques de falsificación hacia el protocolo PKM. Estos ataques hacen que la ES no pueda verificar que el mensaje del protocolo de autorización haya sido generado por la EB, construyendo y enviando una respuesta PKM utilizando información pública que cualquier EB falsa podría utilizar para crear una respuesta similar. Requerir que las ESs se autentiquen con la EB puede eliminar esta vulnerabilidad.

Los ataques contra las SAs se remiten generalmente a las autorizaciones, es decir, el estado de una SA no diferencia entre una autorización u otra abriendo un camino para ataques reiterativos, además las autorizaciones no incluyen la identidad de la EB impidiendo que la ES distinga entre una EB autorizada o no, sin embargo, si se desea ocultar la identidad de la EB al usuario para que el esquema de cifrado proteja las ES contra la falsificación, esto puede llevar a nuevos ataques causando un problema relacionado con los datos de las SA, ya que las ESs no pueden distinguir la autorización ni reconocer los datos reutilizados de las SA, haciendo el esquema vulnerable a un ataque con la reutilización de la llave de cifrado. La manera más segura de corregir la vulnerabilidad es agregar un valor al azar a la EB y a las ESs para la autorización de las SA, requiriendo la entrada de ambas partes para la protección de sus datos. Una identificación de EB autenticada también eliminará las amenazas contra las ESs causadas por la asimetría de las credenciales utilizadas por el estándar en las SA de autorización.

Otra debilidad notable es la necesidad de la legitimación mutua, al momento de la autenticación de un certificado X.509 de la EB, el protocolo asume que se publican correctamente de manera que dos entidades con diferentes pares de llaves públicas o privadas pueden certificarse con la misma dirección MAC, es decir, una entidad podría enmascararse como otra. La manera de proteger la ES contra la falsificación es sustituir el esquema de autentificación del estándar por uno que la proporcione de manera mutua.

Los riesgos presentes en la gestión de las claves se dan a la hora de administrar estas debido a la utilización del espacio secuencial en las claves de cifrado de tráfico (TEK) las cuales son usadas para cifrar la transmisión de datos entre la EB y la ES , aquí el protocolo identifica cada TEK con un número de secuencia de 2 bits permitiendo la utilización de 4 valores (0 a 3) para su representación, esto causa que el identificador del TEK sea comparado cada cuatro claves desde 3 hasta 0 dejando la estación abierta para un ataque

el cual se originaría por la reutilización de las claves que han expirado, si el ataque se repite y ninguna especificación del protocolo permite que la ES se entere, el modelo de cifrado volverá a utilizar la TEK inicializando el vector correspondiente en el proceso exponiendo la TEK y los datos. Otro punto en los problemas que se presentan en el TEK es el tiempo de vida que este maneja, el cual se configura entre 30 minutos y 7 días con 12 horas por defecto, si aquí se utiliza el algoritmo DES en modo CBC la seguridad de los datos puede estar comprometida debido a que este algoritmo es inseguro después de la operación en $2^{n/2}$ bloques con la misma clave de cifrado, donde *n* es el tamaño del bloque, es decir, cuando el DES se usa con un tamaño de bloque de 64 bits, después de 2^{32} bloques el cifrado es inseguro. Se propone ampliar el tamaño del identificador de la llave para que más identificadores puedan ser transportados a lo largo del valor de tiempo de vida de la AK, si un AK dura por lo menos 7 días, y un TEK dura tan solo 30 minutos, entonces, los datos de las SA pueden consumir hasta 3360 TEKs sobre el tiempo de vida del AK, permitiendo que el tamaño de SAID crezca de 2 a 12 bits. Aquí se plantea la situación de cuando un TEK debe expirar, en el estándar el TEK expira después de un periodo de tiempo configurable, aunque esto es necesario, no es suficiente conduciendo estos tiempos de vida a más riesgos de seguridad.

2.4 SOLUCIONES DE SEGURIDAD PROPUESTAS PARA EL ESTÁNDAR 802.16

El grupo de trabajo para el estándar 802.16 diseñó algunos mecanismos de seguridad dando soluciones relevantes a los problemas presentados en este estándar, brindando seguridad a las conexiones enfocándose en las siguientes áreas de trabajo.

- El estándar 802.16 adiciona el uso del AES para darle un mayor poder de cifrado de datos a este. Dado que el estándar DES empezaba a quedarse anticuado, a causa sobre todo de la longitud tan corta de sus claves, y el Triple DES no es excesivamente eficiente cuando se implementa con software, también se tomó en cuenta que el método de cifrado utilizado por el estándar pueda conseguir que un atacante no descubra directamente los datos transmitidos, haciendo que se deduzca información indirectamente. Por ejemplo, al utilizar mensajes con una cabecera fija, la aparición de los mismos datos cifrados varias veces en una transmisión puede indicar dónde empiezan los mensajes en un cifrado en bloque, si dos bloques de texto en claro son iguales y se utiliza la misma clave, los bloques cifrados también serán iguales. Para contrarrestar esta propiedad, se pueden aplicar distintos modos de operación al cifrado en bloque al utilizar el algoritmo de cifrado AES en modo CBC donde se suma a cada bloque de texto en claro, antes de cifrarlo, (bit a bit, con XOR) el bloque cifrado anterior. Al primer bloque se le suma un vector de inicialización (VI), que es un conjunto de bits aleatorios de la misma longitud que un bloque. Escogiendo vectores distintos cada vez, aunque el texto en claro sea el mismo, los datos cifrados serán distintos. El receptor debe conocer el valor del vector antes de empezar a descifrar, pero es necesario guardar este valor en secreto, normalmente se transmite como cabecera del texto cifrado.

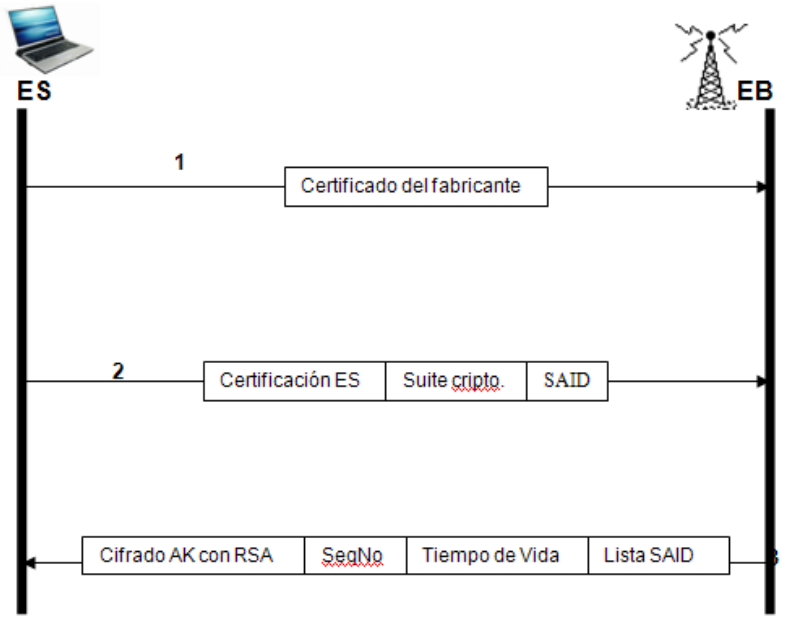
- Una propuesta de seguridad para el estándar es introducir esquemas más flexibles de autenticación utilizando el protocolo de autenticación extensible EAP con el estándar IEEE 802.1x, esta especificación controla el acceso a la red basándose en los puertos físicos de redes LAN cableadas e inalámbricas para transportar los mensajes EAP, pero en esta propuesta existen dos problemas principales dentro de los planes de integración de los estándares 802.16 y 802.11x. La especificación 802.1x no proporciona protección frente a los ataques de hombre en el medio, ni tampoco protege de los ataques basados

en secuestro de sesión. Los ataques mediante hombre en el medio están basados en el hecho de que el tráfico se redirige desde una ES a la EB, lo que permite al atacante ver todos los datos que se están transmitiendo desde y hacia dicho nodo, este tipo de ataque tiene éxito debido a que la EB no realiza la autenticación de la ES, por lo que de forma inherente esta confiando en exceso en el proceso de autenticación cliente – servidor. Por ejemplo, en la especificación 802.1x no existe un método que permita a la ES estar seguro de que se está autenticando frente a la autentica EB. Respecto al otro ataque, el éxito del secuestro de sesión está en la carencia de confidencialidad del mensaje y en su autenticación, un atacante puede separar de la red una ES legítima y posteriormente falsificar su identidad para continuar con la sesión de comunicación sin que la EB se dé cuenta de esto.

- Codificar los mensajes en las tramas de gestión 802.16 ofreciendo autenticación durante el establecimiento del enlace mediante la inclusión de dos mensajes PKM para realizar solicitudes y envíos de respuestas EAP.

- Se debe trabajar la autenticación nativa del protocolo PKM, ya que este protocolo al intercambiar claves AK lleva a cabo este cambio utilizando tres mensajes entre EB y ES, como se muestra en la figura 8 [2]. Para mayor información ver el Anexo D.

Figura 8. Autenticación PKM.



Esta autenticación nativa hace que se adicionen campos a los mensajes, uno al mensaje dos y cuatro al mensaje tres, donde las claves AK se deben calcular de otra forma haciendo posible que esta se genere con la misma longitud en bits (160) de la AK existente, incluyendo el mecanismo de aleatoriedad en la ES y la EB mediante la asignación de números al azar públicos (en el mensaje 3) para ser asignados a estas entidades, para que se pueda identificar la EB autorizada con el uso de un valor que contenga las identidades certificadas de la EB y ES, también, el número generado aleatoriamente para la EB y el número que identifique la ES, así estas entidades pueden utilizar esta información para administrar sus llaves con las entidades que han sido autorizadas. Esto garantiza que EB y ES mantengan un AK actualizado sin importar nuevas modificaciones en la conexión, incluyendo también la dirección MAC permitiendo ligar

esta clave con un conjunto particular de conexiones y proteger de ataques reiterativos las entidades utilizando el bit que ha sido adicionado.

2.5 RESUMEN DE LOS PROBLEMAS DE SEGURIDAD DEL PROTOCOLO PKM

Los ataques de seguridad más comunes en el 802.16 operan generalmente a nivel MAC, y son la captura de tramas para modificarlas, reenviarlas y reutilizarlas causando vulnerabilidades, entre una ES y EB válida.

Las principales vulnerabilidades de seguridad del estándar están basadas en la necesidad de mecanismos de autenticación de datos, carencia de definiciones explícitas en la autorización de las SA, significando esto que nunca recibe los mismos datos SAs que se envían, y la falta de autenticación mutua entre la EB y la ES.

En relación con esto, la autenticación que lleva a cabo el 802.16 es una operación primordial, ya que por utilizar un medio inalámbrico donde se generan llaves públicas y privadas, que pueden ser atacadas en cualquier momento por personas no autorizadas con el fin de romper la integridad y confidencialidad de los datos. Por otra parte, la seguridad del protocolo no está en el AK ni en el TEK de la EB, está en la identificación debidamente autorizada de cada EB con la ES correspondiente durante el transcurso de la sesión.

CAPÍTULO 3. ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN

La seguridad de un sistema de información no solo depende de la seguridad que sus protocolos proveen en todos los niveles, de la confiabilidad de los algoritmos de cifrado que utilicen y de sus métodos para contrarrestar ataques provenientes de diferentes medios, sino que también es necesario garantizar seguridad en otros aspectos tales como, locaciones físicas en las que se encuentran instalados los equipos necesarios para el normal desempeño de la red, mecanismos de control de acceso a personal autorizado, asignación del personal idóneo y calificado para desempeñar oficios relevantes dentro del sistema de información especialmente relativos a la seguridad, sistemas de vigilancia de la infraestructura que resulta indispensable para el funcionamiento adecuado de la red.

Todos estos puntos, igual de importantes que la seguridad inherente a los protocolos que las redes utilizan, son parte de un conjunto de elementos que tienden a asegurar la integridad de la información crítica que circula por una red y que además son independientes de los protocolos, algoritmos y tecnología que ella emplee para cumplir con sus objetivos. Es por esto que a lo largo de los años, las empresas se estén preocupando por adoptar sistemas que gestionen todos estos puntos de una manera confiable, segura y a la vez de fácil implementación en sus redes existentes.

Atendiendo a la necesidad de las empresas de proveer a sus sistemas de información de una seguridad integral, la cual permita brindar más confianza a los clientes y/o usuarios de la misma y de esta manera no solo garantizar eficacia y eficiencia en su operación sino que también garantizar mayores ingresos económicos. Distintas entidades de estandarización alrededor del mundo han presentado varias propuestas de estándares de gestión de seguridad de la información; a veces diseñados para una región en particular pero que

debido a su gran acogida en otros lugares se han convertido casi que en estándares internacionales; tal es el caso del BS7799, el cual fue desarrollado para la Gran Bretaña pero que posteriormente ISO modificó para convertirlo en un estándar mundial llamado ISO17799.

Los estándares relacionados con seguridad informática se clasifican en 6 clases según la Dirección Nacional de Informática y Comunicaciones [27]:

Estándares para gestión de seguridad de la información

Estándares para evaluación de seguridad en sistemas

Estándares para desarrollo de aplicaciones

Estándares para servicios financieros

Estándares para riesgos

Estándares para autenticación

Dentro de los estándares para gestión de seguridad de la información se encuentran los siguientes estándares que se consideran los más relevantes a nivel mundial:

3.1 RFC 2196

El Grupo de Trabajo en Ingeniería de Internet (IETF) realizó esta guía llamada: *RFC2196 Site Security Handbook* como guía práctica para asegurar servicios e información [27].

Está basada en una estrategia militar compuesta por dos acciones [8]:

Proteger y proceder

Seguir y perseguir

Esto debido a que el responsable del desarrollo de la misma tenía un amplio conocimiento del mundo militar, estrategias y tácticas para enfrentar enemigos que se suponen tienen mayor capacidad combativa expresada en recursos [8].

La idea general es hacer un análisis de vulnerabilidades del sistema en donde se encuentren las falencias en cada porción de la red y se asigne un nivel de riesgo a cada una de ellas, obteniendo también una clasificación de la información según su nivel de importancia dentro de la organización [8].

Según el autor de [8], este tipo de protección se puede representar gráficamente como una muralla, o hablando en términos informáticos como un *firewall* alrededor del sistema de protección de la información con la mayor deficiencia que es que cuando una muralla cae el enemigo puede asaltar fácilmente todo lo que está detrás de ella.

Desde nuestro punto de vista, no es recomendable asignar tanta responsabilidad en la seguridad de un sistema de información a un solo elemento del conjunto en general por muy fuerte, robusto, complejo o avanzado que este sea, ya que no solo existen ataques provenientes del exterior de las redes sino que existen ataques provenientes desde dentro de la red y esto hace que este modelo de protección no sirva realmente en estos casos.

Existen datos estadísticos los cuales muestran que entre el 70% y el 80% de los ataques sufridos por sistemas de información, provienen desde dentro del propio sistema y que el resto son ataques externos principalmente desde internet [8].

3.2 BS7799

Desarrollado por el British Estándar Institute (BSI), ha tenido una gran aceptación en todo el mundo dando origen a otros estándares de seguridad de información. En la actualidad existen 3 partes del estándar [27].

BS7799 se enfoca en la seguridad de la información como parte fundamental del funcionamiento de una organización y que puede estar presente en diferentes formatos: escrita sobre papel, almacenada electrónicamente, transmitida por correo convencional o usando medios electrónicos, puede ser presentada en medios audiovisuales o utilizada en forma verbal. La seguridad de la información en este estándar se basa en tres premisas fundamentales [25]:

Confidencialidad: Es necesario asegurar que la información es accesible sólo al personal que este autorizado para accederla.

Integridad: Salvaguardar la precisión y mantener completa la información dentro de la organización y a su vez preservar los métodos de procesamiento empleados en la distribución, almacenamiento y gestión de la misma.

Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información en el momento en que ésta sea requerida.

Como se mencionó anteriormente, este estándar está dividido en 3 partes, cada una de ellas trata aspectos diferentes en la seguridad de una organización. Las dos primeras partes sirvieron de base para el nacimiento de otros estándares como el AS/NZS 4444 que es el Estándar para la Gestión de la Seguridad de la Información Australiano/Neozelandés,

basado en la primera parte de BS7799; el ISO/IEC 17799 también surgió de esta parte y recientemente el ISO/IEC 27001 basado en la segunda parte del estándar [5,20].

3.2.1 BS7799 – 1. Publicado en 1999 se denominó: Código de Buenas Prácticas para la Gestión de Seguridad de la Información [27].

Los dos primeros capítulos presentan aspectos importantes para iniciar, implementar y mantener un sistema de seguridad para la información. Está estructurado en 10 secciones las cuales presentan controles de seguridad. En el 2004 el IT (Institute Governance) resumió estas secciones [25].

3.2.2 BS7799 – 2. *Especificaciones para un ISMS.* Identifica, gestiona y minimiza el rango de amenazas, siguiendo una metodología explicita, las amenazas que comprometen regularmente a la seguridad de la información. Publicado en 2002 [3].

El estándar puede ser dividido en 10 capítulos, los cuales contienen un número de objetivos y controles necesarios para cumplirlos. La tabla 3. muestra el número de objetivos y los controles en cada capítulo [13].

El BS7799 – 2 modela un procedimiento con 6 diferentes fases que deben ser seguidas secuencialmente ya que cada una de ellas tiene como resultado un producto el cual es usado como entrada para la siguiente fase [13].

3.2.3 BS7799 – 3. *Guía para el Manejo de Riesgos de Seguridad de la Información.* Publicado en el año 2006 *p*resenta un contenido enfocado hacia el manejo de los riesgos que se presentan en los Sistemas de Gestión de Seguridad de Información para que éstos se vean afectados lo menos posible [4].

Por ser una norma reciente, no ha sido adoptada internacionalmente aún, contrario a las dos primeras partes las cuales han servido como base para el diseño de diferentes normas de gestión de seguridad muchas de ellas a nivel regional. Tal es el caso de algunas normas australianas y alemanas.

Tabla 3. Número de objetivos y controles en BS7799 – 2 [7].

AREA	OBJETIVOS	No. DE CONTROLES
Políticas de seguridad	1	2
Organización de la seguridad	3	10
Clasificación de activos y controles	2	3
Seguridad del personal	3	10
Seguridad física y perimetral	3	13
Gestión de comunicaciones y operaciones	7	24
Control de acceso	8	31
Desarrollo de sistemas y mantenimiento	5	18
Gestión de continuidad del negocio	1	5
Cumplimiento	3	11

3.3 ISO 17799

Posterior a la publicación de la norma británica BS7799, ISO adopta ésta y publica en el año 2000 haciendo de ella un estándar internacional llamado ISO/IEC 17799. Presenta una serie de recomendaciones dirigidas a quienes tienen la responsabilidad de iniciar, implantar o mantener la seguridad de una organización [23].

La ISO/IEC 17799 contiene 134 controles para la seguridad de la información detallados, basados en 11 áreas [26]:

Políticas de seguridad de la información

Organización de la seguridad de la información

Gestión de activos

Seguridad del recurso humano

Seguridad física y perimetral

Gestión de comunicaciones y operaciones

Control de acceso

Adquisición de sistemas de información, desarrollo y mantenimiento

Gestión de incidentes de seguridad de la información

Gestión de continuidad de negocio

Cumplimiento

Con la distribución de las áreas empleadas en el estándar se observa claramente la dependencia que tiene este estándar de los capítulos presentados inicialmente por el BS7799 – 1.

Una descripción completa del alcance del estándar, objetivos, métodos y prácticas está disponible en el documento [22].

3.4 SERIE ISO 27000

La familia de estándares ISO 27000 fue desarrollada a partir del año 2005 teniendo como base nuevamente el estándar BS7799 y en los próximos años reemplazarán incluso a los estándares internacionales originados a partir de éstos, tales como el ISO/IEC 17799 y el BS7799 – 2.

La familia de estándares ISO 27000 está compuesta por [22]:

ISO 27001: Basado en la norma BS7799-2:2002 y publicado en 2005, presenta una guía para la certificación de SGSI en las organizaciones y establece unas condiciones de adaptación para aquellas organizaciones que estaban certificadas bajo la norma que reemplazo BS 7799-2:2002 [22].

ISO 27002: Estándar que reemplazará próximamente a ISO 17799, presenta una guía de buenas prácticas para la gestión de la seguridad de la información [22].

ISO 27003: Se encuentra actualmente en fase de desarrollo, tiene su origen en el anexo A de la norma BS7799-2 y otros documentos publicados por BSI. Se pretende que su publicación se lleve a cabo en 2008 y contendrá una guía para la implementación de ISMS [22].

ISO 27004: En fase de desarrollo, su publicación se llevará a cabo presumiblemente en el 2008 y su contenido tendrá como fin el de especificar técnicas y métricas para medir la eficacia de un ISMS [22].

ISO 27005: En proceso de desarrollo, se basa en la norma BS7799-3, y su publicación se hará entre 2007 y 2008. Servirá de apoyo a la ISO 27001 conteniendo una guía para la gestión del riesgo de la seguridad [22].

ISO 27006: Publicada en Febrero de 2007, contiene la especificación de los requisitos para la acreditación de entidades de auditoría y certificación de ISMS [22].

3.5 SELECCIÓN DEL ESTANDAR DE SEGURIDAD DE LA INFORMACIÓN

Dentro del presente trabajo de grado y dando solución al segundo objetivo especifico "Identificar el estándar de seguridad de información adecuado para garantizar un nivel de protección alto enmarcado dentro del ámbito de la realización del proyecto" se ha escogido seguir el estándar ISO 27001-27005, ya que este se puede adoptar por muchos sectores entre ellos se encuentra el de las telecomunicaciones, destacándose en empresas dedicadas a servicios de tecnologías de la información comprometiéndose estas con la seguridad de datos de sus clientes, de esta forma, el estándar permite establecer, implementar, utilizar, monitorear, revisar, mantener y mejorar un sistema de gestión de

seguridad de la información (SGSI), otro factor en la escogencia de este estándar es que este es certificable, es decir, que la organización que tenga implantado un SGSI puede pedir una auditoria a una entidad certificadora acreditada y en caso de superar esta con éxito, obtener la certificación según ISO 27001 [1], este SGSI tiene como propósito garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados de una forma sistemática, continua y eficiente adaptándola a los cambios que puedan ocurrir en la red ya implementada así como los posibles riesgos, el entorno a la que está expuesta esta clase de redes y las tecnologías que en ella se utilicen.

Seguir un SGSI es el modo más eficaz para preservar la confidencialidad de la información, es decir, lograr que esta sea accedida por aquellas personas autorizadas; preservar también la integridad, la cual busca mantener la información sin ningún cambio al igual que sus métodos de proceso; y la disponibilidad, en donde la información y los sistemas como se trata ésta sea accedida únicamente por los usuarios autorizados en el momento que estos lo requieran. El SGSI nunca va a garantizar la seguridad total, pero para acercarse a este propósito, es necesario una mejora continua asumiendo los riesgos en lugar de hablar de completa seguridad, de este modo, se evitan inversiones innecesarias y poco efectivas que se producen por contrarrestar amenazas sin una evaluación previa, por la falta de contramedidas, por la implantación de controles que no tienen proporción con lo que se desea proteger ocasionando costos elevados, por la falta de claridad en la asignación de funciones y responsabilidades sobre la información valiosa manejada en la red entre muchas otras. Finalmente el estudio del presente estándar de seguridad brinda un conjunto de recomendaciones que pueden proporcionar un nivel de seguridad apropiado para el diseño seguro de la red inalámbrica WiMAX, las diferentes guías de seguridad propuestas por este estándar es solo el punto de partida para ser utilizadas,

junto con la evaluación de riesgos que presenta el 802.16, para identificar las medidas que se deberían implementar en el futuro para la red WiMAX de la RUP o implementar medidas que posiblemente se encuentren pero que son ineficientes como políticas de seguridad, control de acceso, administración de la continuidad del negocio, donde la RUP como organización debería hacer cumplir la política y verificar su cumplimiento.

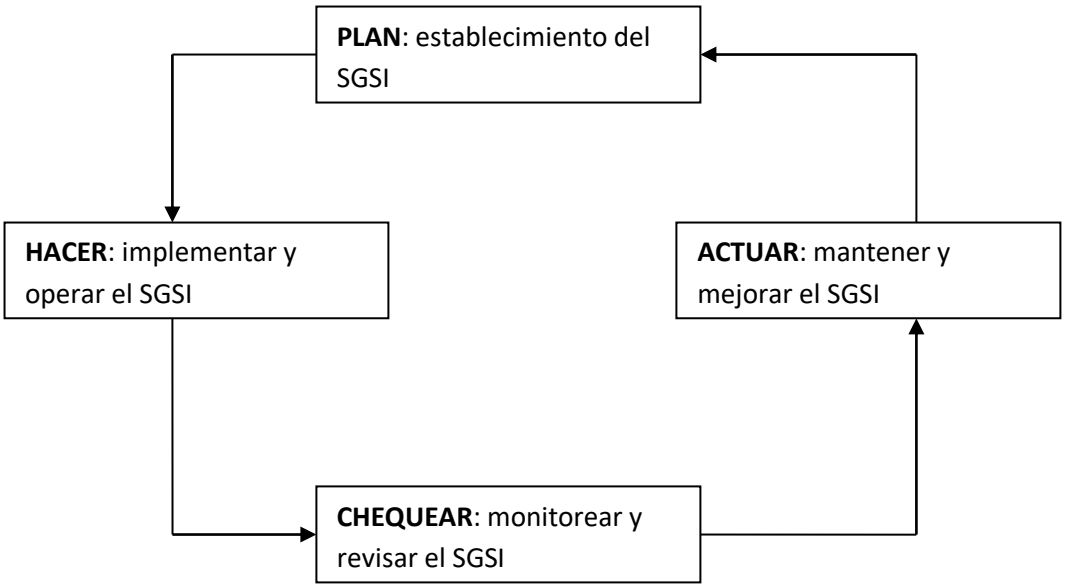
Este estándar maneja el proceso Planear-Hacer-Chequear-Actuar (PDCA), donde en la fase PLANEAR se realiza la evaluación de las amenazas, riesgos e impactos a los que se puede ver enfrentada la red, en la fase HACER se eligen e implementan los controles que reduzcan el riesgo a niveles considerados como aceptables, en CHEQUEAR Y ACTUAR se monitorea, mantiene y mejora el proceso, documentando las evidencias volviendo a adaptar los controles según los nuevos niveles obtenidos y requeridos. Una vez recolectada toda la información, de deben establecer las políticas redactando los procedimientos y normas en un documento conciso, fácil de entender por parte de los integrantes de la RUP no yéndose al extremo de bloquear productividad en aras de la seguridad.

Este proceso por ser cíclico permite adaptar la seguridad al cambio continuo llevado a cabo en la red y su entorno, para propósitos del estándar 27001, se debe aplicar el modelo PDCA aplicado a los procesos SGSI, según la figura 10 [22].

Implementar estas políticas puede exigir algunos recursos financieros y humanos para la RUP, pero el retorno de la inversión es efectivo en el tiempo ya que con ISO 27001 la implementación de controles de seguridad son hasta siete veces menores cuando se tienen en cuenta al principio del diseño e implementación de las soluciones del negocio, en este caso el diseño de la RUP, evitándose compras innecesarias de productos de seguridad como antivirus, sistemas de detección de intrusos, firewalls, sistemas antispam,

software de filtrado de contenidos y redes privadas virtuales (VPN), ya que estas inversiones en tecnología se ajustarán a las necesidades y prioridades conocidas en el entorno que ha sido controlado, logrando que los errores detectados regularmente sean solucionados con medidas que conlleven un costo moderado y los que se logren producir, sean solucionados y controlados por métodos ya establecidos, demostrando un alto nivel de conciencia en proteger la información asegurando la continuidad de la puesta en marcha de la red ante cualquier incidencia por grave que ésta sea.

Figura 9. Modelo PDCA aplicado al proceso SGSI.



En forma general, la estrategia a seguir para llevar a cabo el SGSI en el diseño de la red WiMAX para evaluar la seguridad de las sedes que conforman la RUP la cual se describirá en el capitulo cuatro será la siguiente [19]:

- Identificación de las personas encargadas de cada sede que conforma la RUP las cuales deberán colaborar para la obtención de la correspondiente información.

- Por medio de las entrevistas o revisión de documentación si esto se permite, obtener información que haga referencia a la seguridad de la información como por ejemplo los aspectos técnicos que se manejan como topologías de red, servicios existentes, dispositivos de seguridad en cada sede y su descripción funcional por ejemplo firewalls, Sistema de Detección de Intrusos, antivirus etc., existencia de otros puntos de conexión con otras redes, conocer algunos fallos detectados en cada sede de las sedes que conforman la RUP, plan de direccionamientos de red, si estos son públicos o privados, documentación existente que trate sobre las sedes de la RUP, existencia de gestión y servicios de red. Se deben tener en cuenta también aspectos organizativos que traten sobre los departamentos en los cuales están divididos cada una de las sedes y cuál es su relación con los demás departamentos, describir que políticas está siguiendo actualmente y si en verdad se están cumpliendo por ejemplo la norma ISO 9000 etc.

- Con la información recolectada se deben hacer una serie de análisis técnicos para ver en qué estado están a nivel de seguridad en este aspecto, para poder así detectar problemas de seguridad, existentes o potenciales, que puedan afectar a la integridad de los sistemas de la RUP como su funcionamiento o rendimiento. La información mínima que se debe recopilar debe ser la siguiente:

Determinación de los sistemas existentes: Aquí se debe determinar el nombre, tipo y fabricante del sistema, la ubicación, los responsables, software como sistemas operativos, los programas que corren en este y el estado de actualizaciones.

Determinación de las aplicaciones: nombre, fabricante y versión de la aplicación, en que sistema corre, como interactúa con otras aplicaciones, responsables y estado de las actualizaciones.

Análisis de vulnerabilidades en sistemas y aplicaciones: Se deben analizar los sistemas cuyo mal funcionamiento pueda ser la causa de un impacto negativo en los procesos de la red como pueden ser los servidores que tienen acceso público desde Internet, los puertos de los sistemas que pueden ser accedidos en forma remota identificando si están abiertos, cerrados o filtrados por algún firewall.

Se debe hacer un análisis local el cual permitirá ver el estado de seguridad del sistema recolectándose información a nivel general la cual incluya: nombre, responsable, tipo de sistema, sistema de archivos, utilización de memoria, actualizaciones, aplicaciones instaladas, puertos a la escucha y conexiones activas, usuarios y contraseñas, configuración de la red y tareas de ejecución periódica.

Es necesario revisar los diferentes dispositivos para detectar posibles fallos, encontrar formas más eficientes de implementarlos y para que mejoren su seguridad, estos dispositivos son los electrónicos de red (routers, switches, bridges, etc.), dispositivos de seguridad (firewalls, dispositivos de prevención de intrusiones, servidores de autenticación, etc.), aplicaciones (servidores Web, ftp, de correo, etc.) y en general cualquier dispositivo con una funcionalidad necesaria que pueda suponer una posible fuente de vulnerabilidades y elevación del nivel de riesgo asumido por la red.

- Después de la recolección general y técnica de información se procederá al análisis de toda la información recogida y situaciones existentes, estudiando las posibles carencias en seguridad de la información tomando como base los códigos de buenas prácticas existentes aplicables a los distintos sistemas y procesos analizados, metodologías y

estándares, en este caso el ISO 27001, y la experiencia y conocimiento aportado por el equipo de trabajo encargado del proyecto.

- Se elaborará un informe en donde aparecerá el estado de la seguridad de la información donde se proporcionará una visión global y detallada del estado de la red en cuanto a la seguridad de la información. En este informe se señalarán los aspectos mejorables que correspondan a la seguridad de la información así como proponer acciones correctivas priorizándolas de acuerdo con la relevancia que tengan para la RUP.

Este informe contendrá la información obtenida durante la recolección técnica de la información, estado actual de la red y sistemas de información, según esta información se revisarán las implicaciones existentes respecto a la seguridad de la información y se recomendarán las acciones necesarias para disminuir los problemas encontrados, después de esto se ordenarán las acciones según una calificación basada en la criticidad de su aplicación, esta calificación puede ser **crítica** si se requiere una aplicación inmediata para llevar a cabo las acciones recomendadas para afrontar su aplicación según el grado de riesgo, calificación **alta** la cual requiere una aplicación que se lleve a cabo en tres meses, calificación **media** llevada a cabo de tres a seis meses y calificación **baja** la cual llevará a cabo la acción de seis meses a un año. Finalmente, se plantearán una serie de medidas y controles de seguridad aplicables tal como se recomiendan en las guías de buenas prácticas según la norma ISO 27001.

El informe debe redactarse de forma clara y en un lenguaje fácilmente comprensible, evitando términos muy técnicos en la medida de lo posible, un resumen de los principales resultados y riesgos debido al estado actual de implementación de medidas, en lo que a seguridad de la información se refiere.

- Finalmente a la hora de implantar la estrategia de aseguramiento y protección de la información, se deben destinar unos recursos para llevar a cabo estas tareas, se harán labores de seguimiento para verificar que las tareas estén siendo llevadas a cabo por los responsables de su realización dentro de los tiempos determinados y se llevarán a cabo reuniones para revisar e informar periódicamente de cómo están siendo implantadas estas tareas.

CÁPITULO 4. PLANEACIÓN Y DISEÑO PARA LA RUP BAJO LA NORMA IEEE 802.16 CON UN NIVEL DE SEGURIDAD ALTO BASADO EN SOLUCIONES CRIPTOGRÁFICAS

En este capítulo se presentará una propuesta para la interconexión de las sedes que conforman la RUP haciendo uso de los criterios de seguridad previamente estudiados tales como seguridad de los algoritmos criptográficos y estándares de autenticación que emplea el estándar IEEE 802.16, así como también políticas de seguridad de la información a seguir según el estándar de Gestión de la Seguridad de la Información ISO 27001 escogido durante la realización del proyecto. De esta manera se busco diseñar una red inalámbrica de banda ancha capaz de soportar servicios con alta demanda de recursos y que a su vez tenga una alta confiabilidad en su desempeño.

Los pasos a seguir para la realización del diseño de esta red son tomados del trabajo de grado “Criterios para la Interconexión de Sitios Remotos bajo los Estándares IEEE 802.11 y 802.16”, el cual presenta una metodología para llevar a cabo la interconexión de sedes remotas de la Universidad del Cauca haciendo un estudio previo de las tecnologías inalámbricas llamadas comercialmente Wi-Fi y Wimax como alternativas para la implementación de estas conexiones y en el que se concluye que la mejor opción para conectar dichos sitios remotos es precisamente el estándar IEEE 802.16 o Wimax como fue adoptado por la industria de las telecomunicaciones alrededor del mundo.

Como primera instancia en el proceso de la planeación y diseño de una red basada en el estándar IEEE 802.16 o WiMAX para la RUP, se nombran las políticas de seguridad a seguir definidas en el estándar de seguridad de la información ISO/IEC 27001, el cual presenta las mejores alternativas de gestión de seguridad adecuadas al ámbito del presente trabajo.

4.1. POLITICAS DE SEGURIDAD INALÁMBRICAS PARA LA RED UNIVERSITARIA DE POPAYAN

A continuación se definen de manera general los requerimientos técnicos que cualquier administrador de la red WiMAX y de sus sistemas deberá configurar y así administrar los riesgos presentes manteniendo un nivel de seguridad adecuado para esta clase de redes, esto siguiendo algunos de los objetivos de control y controles presentes en el estándar de seguridad de la información ISO/IEC 27001 cláusulas del 5 al 15 los cuales proporcionan consultas y lineamientos para la implementación de las mejores prácticas en soporte de los controles especificados en A.5 al A.15 de su respectivo anexo. Estos objetivos se pueden dividir así:

4.1.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

ENTIDADES EXTERNAS En este punto se muestra cómo manejar la seguridad de la información en la red y los medios de procesamiento de la información a los cuales entidades externas tienen acceso. Aquí se deberán tener en cuenta el adecuado manejo de todos los puntos de entrada y salida de la red, centro de datos y salas de servidores, áreas de soporte IT y operaciones de la red entre otros.

1. Comprobar que las cámaras cubren los lugares de entrada clave en cada una de las sedes de la red.

2. Comprobar que los equipos de monitorización de alarmas esté funcionando adecuadamente.

3. Comprobar que en las áreas de trabajo no se escribe, registra o almacena de manera inapropiada información sobre la topología de la red o relacionada con las cuentas de usuario.

4. Comprobar que los conectores de red se encuentran desactivados en áreas públicas, salas, y demás áreas no utilizadas.

5. Comprobar que las personas que entran a la red lo hacen a través de los puntos de control monitorizados, utilizando tarjetas electrónicas con clave o identificándose ante un guardia de seguridad o cualquier otro personal en recepción.

6. Asegurar y proteger adecuadamente los medios de copias de seguridad y los discos de reparación de sistemas.

Con el objetivo de tener una idea de los requerimientos técnicos que el estándar exige para dar cumplimiento a sus políticas de seguridad, se realizó una encuesta (anexo E) a cada uno de los encargados del área de sistemas en las instituciones que conforman la RUP. Los datos obtenidos para la parte de organización de la seguridad de la información están consignados en la tabla 4.

Se puede observar que los controles básicos para tener una organización de la información adecuada en una institución son cumplidos en su gran mayoría por las instituciones que conforman la RUP.

TABLA 4. Controles para la organización de la seguridad de la información según el estándar ISO/IEC 27001 que se cumplen en las instituciones que conforman la RUP.

	INSTITUCIONES						
CONTROL	UNICAUCA	FUP	SENA	ITC	AUTONOMA	MAYOR	UCC
1	✓	✗	✓	✓	✗	✗	✗
2	✓	✗	✓	✓	✓	✓	✗
3	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	✓	✓	✓
6	✓	✓	✓	✓	✓	✓	✓

4.1.2 CONTROL DE ACCESO

CONTROL DE ACCESO AL SISTEMA DE OPERACIÓN. A continuación se indicarán algunas sugerencias para evitar el acceso no autorizado a los sistemas operativos más utilizados, los de la familia Windows NT y los sistemas operativos Linux.

1. Mantener al día las nuevas herramientas de seguridad desarrolladas por Microsoft y sus mejores prácticas, así como todos los paquetes de servicio y parches de seguridad que hayan salido en forma reciente.

2. Desactivar todos los servicios que no sean necesarios como por ejemplo los de archivos de impresión y configurar adecuadamente aquellos servicios que si sean verdaderamente necesarios.

3. Utilizar filtros IPSec para Windows 2000 y 2003 y el servidor de seguridad para conexión a Internet de Windows XP y así bloquear el acceso a cualquier puerto que se encuentre a la escucha.

4. Proteger los servidores conectados a Internet mediante muros de fuego o routers de red.

5. Limitar los privilegios interactivos de inicio de sesión para evitar ataques de escala de privilegios que llevan a adquirir la cuenta del administrador de la red.

6. Utilizar las directivas de grupo en Windows 2000 y 2003 para crear y distribuir configuraciones seguras.

7. Mantener los servidores más importantes en sitios físicamente seguros, definiendo contraseñas a nivel de BIOS para proteger la secuencia de inicio y también extraer la unidad de disquete o CD para evitar el inicio de sistemas operativos alternativos.

8. Se deben utilizar contraseñas eficaces combinando números y metacaracteres con una longitud mayor a 8 caracteres.

9. Se deben de utilizar herramientas que automáticamente cierren la sesión de usuario una vez este finalice la llamada.

10. Se deben limitar los intentos de inicio de sesión con máximo tres intentos fallidos antes de desconectar al usuario; y registrar los intentos exitosos y fallidos para así poder detectar y seguir a los atacantes de la red.
11. Se debe bloquear a los usuarios fallidos en las aplicaciones de control remoto.
12. Mantener actualizado la versión del kernel en los sistemas operativos Linux.
13. Eliminar los archivos que tengan el identificador de usuario SUID y el de grupo SGID de root para evitar que las malas prácticas de configuración y administración dejen comprometido el sistema, y así evitar violaciones en los permisos de archivos y directorios.
14. Escribir la información del archivo de registro en un medio que sea difícil de modificar o utilizar el comando syslog para enviar información critica de un registro a un PC seguro y así evitar que un atacante limpie los registros del sistema eliminando pistas de sus actividades.

De igual manera que en el punto anterior, los resultados que se obtuvieron de la encuesta respecto a esta parte de los controles en cada sede de las instituciones que conforman la RUP están consignados en la tabla 5.

La tabla 5 muestra que se tienen grandes falencias en cuanto a los controles que se deben cumplir para asegurar el acceso al sistema de operación de las redes, especialmente en la sede “Los Robles” de la Fundación Universitaria de Popayán, en el Colegio Mayor de Popayán y en la sede Norte de la Universidad Cooperativa de Colombia.

Los controles que no cumplen tanto la Universidad del Cauca, como la Universidad Autónoma y el Instituto Tecnológico de Comfacauca que tienen que ver con los sistemas

operativos de la familia Windows 2000 y Windows 2003 server no son cumplidos ya que éstas sedes no utilizan estos sistemas operativos en sus sistemas de operación de la red.

TABLA 5. Controles para el acceso al sistema de operación según el estándar ISO/IEC 27001 que se cumplen en las instituciones que conforman la RUP.

	INSTITUCIONES						
CONTROL	UNICAUCA	FUP	SENA	ITC	AUTONOMA	MAYOR	UCC
1	✓	✓	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓	✓	✓
3	✓	✗	✓	✓	✓	✓	✗
4	✓	✗	✓	✓	✓	✗	✗
5	✓	✓	✓	✓	✓	✓	✓
6	✗	✗	✗	✗	✗	✗	✗
7	✗	✗	✗	✗	✗	✗	✗

8	✓	✓	✓	✓	✓	✓	✓
9	✓	✗	✗	✓	✗	✗	✗
10	✗	✗	✗	✗	✗	✗	✗
11	✗	✗	✗	✓	✗	✗	✗
12	✓	✓	✓	✓	✓	✓	✓
13	✓	✗	✗	✓	✓	✗	✗
14	✓	✗	✗	✓	✓	✗	✗

CONTROL DE ACCESO A REDES. A continuación se indicará como evitar el acceso no autorizado a los servicios de red.

1. Revisar el registro de actividades de todos los usuarios para comprobar si existe alguna sobrecarga de acceso a la red que este consumiendo el ancho de banda.

2. Los usuarios remotos tienen que utilizar contraseñas adecuadas para mantener sus privilegios y se debería analizar periódicamente la calidad de estas.

3. Evitar la instalación de impresoras sin la debida configuración de seguridad, las cuales ofrecen conectividad abierta de fábrica, permitiendo la libre conexión a todas las impresoras de la red de forma remota.

4. En general, para evitar que algún usuario pueda tener acceso fácilmente a la red, esta debería mantener un registro de todos los equipos que tengan acceso al sistema para saber de antemano quien puede acceder a la red, que sistemas operativos se están utilizando y que direcciones del identificador MAC pueden acceder entre otros aspectos.

5. Se deben emplear mecanismos de autenticación basados en el uso de tarjetas inteligentes o testigos de hardware.

6. Buscar y eliminar la utilización no autorizada de software de control remoto.

7. Evitar la reutilización de claves compartidas ya que estas al ser utilizadas por las estaciones pueden ocasionar graves problemas de seguridad al no cambiarlas con la suficiente frecuencia.

8. Evitar por completo el tráfico no deseado en la frontera de red escuchando los puertos no utilizados de un sistema para poder detectar las peticiones de conexión de los puertos supuestamente silenciosos. Limitar al máximo la salida a Internet de cualquier usuario dentro de la red.

9. Migrar si es posible a una topología de red conmutada para evitar en un enlace entre redes Ethernet e inalámbrica herramientas que puedan capturar, interpretar y almacenar paquetes que viajan por la red.

10. Utilizar herramientas que descubran rastreadores basados en red que dispongan de detecciones en modo promiscuo y así evitar que el tráfico que es trasmitido a los demás equipos contenidos en un segmento de red sean analizados por algún delincuente informático.

11. Utilizar contramedidas electrónicas ECM para impedir la utilización del espectro radio específico evitando ataques que puedan afectar cualquier dispositivo de red.

12. Utilizar contra medidas electromagnéticas ESM que incluyan la interceptación, identificación, análisis y localización de alguna entidad que pueda interferir las fuentes de transmisión de alguna Estación Base.

13. Utilizar antenas direccionales o no isotrópicas para poder comunicar un área determinada dirigiendo la energía en una dirección común.

14. Estar prevenido siempre para afrontar ataques DoS de tráfico de red, enviando este tráfico a otros dispositivos y limitarlo utilizando algún protocolo de autenticación mutua como el protocolo de autenticación extensible EAP, que verifique el origen de los mensajes mediante la generación de claves fuertes de cifrado entre estaciones de trabajo de la red.

15. Verificar que los armarios de los equipos de telecomunicaciones sean físicamente seguros no permitiendo las zonas de acceso público, evitando así que algunos enlaces T1 entre edificios sufra de algún ataque de hombre en el medio.

16. Cambiar periódicamente los valores por defecto y las contraseñas de los equipos de red que vienen configurados de fábrica, ya que estos no ofrecen medidas de seguridad reales cuando traen estas configuraciones ya establecidas.

17. Cuando resulte posible y práctico configurar entradas estáticas entre el firewall y los routers de frontera en sistemas muy críticos en el protocolo de resolución de direcciones ARP al instalar un switch, así como Introducir manualmente las direcciones MAC en cada uno de estos dispositivos.

18. Para impedir el rastreo de contraseñas en texto plano se deberá cifrar todo el tráfico con un producto como SSH antes de ser enviado en forma de texto plano, o utilizar un túnel basado en IPSec para realizar cifrado extremo a extremo.

19. Se debe utilizar un método fuerte de cifrado con un buen algoritmo como el AES con una clave larga y adecuadamente protegida.

20. Utilizar un algoritmo de clave pública como el RSA para asegurar que los datos personales de los usuarios se mantengan privados así las claves de otros usuarios se vean comprometidas.

Los datos recopilados por medio de la encuesta realizada están consignados en la tabla 6, la cual evidencian muchas fallas en cuanto a los controles que se deben cumplir para asegurar un acceso a las redes de cada institución que sea seguro. Se deben mejorar en muchos aspectos especialmente en la sede “Los Robles” de la Fundación Universitaria de Popayán, el Colegio Mayor y la Universidad Cooperativa de Colombia, las cuales presentan el mayor número de falencias a dichos controles.

TABLA 6. Controles para acceso a redes según el estándar ISO/IEC 27001 que se cumplen en las instituciones que conforman la RUP.

	INSTITUCIONES						
CONTROL	UNICAUCA	FUP	SENA	ITC	AUTONOMA	MAYOR	UCC
1	✗	✗	✗	✗	✗	✗	✗
2	✓	✓	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓	✓	✓
4	✓	✗	✗	✓	✗	✗	✗
5	✓	✗	✗	✓	✗	✗	✗
6	✓	✓	✓	✓	✓	✓	✓
7	✓	✓	✓	✓	✓	✓	✓
8	✓	✗	✓	✓	✗	✗	✓
9	✓	✗	✗	✓	✓	✗	✗

	INSTITUCIONES						
CONTROL	UNICAUCA	FUP	SENA	ITC	AUTONOMA	MAYOR	UCC
10	✗	✗	✗	✗	✗	✗	✗
11	✗	✗	✗	✗	✗	✗	✗
12	✓	✗	✗	✗	✗	✗	✗
13	✗	✗	✗	✗	✗	✗	✗
14	✓	✗	✗	✗	✓	✗	✗
15	✓	✗	✓	✓	✓	✗	✗
16	✓	✓	✓	✓	✓	✓	✓
17	✓	✗	✓	✓	✓	✗	✗
18	✓	✗	✗	✗	✓	✗	✗
19	✓	✓	✓	✓	✓	✓	✓
20	✓	✓	✓	✓	✓	✓	✓

4.1.3 GESTIÓN DE COMUNICACIONES Y OPERACIÓN

PROTECCIÓN CONTRA SOFTWARE MALICIOSO Y CÓDIGO MÓVIL. En este apartado se muestra la forma en cómo se debe proteger el software y la información aplicando controles de detección, prevención y recuperación para proteger a la red de cualquier código malicioso y móvil que pueda afectarla.

1. No utilizar software de control remoto con la configuración predeterminada si se utilizan sistemas de autenticación de la familia Windows 2000 y 2003 ya que estos utilizan algoritmos de cifrado débil para tráfico de sesiones y utiliza sistemas de ocultación de contraseñas poco complicadas.

2. Al utilizar estas aplicaciones habrá que configurarlas para mejorar sus seguridad basándose en artículos de interés, boletines que Microsoft saca periódicamente, listas de verificación, herramientas de seguridad, freeware y aplicación de todos los parches disponibles que salen periódicamente.

3. No ejecutar programas localizados en Internet, lo más conveniente es descargarlos al computador, verificar si contienen virus y por ultimo si hay sospechas de algún archivo maligno probarlo en un sistema que no sea crítico.

4. Utilizar herramientas que permitan conocer el objetivo de cualquier programa que se encuentre en ejecución en algún sistema Windows o Linux, mostrando todos los puertos que se encuentran a la escucha y programas asociados y así poder detectar cualquier paquete entrante enviado de forma sospechosa.

5. Evitar la compresión de datos en SSH antes de cifrar la información así esto mejore los resultados en los enlaces si la red se vuelve lenta, ya que la compresión se suele predecir porque esta depende de la longitud de los datos originales, es necesario

intercalar algunos bytes nulos en el flujo de datos y evitar así ataques de análisis de tráfico como el de hombre en el medio y ataques pasivos como el automatizado mediante diccionario.

6. Controlar las claves públicas utilizadas en cada computador SSH y utilizar la autenticación de certificado cliente evita los ataques de hombre en el medio.

7. Utilizar versiones SSH actualizadas, ya que la versión SSH 1 provocaría ataques de diccionario para recuperar claves.

8. Utilizar siempre que sea posible, herramientas de cifrado de comunicaciones como SSH, SSL, correo electrónico seguro mediante PGP, sistemas de cifrado de la capa IP como IPSec, y así rechazar los ataques de escucha de las comunicaciones en la red.

9. Verificar que los servidores Web estén actualizados mediante parches. Realizar buenas prácticas en su configuración, validar también las entradas efectuadas por los usuarios y auditar de forma regular cualquier aplicación.

10. Mantener actualizado el software cliente de Internet, también obtener y utilizar de forma regular antivirus y comprobar que las firmas de estos se encuentren actualizadas con una periodicidad diaria y configurar todas sus funciones de exploración automatizada tanto como se pueda.

Los datos recopilados a través de la encuesta realizada a los encargados del área de sistemas en cada sede de las instituciones que conforman la RUP respecto a la protección contra software malicioso, se consignan en la tabla 7.

La tabla 7 nos muestra que el software que se ejecuta en los servidores y equipos que pertenecen a las redes de cada institución está bien controlado. Cabe anotar que los

controles numerados como 1 y 2 solo se cumplen en la sede de la Fundación Universitaria de Popayán sede "Los Robles" debido a que es la única institución que utiliza los sistemas operativos Windows 2000 y Windows server 2003 en sus equipos de control de la red.

TABLA 7. Controles para la protección contra software malicioso y código móvil según el estándar ISO/IEC 27001 que se cumplen en las instituciones que conforman la RUP.

	INSTITUCIONES						
CONTROL	UNICAUCA	FUP	SENA	ITC	AUTONOMA	MAYOR	UCC
1	✗	✓	✗	✗	✗	✗	✗
2	✗	✓	✗	✗	✗	✗	✗
3	✓	✓	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓	✓	✓
5	✗	✗	✗	✗	✗	✗	✗
6	✓	✗	✗	✓	✓	✗	✓
7	✓	✗	✓	✓	✓	✓	✓

8	✓	✗	✓	✓	✓	✓	✓
9	✓	✓	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓	✓	✓

Como resultado de la encuesta realizada se tiene que la sede con mayores falencias en cuanto a seguridad y controles de acceso a los equipos de red es la Fundación Universitaria de Popayán. Los equipos que utiliza tanto en el área de servidores como en el área de equipos terminales tienen muchos años en uso, lo cual hace necesario la actualización de los mismos para lograr cumplir con los objetivos mínimos de seguridad que presenta el estándar ISO/IEC 27001.

Las instituciones que mejor posicionadas se encuentran en cuanto a controles de seguridad para sus redes son la Universidad del Cauca y el Instituto Tecnológico de Comfacauca. Cumplen con la mayoría de los controles aquí presentados lo cual garantiza un nivel de seguridad de información alto, aunque esto no significa que los sistemas de estas instituciones sean 100% seguros.

Las políticas de seguridad que siguen las instituciones no están definidas explícitamente en ninguna de las sedes, se siguen algunas recomendaciones de seguridad pero éstas no están plasmadas en ningún medio ya sea magnético o impreso. El ITC está trabajando en un documento de políticas de seguridad el cual estará disponible para ser aplicado en este año pero que no sigue ningún estándar de gestión de seguridad de la información en

particular sino que responde a necesidades propias de su organización. En la Universidad del Cauca se tiene un documento de políticas de seguridad el cual es el resultado del trabajo de grado "CRITERIOS PARA ESTABLECER POLITICAS DE SEGURIDAD DE LA INFORMACION Y PLAN DE CONTINGENCIA, CASO DE ESTUDIO EL CENTRO DE DATOS DE LA UNIVERSIDAD DEL CAUCA" y que presenta algunas propuestas de acciones para asegurar la información siguiendo el estándar de seguridad de la información ISO/IEC 27001.

4.2. DISEÑO DE LOS ENLACES

El proceso seguido para realizar las políticas de seguridad de la información en el diseño de la red WiMAX para la RUP comienza con la manera adecuada de cómo se pueden administrar y como están presentes los riesgos en el estándar, es decir, una vez identificados los riesgos que este presenta (ver cápitulo dos), comprendiendo e identificando las vulnerabilidades y sus posibles vías potenciales de ataque, al igual que las amenazas con sus objetivos potenciales que son la confidencialidad, integridad y disponibilidad de la información, y como estas pueden violar la seguridad del entorno de sistemas de información de la red inalámbrica, se deberán tomar en cuenta al identificar las vulnerabilidades, que contramedidas se deben de seguir como firewalls, software antivirus, controles de acceso, cifrado de datos, capacitación de empleados en las políticas a seguir para la red inalámbrica, sistemas de detección de intrusos entre otros; evitando así una potencial vía de ataque a la que se pueda ver expuesta la red WiMAX.

Como se mencionó anteriormente, el proceso de diseño de los enlaces de la red WiMAX para la RUP es tomado del trabajo de grado "Criterios para la Interconexión de Sitios Remotos bajo los Estándares IEEE 802.11 y 802.16", el cual plantea 3 fases: *Configuración del Enlace*, *Levantamiento del Sitio* y *Selección de Equipos*.

4.2.1 CONFIGURACIÓN DEL ENLACE. Las sedes de las instituciones que conforman la RUP se encuentran ubicada en el área urbana de la ciudad de Popayán a excepción de la sede Los Robles de la Fundación Universitaria de Popayán y la sede Norte del SENA, esto hace que estos dos puntos sean los más críticos en el diseño de la red. La topología escogida para la implementación del diseño es PTM, ya que esta clase de red es utilizada debido a que la Estación Base puede brindar conectividad a las diferentes Estaciones Suscriptoras que se ubicarán en las sedes de la RUP siendo esta topología más efectiva en el entorno en el cual se encuentra la ciudad de Popayán desde el punto de vista beneficio, costo y seguridad, finalmente esta topología es la que mas predomina a nivel mundial en entornos urbanos siendo mucho más efectiva en la ciudad debido a la ubicación geográfica, características demográficas y topográficas entre otras que presenta la ciudad.

La Estación Base estará ubicada en la terraza de la Facultad de Ingeniería Electrónica y Telecomunicaciones de la Universidad del Cauca, mejor conocida como "El palomar", y con estaciones suscriptoras ubicadas en cada sede de las instituciones que conforman la RUP, es la mejor opción en cuanto a infraestructura, seguridad, costo de implementación y operación, gestión de la red y disponibilidad de la misma. La banda de operación del sistema es la de 5.8 GHz por ser no licenciada y estar separada en 0.8 GHz de la banda de operación del proveedor de servicios de Internet a través de WiMAX UNE, evitando así la interferencia entre los sistemas.

Ubicación de los Extremos a Conectar

UNICAUCA: Será la ubicación de la estación base del sistema, con soporte PTM y la cual dará servicio e interconexión a las demás sedes de las Instituciones que conforman la RUP. El sitio mejor ubicado y con las mejores condiciones de infraestructura de torre, fuentes de corriente alterna, seguridad, cercanía de puntos de red, accesibilidad y costos para la ubicación, gestión y mantenimiento de los equipos es la terraza de la FIET o "El Palomar" como se le conoce comúnmente. La tabla 8 muestra los datos de ubicación geográfica del sitio.

Tabla 8. Datos ubicación geográfica de la EB en UNICAUCA.

UNICAUCA EL PALOMAR	
Latitud	2°26.800'' N
Longitud	76°35.197'' O
Altitud	1744

UNIVERSIDAD COOPERATIVA DE COLOMBIA: La estación suscriptora para esta institución estará ubicada en la sede Norte en la que opera la Facultad de Ingenierías y tiene el mayor número de usuarios de toda la Universidad, aunque esta institución también cuenta con otra sede ubicada en el sector sur de Popayán y en la que funciona la facultad de derecho, el número de usuarios es reducido al igual que el número de usuarios en las instalaciones de la biblioteca ubicada a corta distancia de dicho edificio. La tabla 9 muestra los datos de ubicación geográfica del sitio.

Tabla 9. Datos ubicación geográfica de la ES de la UCC.

UNIVERSIDAD COOPERATIVA DE COLOMBIA SEDE NORTE	
Latitud	2°26.800'' N
Longitud	76°35.197'' O
Altitud	1744
Distancia a la EB	1,24 Km

COLEGIO MAYOR DEL CAUCA: Ubicado en el centro de la ciudad, reúne todos sus programas académicos en un solo edificio, lo que hace que el número de posibles usuarios de la red sea elevado. Esta sede cuenta con programas de formación en diferentes áreas del conocimiento y hace que la conexión con otros centros educativos de educación superior sea relevante para el desarrollo de los estudiantes inscritos en sus programas. La institución cuenta con 3 salas de cómputo con un total de 30 computadores habilitados para los estudiantes y con los equipos de control de red ubicados en una pequeña sala. La tabla 10 muestra los datos de ubicación geográfica del sitio.

Tabla 10. Datos ubicación geográfica de la ES del Colegio Mayor.

COLEGIO MAYOR DEL CAUCA	
Latitud	2°26.800'' N
Longitud	76°35.197'' O
Altitud	1744
Distancia a la EB	1 Km

SENA: El Servicio Nacional de Aprendizaje tiene su sede educativa en el sector norte de la ciudad, es ahí donde se forman una gran cantidad de personas en diversas áreas productivas. El número de salas de cómputo es de 10, cada una de ellas con un objetivo específico. Existe además una sala de videoconferencia con equipos avanzados de video, audio y datos. Esta sede es la más alejada de la EB hacia el norte, lo cual la convierte en un punto crítico en el diseño de la red. La tabla 11 muestra los datos de ubicación geográfica del sitio.

Tabla 11. Datos ubicación geográfica de la ES del SENA.

SENA SEDE NORTE	
Latitud	2°26.800'' N
Longitud	76°35.197'' O
Altitud	1744
Distancia a la EB	5,75 Km

COR*PORACIÓN UNIVERSITARIA AUTÓNOMA DEL CAUCA*: Ubicada en el sector centro de la ciudad, opera en un moderno edificio el cual está adecuado con la infraestructura necesaria para albergar una gran cantidad de estudiantes en diferentes programas académicos. Cuenta además con un sistema de alarmas que hacen de esta sede un sitio seguro contra posibles catástrofes naturales y cámaras de vigilancia en ciertos puntos críticos del edificio. La tabla 12 muestra los datos de ubicación geográfica del sitio.

Tabla 12. Datos ubicación geográfica de la ES de la Autónoma.

AUTÓNOMA	
Latitud	2°26.800'' N
Longitud	76°35.197'' O
Altitud	1744
Distancia a la EB	0,95 Km

INSTITUTO TECNOLÓGICO DE COMFACAUCA: El ITC, como ha sido mencionado a lo largo del trabajo, cuenta con el edificio más moderno de todas las sedes de las instituciones que conforman la RUP. En sus instalaciones en el centro de la ciudad de Popayán, operan varios sistemas de alarmas contra incendios, cortes de energía, terremotos. También tienen implementados sistemas de detección de humo, detectores de movimiento en lugares críticos del edificio como el área de servidores de red, área administrativa y sala de docentes. Alberga una gran cantidad de estudiantes tanto de los programas técnicos como del colegio el cual funciona en un edificio contiguo pero que tiene una comunicación directa con el ITC. La tabla 13 muestra los datos de ubicación geográfica del sitio.

Tabla 13. Datos ubicación geográfica de la ES del ITC.

ITC	
Latitud	2°26.800'' N
Longitud	76°35.197'' O
Altitud	1744
Distancia a la EB	1,08 Km

FUNDACIÓN UNIVERSITARIA DE POPAYÁN: En su sede Los Robles ubicada sobre la Vía Panamericana al sur de la ciudad la FUP cuenta con un importante número de estudiantes los cuales se trasladan hasta esta sede campestre a las afueras de Popayán para adelantar sus estudios, esto hace inminente la necesidad de una conexión a fuentes de información para cada uno de los programas que allí se adelantan. Para ello la FUP cuenta con 3 salas de cómputo con un total de 36 equipos pero que en este momento no cuentan con una conexión a internet adecuada para atender los usuarios, adicional a esto, la FUP en su sede Los Robles no cuenta con equipos adecuados para las tareas de gestión y control de la red y sus medidas de seguridad son las más precarias de todas las sedes de las instituciones que conforman la RUP. Cuenta con un enlace satelital a Internet que en este momento tiene un valor elevado y hace que la opción de una conexión de mas bajo costo sea muy tenida en cuenta. La tabla 14 muestra los datos de ubicación geográfica del sitio.

Tabla 14. Datos ubicación geográfica de la ES de la FUP.

FUNDACIÓN UNIVERSITARIA DE POPAYÁN	
Latitud	2°26.800'' N
Longitud	76°35.197'' O
Altitud	1744
Distancia a la EB	9,16 Km

4.2.2 LEVANTAMIENTO DEL SITIO. Para la configuración de red empleada en el diseño es necesario tomar cada enlace por separado verificando que se cumplan las condiciones

para que la señal de radiofrecuencia llegue a su destino de manera que pueda sostener un enlace óptimo para las funciones y servicios que se puedan prestar sobre ellos. En este caso en particular, los puntos más críticos son los enlaces que se deben calcular entre el SENA y el palomar y entre la FUP y El Palomar debido a su gran distancia de separación, los otros enlaces no presentan mayor dificultad en su diseño debido a que el estándar IEEE 802.16 en la frecuencia escogida (5.8 GHZ) y para distancias cortas como las que se presentan en estos enlaces, admite ambientes NLOS. Las condiciones de propagación para los enlaces con las sedes ubicadas en el centro de la ciudad y la de la UCC sede norte inclusive, son los adecuados para trabajar en este tipo de ambientes; algunas de estas condiciones son la no presencia de un gran número de edificios altos en la zona, terreno uniforme en cuanto al tipo de suelo y niveles de altura que en la zona centro de la ciudad de Popayán no sufre cambios drásticos y fuentes de interferencia con otros sistemas que operen en la misma banda.

La ubicación geográfica de las sedes a interconectar se presenta en la figura 10, tomada del programa libre Google Earth.

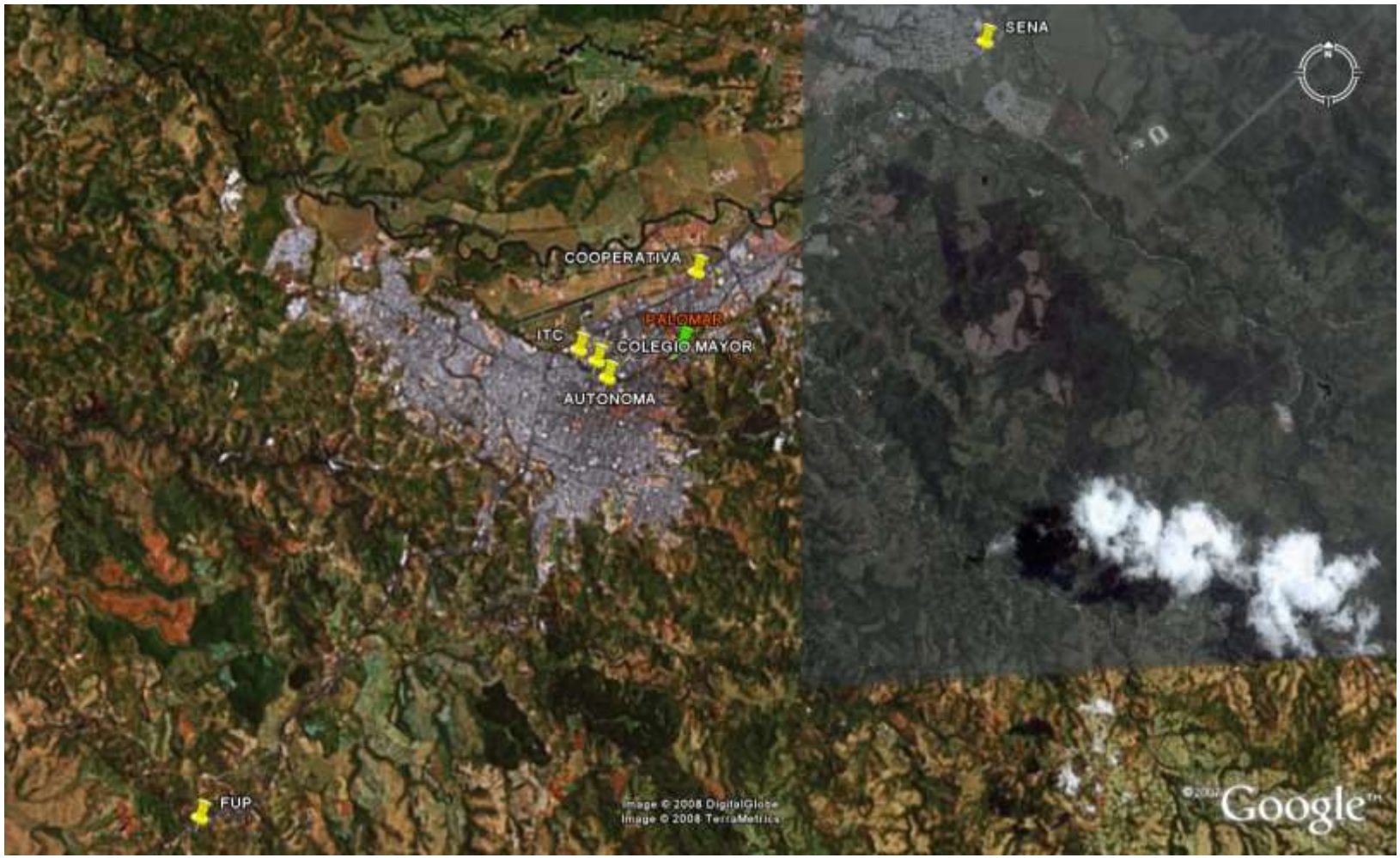


Figura 10. Ubicación geográfica de cada sede a interconectar.

Siguiendo una de las políticas de seguridad para interconexiones inalámbricas el diseño se debe hacer tratando de no radiar potencia hacia zonas que no se necesiten o que no tengan usuarios evitando que posibles atacantes tengan la posibilidad de ubicarse en muchos sitios y desde ahí realizar sus actividades que atentan contra la seguridad de la red y evitando el desperdicio de potencia radiada de una manera inútil. Dado que las ES son fijas, la EB debería radiar sólo hacia los lugares en los que éstas se encuentran. El uso de una antena omnidireccional evidentemente atentaría con esta premisa, así que la opción propuesta es la de emplear 2 antenas directivas o sectoriales las cuales darían el servicio a todas las sedes. La primera atendería la sede norte de la UCC y la sede del SENA y la segunda atendería los nodos del centro de la ciudad y la FUP sede Los Robles, de esta manera se evita radiar en forma imprudente hacia sitios innecesarios.

ANÁLISIS DE RF

La frecuencia de operación escogida para el diseño de la red WiMAX para la RUP es la banda no licenciada de 5.8 GHZ, la cual no interfiere con el sistema WiMAX que funciona actualmente en la ciudad de Popayán puesto en funcionamiento por la empresa de telecomunicaciones UNE que emplea la banda de 5.0 GHZ para dar servicio a sus usuarios. Las condiciones de propagación en este ambiente como la no presencia de gran cantidad de edificios altos en la zona, tipo de terreno prácticamente similar con poco cambio en los niveles de altura. Sin embargo, es necesario realizar un análisis del nivel de interferencia probable con otros sistemas que puedan operar en la zona, para ello se debe contar con equipos especializados en este tipo de mediciones y tener una idea clara del ambiente de RF presente en la zona. Debido a las grandes capacidades que tiene el estándar en cuanto

al manejo de interferencia y modulación, estas otras señales no tendrían que interferir en el correcto funcionamiento de los enlaces aquí propuestos.

4.2.3 PRESUPUESTO DEL ENLACE Y SELECCIÓN DE EQUIPOS. En esta parte se realizan los cálculos de propagación de RF y niveles de potencia en las estaciones suscriptoras para verificar que el enlace es viable. Los datos de potencia de salida del trasmisor, ganancia de antenas, pérdidas en conectores y cables, sensitividad del receptor y pérdidas en las líneas de transmisión son tomados de la información que entregan algunos fabricantes de equipos WiMAX y serán usados de manera tentativa para el cálculo de cada uno de los enlaces.

Los cálculos de propagación de RF se realizan mediante la fórmula:

$$L_{fs}[dB] = 32{,}45 + 20\log f[MHz] + 20\log d[Km] \qquad (4\text{-}1)$$

En donde:

L_{fs}: Pérdidas de espacio libre f: Frecuencia de operación

d: Distancia entre puntos

$$P_{Rx} = P_{Tx} - L_{Tx} - L_{CTx} + G_{Tx} - L_{fs} + G_{Rx} - L_{Rx} - L_{Rx} \qquad (4\text{-}2)$$

Donde:

P_{Rx}: Nivel de señal en recepción en dBm

P_{Tx}: Potencia a la salida del transmisor en dBm

L_{Tx}: Pérdidas en la línea de transmisión en dB

L_{CTx}: Pérdidas por los conectores en los equipos de transmisión en dB

G_{Tx}: Ganancia de la antena transmisora en dBi

L_{fs}: Pérdidas de espacio libre

G_{Rx}: Ganancia de la antena receptora en dBi

L_{Rx}: Pérdidas en la línea de recepción en dB

L_{CRx}: Pérdidas por los conectores en la los equipos de recepción en dB

$$SOM = P_{Rx} - S_{Rx} \tag{4-3}$$

Donde:

SOM: Margen de Operación del Sistema S_{Rx}: Sensitividad del receptor en dBm

Los valores que se utilizan para realizar los cálculos están basados según la selección de los siguientes equipos:

ESTACIÓN BASE: Alvarion BreezeACCES VL [14]

ANTENA ESTACIÓN BASE: EUROPEAN ANTENNAS VECTOR SA16-60-5.5V/9501 [16]

ESTACIÓN SUSCRIPTORA: Axxcelera AB-FULL ACCES II 100/16T1/E1 [15]

ANTENA ESTACIÓN SUSCRIPTORA: Antena Externa integrada en el producto Axxcelera AB-FULL ACCES II 100/16T1/E1 [15]

La escogencia de la estación base es justificada con la posibilidad de manipular la suite de algoritmos criptográficos que utiliza, la flexibilidad que presenta en el manejo de

diferentes sistemas hace que cumpla con los requisitos de seguridad de protocolos de cifrado expuestos en el trabajo de grado como es el de no utilizar el algoritmo DES. Además esta estación base tiene la capacidad de trabajar en una topología PTM haciendo una asignación dinámica de canal para cada estación suscriptora.

La estación suscriptora a su vez, presenta las mejores condiciones de sensitividad, ganancia de antena, y potencia de salida (para los enlaces de subida). De esta manera los valores para el cálculo del enlace son los siguientes:

P_{Tx} Estación Base = 23 dBm

P_{Tx} Estación Receptora = 23dBm

G_{Tx} Estación Base = 17,5 dBi

G_{Rx} Estación Suscriptora = 23dBi

$L_{Tx} = L_{Rx} = 1dB$

$L_{CTx} = L_{CRx} = 0.4$ dB

Sensitividad Estación Suscriptora = -84dBm ~ -70dBm

Sensitividad Estación Base = -71dBm ~ -92dBm

Los valores de la sensitividad varían de acuerdo con el tipo de modulación empleado, por esta razón los fabricantes presentan un rango de valores. En nuestro caso utilizaremos los valores para las mejores condiciones de modulación.

Con los anteriores valores y utilizando las fórmulas (4 - 1), (4 - 2) y (4 – 3) los valores obtenidos para los enlaces de bajada se presentan en la tabla 15.

Tabla 15. Presupuesto de los enlaces Downlink de la red WiMAX para laRUP.

PARÁMETROS	ENLACES DOWNLINK					
	UNICAUCA - COOPERATIVA	UNICAUCA – MAYOR	UNICAUCA – SENA	UNICAUCA – AUTÓNOMA	UNICAUCA – ITC	UNICAUCA – FUP
f [MHz](1)	5800	5800	5800	5800	5800	5800
d[Km]	1,24	1	5,75	0,95	1,08	9,16
L_{fs}[dB](2)	109,5869	107,7185	122,9119	107,2730	108,3870	126,9564
P_{Tx}[dBm]	23	23	23	23	23	23
L_{Tx}[dB]	1	1	1	1	1	1
L_{CTx}[dB]	0,4	0,4	0,4	0,4	0,4	0,4
G_{Tx}[dBi]	17,5	17,5	17,5	17,5	17,5	17,5
G_{Rx}[dBi]	23	23	23	23	23	23
L_{Rx}[dB]	1	1	1	1	1	1
L_{CRx}[dB]	0,4	0,4	0,4	0,4	0,4	0,4
P_{Rx}[dBm](3)	-48,8869	-47,0185	-62,2119	-46,5730	-47,6870	-66,2564
S_{Rx}[dBm](4)	-70	-70	-73	-70	-70	-77
SOM[dB]	21,1131	22,9815	10,7881	23,4270	22,3130	10,7436

(1) El valor de la frecuencia es sólo por facilidad de cálculo, ya que la estación base es la encargada de asignar de forma dinámica las frecuencias tanto de subida como de bajada que emplea el enlace con cada estación suscriptora.

(2) El valor de este parámetro es el resultado de aplicar la fórmula (4 - 1)

(3) Este valor es el resultado de aplicar la fórmula (4 – 2)

(4) Los valores de la sensitividad utilizada en cada enlace varían dependiendo de las condiciones del mismo ya que valores de SOM por debajo de 10dBm son considerados

como prueba de un mal funcionamiento del enlace. Esto quiere decir que se debe utilizar una modulación que permita trabajar con este nivel de S_{Rx}.

De igual manera, se deben calcular los enlaces de subida para asegurar que también están dentro de los parámetros de correcto desempeño del mismo. Estos cálculos se presentan en la tabla 16.

Tabla 16. Presupuesto de los enlaces Uplink de la red WiMAX para la RUP.

PARÁMETROS	ENLACES UPLINK					
	COOPERATIVA UNICAUCA	MAYOR UNICAUCA	SENA UNICAUCA	AUTÓNOMA UNICAUCA	ITC UNICAUCA	FUP UNICAUCA
f [MHz](1)	5800	5800	5800	5800	5800	5800
d[Km]	1,24	1	5,75	0,95	1,08	9,16
L_{fs}[dB](2)	109,5869	107,7185	122,9119	107,2730	108,3870	126,9564
P_{Tx}[dBm]	23	23	23	23	23	23
L_{Tx}[dB]	1	1	1	1	1	1
L_{CTx}[dB]	0,4	0,4	0,4	0,4	0,4	0,4
G_{Tx}[dBi]	23	23	23	23	23	23
G_{Rx}[dBi]	17,5	17,5	17,5	17,5	17,5	17,5
L_{Rx}[dB]	1	1	1	1	1	1
L_{CRx}[dB]	0,4	0,4	0,4	0,4	0,4	0,4
P_{Rx}[dBm](3)	-48,8869	-47,0185	-62,2119	-46,5730	-47,6870	-66,2564
S_{Rx}[dBm](4)	-71	-71	-73	-71	-71	-77
SOM[Db]	22,1131	23,9815	10,7881	24,4270	23,3130	10,7436

CONCLUSIONES

El estándar 802.16 2004 presenta riesgos debido a que su modelo de seguridad fue tomado literalmente de las redes cableadas no prestándole atención a los posibles ataque que éste pudiera sufrir en su medio de transmisión inalámbrico, sin embargo, el estándar 802.16e al ser rediseñado en su estructura de seguridad corrige estas vulnerabilidades presentes en la versión anterior. La suite de algoritmos de cifrado de datos que maneja el estándar IEEE 802.16 con su posibilidad de utilización de forma flexible hace que el estándar tenga un alto nivel de seguridad, esto no significa que sea 100% seguro.

El algoritmo de cifrado de datos que presenta menor nivel de confiabilidad es el DES, el cual se emplea en el estándar IEEE 802.16 como método de cifrado de clave privada en el proceso de autenticación e intercambio de información entre las estaciones suscriptoras y la estación base. Debido a que los avances en la tecnología de cómputo hacen que cada vez sea posible realizar más operaciones en menos cantidad de tiempo, los ataques a este tipo de algoritmo de cifrado se vuelven más fáciles de ejecutar con herramientas hardware y software cada vez más poderosas para lograr quebrar la seguridad del mismo.

El algoritmo de cifrado con clave privada AES y el algoritmo de cifrado con clave pública RSA que emplea el estándar IEEE 802.16 para establecer conexiones entre las estaciones base y las estaciones suscriptoras tienen un nivel de confiabilidad mucho mayor que los utilizados en otro sistema de comunicación de datos inalámbrica como el IEEE 802.11. Esto hace que el ataque a estaciones base WiMAX desde estaciones suscriptoras no autorizadas para hacer uso de los recursos de la red sea en gran medida dificultosa. Todos los ataques que pueden presentarse a este tipo de algoritmos de cifrado necesitan como parte vital para realizar su cometido, el tener a disposición información en texto plano de los datos que se envían, esto es a su vez hace que atacantes exteriores a la red tengan un gran nivel de dificultad tratando de vulnerar la seguridad del estándar, pero a su vez, se podría decir que un posible atacante dentro de la red y que tenga acceso a este tipo de información vital pueda utilizar esta información de manera mal intencionada o maliciosa.

La asignación de valores aleatorios a los identificadores de los certificados digitales de la EB y las ES pueden solucionar los problemas de autenticación mutua y autorización de las SA detectados en la realización del trabajo, esto hace que mejore considerablemente la probabilidad de generar falsificaciones de EB y ES autorizadas, ya que anteriormente los valores de identificación de cada entidad eran fijos, fácilmente detectados y reutilizados.

Reducir el valor de tiempo de vida de la llave, trae como consecuencia menor probabilidad de ser atacada, porque en la actualidad el valor por defecto de este parámetro es de siete días, lo cual se considera un valor bastante riesgoso para los administradores de seguridad.

A pesar que los métodos de cifrado que utiliza el estándar son el mecanismo principal para asegurar la información entre estaciones, el sistema de cifrado no hace diferencia entre usuarios legítimos e ilegítimos, si ambos presentan las mismas claves el cifrado por sí mismo no proporcionará seguridad, debe haber entonces, controles sobre claves de cifrado y del sistema como un todo.

Los Estándares de Gestión de Seguridad de la Información son una herramienta muy útil para contrarrestar las vulnerabilidades que se presenten en un sistema de información de una organización. También dan una pauta para evitar diferentes tipos de inconvenientes a nivel de seguridad que se pueden presentar en un sistema de comunicación de datos y que sin ellos podrían pasar desapercibidos, ocasionando tal vez fallas que pudieran ser previstas con anterioridad.

El estándar de seguridad escogido para el presente trabajo de grado el ISO 27001, fué utilizado como punto de partida para el establecimiento del programa de seguridad para el diseño de la red WiMAX. El documento fué utilizado como una guía para las diferentes áreas que se necesitaban cubrir para dar seguridad a la red y no se tomó como un conjunto de requerimientos los cuales deben cumplirse al pie de la letra, en este punto el

análisis de riesgos del estándar determinó las necesidades más básicas de seguridad para la red.

Las instituciones que conforman la RUP no tienen unas políticas de seguridad definidas, haciendo que los sistemas, equipos y recursos de la red presenten vulnerabilidades y falencias de seguridad no solo en la información sino también en los activos de la organización ya que no se tiene un sistema de gestión de la seguridad como guía para afrontar las posibles fallas dentro de la organización. Aun así, las instituciones que tienen un nivel de seguridad por encima de las otras son la Universidad del Cauca y el Instituto Tecnológico de Comfacauca. Estas instituciones tienen los equipos necesarios para configurar un sistema de comunicación de datos con capacidad de atender a una gran cantidad de usuarios, prestar servicios informáticos de forma segura y atender las posibles fallas en los sistemas de control de manera eficiente, todo esto mediante dispositivos de alarmas, control de acceso, diferenciando adecuadamente el personal y teniendo los equipos en áreas físicamente seguras. Por otro lado, la sede que más dificultades presenta en cuanto a infraestructura de red, seguridad en todos los aspectos y manejo de políticas de seguridad es la sede Los Robles de la Fundación Universitaria de Popayán y en la que se deben hacer grandes esfuerzos para lograr un nivel de seguridad mínimo en sus instalaciones y minimizar las vulnerabilidades que allí se presentan en todos los aspectos.

Según el estudio del estándar 802.16, la red WiMAX propuesta para la RUP es capaz de ofrecer una solución con un nivel de seguridad alto si se siguen adecuadamente las políticas de seguridad expuestas en este trabajo de grado, permitiendo prestar servicios multimediales que demanden una gran cantidad de ancho de banda e interconectar de manera económica y eficiente a las instituciones educativas que conforman la RUP.

RECOMENDACIONES

Estimular el estudio de los algoritmos criptográficos más utilizados en la actualidad ya que éstos están presentes en muchos procesos de comunicación de datos y redes de telecomunicaciones y hacen que los sistemas que los adopten sean cada vez más seguros y confiables. De esta manera se logra tener un conocimiento más amplio del funcionamiento de una red de datos y tener la capacidad de afrontar de mejor manera dificultades que se puedan presentar cuando se presenten ataques a estos sistemas de información.

En el área de criptografía, el paso a seguir es el estudio de la nueva tendencia de cifrado de datos llamada "criptografía cuántica" la cual permitirá en los próximos años romper con facilidad los actuales sistemas de cifrado simétricos y asimétricos.

Se recomienda realizar pruebas a las propuestas de seguridad del presente trabajo de grado las cuales se enfocan en hacer más seguro el protocolo PKM que el estándar 802.16 maneja en su subcapa de seguridad, a fin de verificar el desempeño y hacer mejoras, de ser necesarias, evaluando el nivel de vulnerabilidad que pueda presentarse en el protocolo original y el propuesto para verificar y comparar la integridad de los datos.

Realizar futuras investigaciones en el área de la seguridad de la información, específicamente en cómo pueden ser protegidos los datos contra escritura y su posterior reutilización. Los ataques de este tipo sigue siendo un desafió para los investigadores.

Utilizar equipos de estaciones base que ofrezcan la posibilidad de usar una suite de algoritmos de cifrado flexible en los diseños o implementaciones WiMAX ya que se debe evitar que tanto éstas estaciones como las estaciones suscriptoras utilicen el algoritmo de cifrado de clave privada DES debido a que en este momento es considerado poco seguro y

obsoleto en aplicaciones que demanden un nivel de seguridad bastante alto. De esta manera se evita la mayor vulnerabilidad que presenta el estándar IEEE 802.16.

Adoptar total o parcialmente el estándar de seguridad de la información más adecuado para las necesidades de cada sede que componen la RUP. En UNICAUCA parte de este trabajo ya ha sido realizado mediante la publicación de un documento basado en el estándar ISO/IEC 27001 adoptando ciertas medidas para tener políticas de seguridad dentro de la institución. En el ITC se tendrá próximamente un documento con las políticas de seguridad que la institución va a seguir como medida preventiva contra ataques de diferente índole a sus redes. En un plano más ambicioso se podría pensar en conseguir la certificación en alguno de estos estándares y de esta manera ubicar a la RUP como organización pionera en este campo en Colombia.

Es importante hacer el seguimiento adecuado a las diferentes políticas establecidas en la red relacionadas con el desarrollo de la cultura organizacional en seguridad, tanto en aprendizaje, entrenamiento y educación, como de la correcta aplicación de los mismos en las actividades diarias de cada miembro de la RUP, pues en caso contrario, al no existir los indicadores de seguimiento correspondientes, no se podrá conocer el impacto de dichos planes ni tampoco conocer las acciones necesarias para la corrección oportuna.

Mejorar la infraestructura montada en la sede de Los Robles de la FUP ya que ésta presenta los niveles más bajos en cuanto a inversión en equipos, seguridad física en donde se alojan los componentes de control y gestión de la red y mejorar los controles de acceso a estas instalaciones. De esta manera se lograría minimizar las vulnerabilidades de la red WiMAX de la RUP ya que éste es el punto que presenta más falencias en cuanto a la seguridad en general y puede ser catalogado como el punto más crítico para la seguridad en general de la red WiMAX para la RUP.

REFERENCIAS BIBLIOGRAFÍCAS

[1] ABISHEK, Maheshwari. Implementation and Evaluation of a MAC Sheduling Architecture for IEEE 802.16 Wireless MANs. Department of Computer Science and Engineering Indian Institute of Technology Kanpur. 2006.

[2] AHSON, Syed y ILYAS, Mohammad. wimax standars and security. 2007.

[3] ALEXANDER, Alberto. Gestión en el Manejo de Seguridad en la Información: BS 7799-2:2002. Perú. 2005. 6 p. Disponible en: http://centrum.pucp.edu.pe/excelencia/ensayos/Gestion_manejo_seg_inf_bs7799.pdf

[4] ALLISON, Lucy y MANN, Ian, BS7799-3 (ISO 27005) Risk Assessment, ECSC, 2006.

[5] BAINO, Paul. Evaluation and Security Risks Associated with Networked Information Systems. Royal Melbourne Institute of Technology. 2001.

[6] BAYONA, Camargo y MORENO, Oscar. Advanced Encription Standar (AES). Universidad Nacional de Colombia. Colombia.

[7] COMITÉ BDD/2. Gestión de la Seguridad de la Información BS7799 – 2:1999 Especificaciones para Sistemas de Gestión de Seguridad de la Información. Estándar Británico.

[8] CORLETTI, Alejandro Cesar. Estrategia de Seguridad Informática por Acción Retardante. Universidad Politécnica de Madrid. 2005.

[9] DAMIR, Sarac. Security Mechanisms for IEEE 802.16 Based Mesh Networks. Technische Universit¨at Darmstadt. 2006.

[10] De BUSTOS, José Angel. Criptografía. HispaLinux. España. 2005.

[11] DURÁN, Raúl; HERNÁNDEZ, Luis y MUÑOZ, Jaime. Ataques a DES y Módulos Factorizados de RSA. Departamento de Tratamiento de la Información y Codificación Instituto de Física Aplicada. España. 2000.

[12] FÚSTER, Amparo; De la GUÍA, Dolores; HERNÁNDEZ, Luis; MONTOYA, Fausto; MUÑOZ, Jaime. Técnicas Criptográficas de Protección de Datos 3a Edición Actualizada. Ra-Ma Editores. España. 2004.

[13] HELENIUS, Lauri. Master's Thesis Analysing B2B e-order System Security Threats. Helsinki University of Technology. 2004.

[14] http://www.alvarion.com

[15] http://axxcelera.com

[16] http://www.european-antennas.co.uk

[17] http://goliath.ecnext.com/coms2/summary_0199-6964687_ITM

[18] http://www.is2me.org/index.html

[19] http://www.iso27000.es/sgsi.html

[20] HUERTA, Antonio Villalón. Códigos de Buenas Prácticas de Seguridad. UNE-ISO/IEC 17799, 2004.

[21] HUIDOBRO, José. Seguridad en Redes y Sistemas Informáticos, 2005.

[22] INSTITUTO ARGENTINO DE NORMALIZACIÓN. Esquema 1 de Norma IRAM-ISO/IEC 17799. Argentina. 2002.

[23] ISEC. Programa Integral de la Formación Profesional en Implementación Práctica de Medidas de Seguridad de la Información. Information Security Education Center. 2006 .

[24] JHONSTON, David y WALKER, Jesse. Overview of IEEE 802.16 Security. IEEE Security and Privacy: IEEE Computer Society vol. 2 No. 3. Mayo/Junio 2004. 9 p. Disponible en http://www.computer.org/security.

[25] KRISHNUN, Sansurooah. An assessment of threats of the Physical and MAC Address Layers in WiMAX/802.16. School of Computer and Information Science (SCIS). University Perth, Western Australia. 2006.

[26] LOW, Richard y STAMP, Mark. Applied Cryptanalysis. John Wiley & Sons Inc. USA. 2007.

[27] LUCENA, Manuel. Criptografía y Seguridad en Computadores 4ª Edición. Creative Commons. España. 2007. Disponible en: http://wwwdi.ujaen.es/_mlucena/lcripto.html.

[28] M. H, Lau. Research on the Relationships between Risk Perception, Risk Propensity and Risk-Reducing Decision-Making in a E-Goverment Enviroment. Erasmus University of Rotterdam. Abril de 2006.

[29] TIPTON, Harold F y KRAUSE, Micki. Information Security Managment Handbook Sixth Edition. Auerbach Publications. USA. 2007.

[30] UNIVERSIDAD NACIONAL DE COLOMBIA, DIRECCION NACIONAL DE INFORMÁTICA Y COMUNICACIONES, Lista de Estándares de Seguridad Internacionales, 2003.