UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"GESTIÓN DE REDES INALÁMBRICAS EN LA FACULTAD DE INGENIERÍA"

T E S I S

PARA OBTENER EL TÍTULO DE
INGENIERO EN COMPUTACIÓN

P R E S E N T A

EDSON ARMANDO GUERRERO MARTÍNEZ

DIRECTOR DE TESIS:

ING. RAFAEL SANDOVAL VÁZQUEZ

CIUDAD UNIVERSITARIA MÉXICO D.F. 2009

ÍNDICE

Capítulo 3 Estrategia de gestión de redes inalámbricas.

Capítulo 4 Herramientas de gestión de redes inalámbricas

ÍNDICE DE FIGURAS

Capítulo 1 Fundamentos

Capítulo 3 Estrategia de gestión de redes inalámbricas

Capítulo 4 Herramienta de gestión de redes inalámbricas

Capítulo 5 Implantación de medidas de gestión

Capítulo 7 Configuraciones adecuadas y buenas prácticas

ÍNDICE DE TABLAS

PRÓLOGO

Las redes inalámbricas actualmente son una tecnología que ha crecido su popularidad debido a los beneficios que ofrece, principalmente la movilidad, sin embargo existe una mala reputación resultado de las brechas de seguridad que representa el trasmitir información por medio del aire, en donde cualquier persona puede interceptarla, es por ello que como parte de los recursos institucionales las redes inalámbricas en la Facultad de Ingeniería deben de ser gestionadas de manera que se optimice su funcionamiento.

La existencia de las redes inalámbricas dentro de la Facultad de Ingeniería ha ido creciendo de manera exponencial haciéndolo de manera descontrolada, coexistiendo una gran cantidad de puntos de acceso por toda el área geográfica la institución. En esta situación de completo desconocimiento de las redes inalámbricas vecinas, puede haber puntos de acceso en donde se esté viendo afectado el rendimiento a causa de esta proliferación desordenada.

Los problemas no son sólo para los usuarios, sino que los administradores llegan a tener problemas de rendimiento, interferencias y configuraciones, por lo que conforme las redes inalámbricas van creciendo es cada vez más complicado tener el control sobre ellas. El protocolo 802.11 describe la tecnología de trasmisión de paquetes, la estructura de ellos, entre otras características, sin embargo no resuelve el tema de la gestión y control de las redes inalámbricas.

Cada administrador de las redes inalámbricas deberá estar resolviendo las tareas comunes de administración como los son actualizaciones del firmware de los puntos de acceso, control de potencia de las antenas, localización de los clientes, puntos de acceso que no estén dando servicio, entre otras muchas actividades que se deben desarrollar. No obstante estas acciones serán realizadas sobre las redes que estén a su cargo, es por ello que se necesita de un control de manera general para conocer el panorama en la institución.

Este trabajo pretende proponer una estrategia para la gestión de este recurso de información. La acciones que se plantean como solución a la problemática ya descrita es un proyecto que permita hacer más eficientes las comunicaciones inalámbricas dentro de la institución así como contar con información necesaria para cuando se llegue a presentar algún incidente de cómputo relacionado con las redes inalámbricas existentes en la Facultad de Ingeniería.

ESTRUCTURA DE LA TESIS

En el capítulo **1 Fundamentos** se comienza con la base teórica de las redes inalámbricas, durante el desarrollo de éste se tocarán términos que son necesarios para poder comprender el funcionamiento del las redes 802.11. Es muy importante el entendimiento de los términos y significados ya que estos serán utilizados durante todo este trabajo de tesis.

Una vez comprendida la terminología se presentará el capítulo **2 Problemática actual de la Facultad de Ingeniería** en donde se describe el escenario vigente las redes inalámbricas en la institución, se necesita conocer la problemática para entender la magnitud de la omisión que se tiene en cuanto a la gestión de esta Tecnología de Información que debe de empezar a tomarse en cuenta dentro de los esquemas de seguridad vigentes.

El capítulo **3 Estrategia de gestión de redes inalámbricas** se presenta con el objetivo de hacer un análisis de riesgos que trasciendan en una estrategia integral de protección de las comunicaciones móviles dentro de la Facultad. Se elaborará por medio de una metodología una estrategia que permita resolver las amenazas y vulnerabilidades que se detecten. Una gran consecuencia de esta actividad será la realización de las Políticas de Seguridad en las Redes Inalámbricas para la Facultad de Ingeniería así como un procedimiento de registro para tener un control sobre esta tecnología.

Una forma de controlar la información de las redes inalámbricas existentes en la Facultad, será por medio de una base de datos y un sistema que manipule esta información con el objetivo de gestionar de mejor manera este recurso. El capítulo **4 Herramienta de gestión de redes inalámbricas** describe el procedimiento de desarrollo de esta aplicación.

El capítulo **5 Implantación de medidas de gestión** detalla la manera que se implementarán las acciones descritas como estrategia de gestión de las redes inalámbricas, se tomarán aspectos como la forma en que se publicarán las políticas desarrolladas así como la descripción de herramientas que podrán ser utilizadas para mejorar la operación y mantenimiento de estas tecnologías de radiofrecuencia.

La actividad que se debe de establecer como una práctica obligada en la gestión de Tecnologías de Información está desarrollada en el capítulo **6 Auditoría en redes inalámbricas**. Esta acción se desarrollará en los aspectos de auditoría en la configuración, en el cumplimiento a las políticas, en la seguridad y del servicio.

Por último el capítulo **7 Configuraciones adecuadas y buenas prácticas** se describirán algunas prácticas recomendadas de seguridad, así como algunos programas que servirán como herramientas de monitoreo y auditoría en las redes inalámbricas.

OBJETIVO

Crear los elementos que permitan la gestión de manera ordenada y adecuada en los aspectos normativos, técnicos y de seguridad de las Redes Inalámbricas de la Facultad de Ingeniería de la UNAM; proporcionando para ello un fundamento teórico y práctico, a través del análisis, de políticas y de la creación de una herramienta en línea que consolide las actividades de regulación; generando con todo ello buenas prácticas en la operación de las redes inalámbricas.

CAPÍTULO

1

FUNDAMENTOS

En este primer capítulo se establecen los conceptos básicos de redes de datos y redes inalámbricas que permitirán la mejor comprensión de los capítulos posteriores. Es muy importante el desarrollo y entendimiento de estos fundamentos ya que aquí se acentúa la mayoría de la terminología necesaria que se utilizará para este trabajo de tesis.

1.1 REDES DE COMPUTADORAS

Una red es un sistema de comunicación entre computadoras que permite la transmisión de datos de una máquina a la otra, por lo que se puede compartir recursos e información. Las redes de computadoras poseen dos características principales:

- Se encuentran interconectadas mediante algún medio de transmisión.
- Son autónomas, es decir que no son controladas por otras computadoras, poseen la capacidad de procesar los datos por si solas.

Las redes de computadoras tienen como objetivos principales:

- Compartir recursos, equipos, información, programas que se encuentran de manera local o de la misma forma software distribuido en diferentes computadoras.
- Brindar confiabilidad a la información, disponiendo de alternativas de almacenamiento.
- Transmitir información entre usuarios distantes de la manera más rápida y eficiente posible.

1.1.1 CLASIFICACIÓN DE LAS REDES DE COMPUTADORAS

En la actualidad existes muchos tipos de redes de computadoras cada una con sus características y objetivos diferentes, sin embargo, estas redes de computadoras pueden ser clasificadas de acuerdo a sus características principales. Una de las clasificaciones más comunes de las redes de computadoras son: las redes privadas dedicadas y las redes compartidas.

Las redes privadas dedicadas son aquellas en las existe un único tipo de tráfico además de un determinado número de nodos que tienen como propósito asegurar la calidad, la seguridad y/o velocidad. Normalmente se utilizan para garantizar el servicio de transporte de datos en ciertas condiciones, a grandes grupos de usuarios de la red. Las tecnologías que soportan estas redes dedicadas dependen, en primer lugar, del tipo de información que manejan: voz, video o datos. Este tipo de red puede estructurarse en redes punto a punto o redes multipunto.

En una red punto a punto se permiten las conexiones en línea directa entre equipos y terminales. La ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión y la seguridad que presenta al no existir conexión con otros usuarios. En una red multipunto se permite la unión de varias terminales a su correspondiente computadora compartiendo una única línea de transmisión. La ventaja consiste en la disminución de costos, aunque pierde velocidad y seguridad.

Las redes compartidas son aquellas en las que se une un gran número de usuarios, compartiendo todas las necesidades de transmisión e incluso con comunicaciones de otras naturalezas. Las redes más usuales de este tipo son las de conmutación de paquetes y las de conmutación de circuitos.

Otra forma de clasificar a las redes de computadoras es por su extensión y su alcance.

1.1.1.1 REDES DE ÁREA PERSONAL (*Personal Area Network*, PAN)

Las Redes de Área Personal son de alcance muy limitado (unos pocos metros), y se utilizan para interconectar dispositivos personales de manera inalámbrica (*Personal Computers PCs*, laptops, celulares, *Personal Digital Assistants PDA's,* impresoras, etcétera). Estas redes son de velocidad media (algunos Mbps) y están teniendo creciente desarrollo en los últimos años.

1.1.1.2 REDES DE ÁREA LOCAL (*Local Area Network*, LAN)

Son las redes con una determinada área local, es decir las redes de pequeñas oficinas o empresas que desean aplicar tecnología informática para compartir archivos, software e impresoras de manera eficiente además de permitir las comunicaciones entre los equipos que estén conectados a esa red. Estas redes operan dentro de un área geográfica limitada, permiten el multi-acceso a medios con alto ancho de banda, controlan la red de forma privada con administración local, proporcionan conectividad continua a los servicios locales y conectan dispositivos físicamente adyacentes.

1.1.1.3 REDES DE ÁREA METROPOLITANA (*Metropolitan Area Network*, MAN)

Son las Redes de Áreas Metropolitanas, un poco más extensas que las anteriores ya que permiten la conexión en un nivel más grande, como una ciudad con una población pequeña. Una MAN generalmente consta de una o más LAN dentro de un área geográfica común.

1.1.1.4 REDES DE ÁREA AMPLIA. (*Wide Area Network*, WAN)

Son las Redes de Área Extensa, aquellas de grandes dimensiones que conectan países e incluso continentes. Las redes WAN son las que vinculan las redes LAN, que a su vez proporcionan acceso a las computadoras o a los servidores de archivos en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las organizaciones compartan información entre sí a través de grandes distancias. El software de colaboración brinda acceso a información en tiempo real y a recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona.

TABLA 1.1 Clasificación de las redes

TIPO DE RED	RANGO	ANCHO DE BANDA
PAN	>10 m.	10 Mbps
LAN	1-2 km.	10-1.000 Mbps
MAN	2-50 km	2-155 Mbps
WAN	100-1000 km	1 Mbps - 1 Gbps

1.1.2 TOPOLOGÍAS DE RED

Existen diferentes maneras de conectar los dispositivos de una red, dependiendo de las necesidades que se tengan será la arquitectura que puede adoptar. Cada una de estas clasificaciones de alguna forma compartirá el medio de transmisión de los datos. Las topologías básicas de las redes de datos son las siguientes:

- Topología de Anillo.
- Topología de Bus.
- Topología de Estrella.
- Topología de Árbol.

1.1.2.1 TOPOLOGÍA DE ANILLO

Esta topología hace referencia a su nombre por la forma que toman los equipos conectados entre sí para formar un anillo físico del medio de transmisión. Los equipos que forman parte de la red se conectan uno con otro hasta llegar al último equipo que se conecta al primero. La forma de comunicación entre dos equipos que forman este anillo es mandando un paquete de información que viaja a través del medio pasando por todas las computadoras hasta llegar al destino, haciendo énfasis en que el paquete y la información en general circulará en sólo un sentido.

Para poder formar el anillo y conectar el medio de transmisión a los equipos se necesita de un repetidor que es un circuito que recibe datos por un lado y los envía por el otro. Una de las ventajas de este tipo de topología es que puede operar a grandes velocidades y los mecanismos para evitar las colisiones que se pueden llegar a efectuar entre los paquetes de información son sencillos.

1.1.2.2 TOPOLOGÍA DE BUS

En esta topología se usa un sólo cable como eje de la red al cual se conectan todos los equipos; mejor conocido como *backbone*, que termina en ambos extremos. Cuando los equipos quieren comunicarse se envían los paquetes por el medio de transmisión y todos los equipos pueden escuchar la señal, sin embargo este paquete lleva la información de la dirección a la cual va dirigido, por lo que si no son los destinatarios se ignora la información.

1.1.2.3 TOPOLOGÍA DE ESTRELLA

En esta topología cada uno de los equipos que pertenecen a la red está conectado a un conmutador central. Aquí el envió de los paquetes de información viaja a través del medio de transmisión y llegan al punto central donde cada uno de los equipos puede ver la información, el nodo central o conmutador envía la información recibida a todos los demás nodos de la red.

1.1.2.4 TOPOLOGÍA DE ÁRBOL

En esta topología de tipo jerárquica se compone de un punto raíz a partir del cual se conectan uno o más cables, en donde cada uno de ellos puede tener ramificaciones a cualquier otro punto, es decir que cada ramificación a partir del nodo central puede ramificarse, cabe señalar que en este tipo de topologías no se pueden formar ciclos.

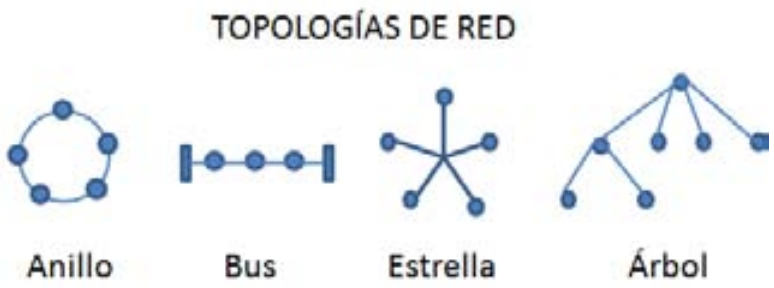


FIGURA 1.1 Topologías de Red

1.2 MODELO OSI (*Open System Interconnection*)

El modelo de referencia de Interconexión de Sistemas Abiertos (*Open System Interconnection*, OSI) creado por la Organización Internacional de Normalización como necesidad de establecer un estándar para el creciente desarrollo de las tecnologías de red y hacer que éstas tecnologías fueran compatibles además de aplicables a todas las redes existentes al momento, surgió en 1984. El modelo OSI ofrece muchas ventajas como por ejemplo reduce mucho la complejidad de los protocolos de interconexión de redes, asegura la interoperabilidad de la tecnología, estandariza interfaces que intervienen en el procesamiento de los paquetes de información, etcétera.

El modelo OSI permite hacer un análisis de cómo la información viaja en la red, de manera muy detallada va llevando paso a paso cómo un paquete de información pasa a través de diferentes capas de este modelo. Las capas del modelo OSI son 7, las cuales se describen a continuación:

- Capa Física. Transmisión de datos a nivel binario esto se logra mediante la transmisión física de las señales con niveles de voltajes diferentes, en esta capa interviene lo que son los elementos físicos como cables de red, conectores, voltajes, velocidades de transmisión de datos.

- Capa de Enlace de Datos. Su objetivo es dar fiabilidad a la transmisión de las señales eléctricas, tener el control directo de enlaces, acceso a los medios, provee transferencia confiable de datos a través de los medios, conectividad y selección de ruta entre sistemas, direccionamiento lógico además de una tarea muy importante: el control de flujo.

- Capa de Red. La asignación de dirección de red y determinación de la mejor ruta es decir el direccionamiento, provee transferencia confiable de datos a través de los medios. Conectividad y selección de ruta entre sistemas.

- Capa de Transporte. El objetivo principal de este nivel consiste en asegurar la calidad de transmisión de datos, ordenar la información, ajustar la velocidad de información. Se ocupa de aspectos de transporte entre dispositivos, además de establecer, mantener y terminar circuitos virtuales, detección de fallas y control de flujo de información de recuperación.

- Capa de Sesión. Comunicación entre los dispositivos: establece, administra y termina sesiones entre aplicaciones.

- Capa de Presentación. Representación de los datos, garantiza que los datos sean legibles para el sistema receptor, formato de los datos, estructuras de datos, negocia la sintaxis de transferencia de datos para la capa de aplicación.

- Capa de Aplicación. Procesos de red a aplicaciones, suministra servicios de red a los procesos de aplicaciones como los son por ejemplo correo electrónico, transferencia de archivos y emulación de terminales.

FIGURA 1.2 Modelo OSI

1.3 MODELO TCP/IP

El modelo TCP/IP creado por el Departamento de Defensa de los Estados Unidos como una necesidad de tener compatibilidad entre las redes y medios de transmisión en épocas de guerra, fue desarrollado como un estándar abierto es decir que cualquier persona podía usar el estándar. *Transfer Control Protocol* (TCP), proporciona mecanismos de control de flujo y errores entre los extremos que están llevando a cabo la comunicación, por otro lado *Internet Protocol* (IP), es un protocolo que proporciona mecanismos de interconexión entre redes de área local.

El modelo TCP/IP está compuesto por 4 capas:

- Capa de Aplicación. Maneja aspectos de presentación, codificación y control de dialogo.

- Capa de Transporte. Tiene como objetivo la calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. El protocolo para el control de la transmisión (TCP) ofrece maneras flexibles de alta calidad para crear comunicaciones de red confiables sin problemas de flujo y con un nivel de error bajo. Orientado a conexión.

- Capa de Red. El propósito de la capa es dividir los segmentos TCP en paquetes y enviarlos desde cualquier red. Los paquetes llegan a la red destino independientemente de la ruta que utilizaron para llegar allí. El protocolo específico que rige esta capa se denomina *Protocolo de Internet* (IP). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. La relación entre IP y TCP es importante. Se puede pensar en el IP como el que indica el camino a los paquetes, en tanto que el TCP brinda un transporte seguro.

- Capa Física. Esta capa guarda relación con todos los componentes, tanto físicos como lógicos, necesarios para lograr un enlace físico. Incluye los detalles de tecnología de red, y todos los detalles de la capa física y de enlace de datos del modelo OSI.

La capa física se refiere a cualquier tecnología en particular utilizada en una red específica. Independientemente de los servicios de aplicación de red que se brinden y del protocolo de transferencia que se utilice, existe un sólo protocolo de Internet, IP. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier computadora en cualquier parte del mundo pueda comunicarse en cualquier momento.

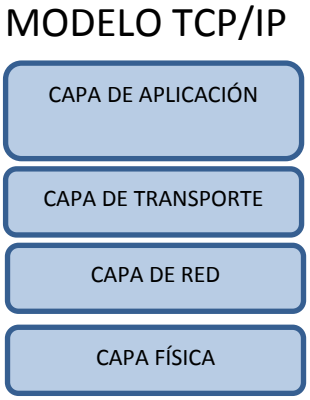


FIGURA 1.3 Modelo TCP/IP

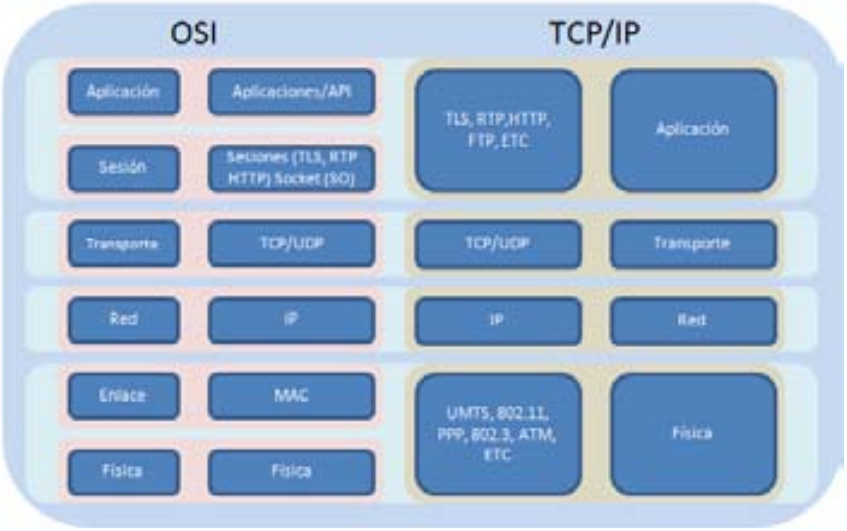


FIGURA 1.4 Modelos OSI – TCP/IP

1.4 REDES INALÁMBRICAS

Las redes inalámbricas es un término nuevo que se ha formado en un tiempo relativamente corto, gracias al gran avance y popularidad de las comunicaciones móviles. En el mercado, se ha visto reflejado este *boom* de lo referente a la movilidad de las redes e Internet. Obviamente esto ha beneficiado al desarrollo de las redes inalámbricas locales, como por ejemplo en que la implementación de una red inalámbrica se ha simplificado, el bajo costo de los elementos que la conforman, y flexibilidad para su uso. Las redes inalámbricas pueden ser conectadas a una red LAN cableada como una extensión del sistema o pueden operar de manera independiente para permitir conexiones de datos entre computadoras.

Las redes inalámbricas pueden proveer de casi todas las funciones y las altas tasas de transferencia ofrecidas por una red cableada LAN. Las velocidades en las que una red WLAN opera típicamente son entre los 1 Mbps a 54 Mbps.

En la industria el estándar referente a las redes inalámbricas que describe las especificaciones inalámbricas es el 802.11, fue liberado en junio de 1997, en su primera versión.

Desde la perspectiva del usuario, sus funciones y uso son exactamente como una red Ethernet LAN, sin embargo el poder controlar el acceso en un medio de transmisión como el aire los métodos son más complejos que aquellos que se controlan por un medio cableado (Ethernet).

Hay diferentes versiones de redes inalámbricas 802.11 WLAN, las diferencias de estas redes radican en la banda de frecuencia en que operan, el tipo de acceso inalámbrico y las velocidades máximas de transmisión.

1.4.1 TIPOS DE REDES INALÁMBRICAS

En la actualidad existe variedad de estándares que permiten la conectividad entre dispositivos, así mismo las computadoras hoy en día ya traen soporte para más de un estándar de conectividad de dispositivos para hacerlas operables entre ellas, es así que en los últimos años los estándares de conectividad inalámbrica y tecnologías han emergido y tenido un gran auge que sigue en aumento. Estas tecnologías hacen que los usuarios puedan acceder a una amplia gama de recursos de cómputo y telecomunicaciones de manera fácil y simple. Con estos estándares de conectividad inalámbrica se tiene la posibilidad de poder crear redes punto a punto de manera inalámbrica sin que el usuario necesite tener conocimientos técnicos avanzados. Con el auge de estos nuevos estándares las velocidades de transmisión han ido mejorando haciéndolos más populares.

Hay muchas tecnologías y estándares como lo son Bluetooth, Asociación de datos Infrarrojos (*Infrared Data Association,* IrDA), Radiofrecuencia (*HomeRadioFrequency*, HomeRF), y los estándares de IEEE 802.11. El principal propósito de estos estándares y tecnologías es usar la radio-tecnología para hacer transmisiones de datos de manera inalámbrica, además de poder formar redes y comunicarse con varios dispositivos con tecnologías compatibles, sin embargo no se debe de perder en cuenta que la elección de la tecnología inalámbrica para su uso, dependerá de cuál va ser su ámbito de aplicación.

1.4.1.1 BLUETOOTH

Bluetooth es una tecnología inalámbrica de alta velocidad, baja potencia y que usa las microondas, diseñadas para conectar teléfonos, laptops, PDA´S y otros equipos portátiles. A diferencia de los infrarrojos, no requiere que los dispositivos estén alineados para poder trasmitir datos. Esta tecnología hace algunas modificaciones en el estándar de redes inalámbricas 802.11 pero estas modificaciones lo hacen pequeño y de bajo costo. Su funcionamiento depende del área de cobertura de cada dispositivo, si

se está dentro del rango de alcance del dispositivo y se encuentra otro dispositivo con la misma tecnología, los dispositivos comienzan a intercambiar información de conectividad y forman la red sin necesidad de configuración alguna por parte del usuario.

Algunas características importantes de la tecnología de Bluetooth son:

- Opera en la banda ISM (*Industrial, Scientific and Medical*) en los 2.56 GHz, la cual es global (no se requiere licencia para su uso).
- Usa el espectro ensanchado por salto de frecuencia (*Frequency Hop Spread Spectrum*, FHSS).
- Puede soportar arriba de ocho dispositivos en una red pequeña conocida como "piconet".
- Es Omnidireccional es decir no se necesita estar alineado con el dispositivo para trasmitir o recibir datos.
- Alcanza de 10 a 100 metros.
- Tecnología de bajo costo.
- Consume aproximadamente 1 mWatt de potencia.

1.4.1.2 IrDA (*Infrared Data Association*)

IrDA es una organización internacional que crea y promueve el estándar de bajo costo de interconexión de datos por medio de infrarrojos. IrDA ofrece un conjunto de protocolos a nivel de la capa de transferencia de datos, además del manejo redes de este tipo y sus diseños de operatividad. Los protocolos de IrDA tienen como vehículo de entrega de datos IrDA DATA y para el control de envió de información IrDA CONTROL. En general IrDA es usada para proveer conectividad inalámbrica del tipo punto a punto con un estrecho ángulo de cobertura alrededor de 30° y está diseñado para operar en una distancia de 0 a 1 metro de distancia a una velocidad de 9600 bits por segundo a 4 Mbps. Algunas características importantes de esta tecnología son:

- Alcance: desde el contacto hasta 1 metro ó 2.
- Consume muy poca potencia.
- Transmisión de datos desde 9600 bps con la velocidad primaria o 115 kbps hasta un máximo de velocidad de 4 Mbps.
- Comunicación bidireccional.
- Los paquetes de información enviados son protegidos usando Control de Redundancia Cíclica (CRC) que es un mecanismo de detección de errores en sistemas digitales, CRC-16 para velocidades arriba de 1.152 Mbps y CRC-32 para 4 Mbps.

1.4.1.3 HomeRF (*Home RadioFrequency*)

HomeRF es parte de la Unión Internacional de Telecomunicaciones y que primordialmente trabajó en el desarrollo del estándar de bajo costo de radiofrecuencia (RF) para voz y datos; el grupo de trabajo de HomeRF desarrolló *Shared Wireless Access Protocol* (SWAP) que es una especificación de la industria que permite a PCs, periféricos y otros dispositivos comunicarse con voz y datos de manera inalámbrica, es similar a 802.11 pero con una extensión de tráfico de voz. Puede operar con topología Ad-Hoc o con una de tipo infraestructura, se requiere un punto de coordinación del sistema. Las paredes y techos no causan problemas de pérdida de funcionalidad y el identificador provee de un poco de seguridad, es robusta y fiable además de minimizar el impacto de interferencia de ondas de radio.

Algunas características de HomeRF son las siguientes:

- Opera en la banda ISM en el rango de los 2.45 GHz y no se necesita licencia.

- Alcanza arriba de 45 metros.
- Emplea una frecuencia de saltos de 50 saltos por segundo.
- Soporta Acceso Múltiple por División del Tiempo (*Time Division Multiple Access, TDMA*) para proveer entrega interactiva de voz y utiliza CSMA/CA (*Carrier Sense, Multiple Access, Collision Avoidance*) de alta velocidad para entrega de paquetes de datos.
- Puede formar una red de hasta con 127 nodos.
- Consume una potencia de 100mW.
- Su velocidad de transmisión es de hasta 2 Mbps.
- Arriba de 6 conexiones de voz bidireccional o full dúplex.
- Seguridad y compresión de datos.

1.4.2 FAMILIA DE PROTOCOLOS 802.11

El protocolo 802.11 pertenece a la familia de IEEE 802 en el que se describen las especificaciones para las tecnologías de redes de área local.

Las especificaciones de IEEE 802 se centran en las dos últimas capas inferiores del modelo OSI ya que incorporan tanto componentes físicos como componentes de enlace de datos. Todas las redes 802 tienen un componente de la subcapa de control de acceso al medio (*Medium Access Control*, MAC) y un componente físico. MAC es un conjunto de reglas para determinar cómo acceder al medio y enviar datos, pero los detalles de la transmisión y recepción los proporciona la capa física.

La especificación base del protocolo 802.11 incluye la subcapa MAC del protocolo 802.11 y dos capas físicas: una capa física de Dispersión del Espectro de Salto de Frecuencia *(FHSS, Frecuency-Hopping Spread-Spectrum)* y una capa de enlace de Dispersión del Espectro de Secuencia Directa *(DSSS, Direct-Sequence Spread-Spectrum)*. Las revisiones posteriores a 802.11 han añadido capas físicas adicionales.

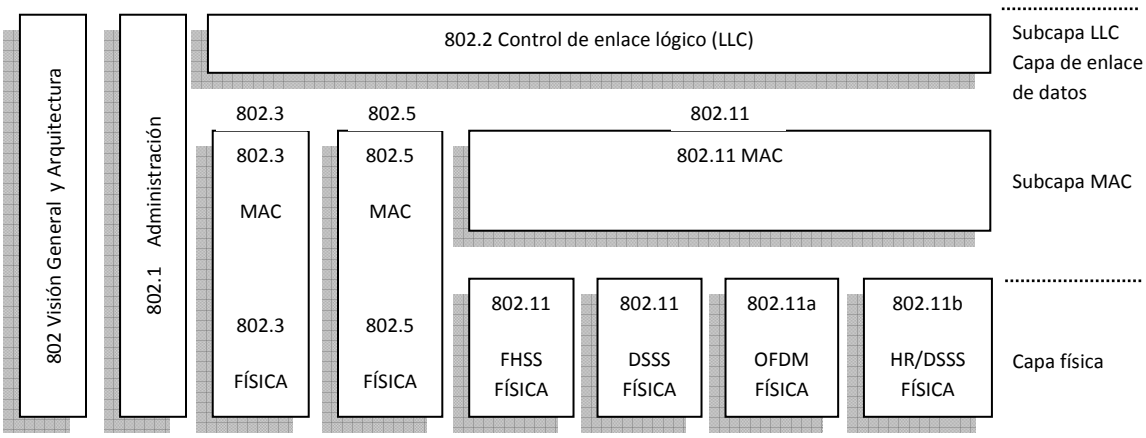


FIGURA 1.5 Familia 802.11 y su relación con el modelo OSI.

El uso de ondas de radio como capa física requiere también una capa física relativamente compleja. 802.11 divide la capa física en dos componentes de medio físico genéricos: el Procedimiento de Convergencia de Capa Física (*PLCP, Physical Layer Convergence Procedure*) para asignar las tramas MAC en el medio y un sistema Dependiente del Medio Físico (*PMD, Physical Medium Dependent*) para transmitir dichas tramas. El PLPC crea un puente entre el límite del MAC y de las capas físicas. En 802.11, el PLCP añade diversos campos a la trama a medida que se transmite en el aire.

A continuación se presenta un cuadro que da una breve descripción de la familia del estándar 802.11:

TABLA 1.2 Familia del protocolo 802.11

FAMILIA 802.11	Descripción
802.11a	Estándar creado para la operación de redes WLAN en espectro de 5 GHz con velocidades de transmisión arriba de los 54 Mbps. Describe una capa física basada en un Multiplexado de División de Frecuencia Ortogonal (*OFDM, Orthogonal Frequency Division Multiplexing*). Fue publicado en el año de 1999.
802.11b	Estándar creado para la operación de redes inalámbricas de área local en el espectro electromagnético de los 2.4 GHz con velocidades arriba de los 11 Mbps. Especifica una capa de Secuencia Directa de Alta Velocidad (*HR/DSSS, High-Rate Direct Sequence*). Publicado en 1999.
802.11c	Provee la documentación de los procedimientos de la subcapa MAC del protocolo 802.11 de la Organización Internacional de Estándares/ Comisión Internaciones Electrotécnica (ISO/IEC).
802.11d	Publica las definiciones y requerimientos para habilitar el estándar 802.11 para poder operar en países que aun no están utilizando.
802.11e	Intenta hacer mejoras en la subcapa MAC de 802.11 para incrementar la calidad en el servicio lo mejor posible (*QoS, Quality of service*). Las mejoras en la capacidad y eficiencia están previstas para permitir aplicaciones tales como voz, video o audio sobre redes inalámbricas 802.11.
802.11f	Desarrollo de prácticas recomendadas para la implementación 802.11 en los conceptos de puntos de acceso y sistema de distribución. El propósito es incrementar la compatibilidad entre dispositivos de puntos de acceso de diferentes fabricantes.
802.11g	Es la capa física más moderna del bloque. Ofrece una velocidad superior a través del uso de OFDM con respecto al estándar 802.11 manteniendo una compatibilidad con dispositivos 802.11b. La velocidad objetivo es de al menos 20Mbps. Cuando coexisten usuarios 802.11b y 802.11g en el mismo punto de acceso, se requiere de un coste operativo de protocolo adicional, reduciéndose la velocidad máxima para los usuarios de 802.11g.
802.11h	Aumento de la subcapa MAC 802.11 y la capa física de 802.11a para proveer gestión de la red y control de las extensiones del espectro y administración de la banda de los 5 GHz. Esto permitirá la aceptación del estándar en algunos países europeos.
802.11i	Refuerzo de la seguridad y de los mecanismos de autenticación del estándar 802.11.
802.11x	Ligado al refuerzo de la seguridad del estándar 802.11b.

1.4.3 MECANISMO DE ACCESO AL MEDIO

El mecanismo de acceso al medio de 802.11 es Acceso Múltiple con Sensado del Medio y Detección de Colisiones (*CSMA/CA, Carrier Sense and Multiple Access / Collision Avoidance*) el cual tiene cuidado de no trasmitir información a menos que tenga la atención de los receptores y que nadie más este transmitiendo, esto es conocido como escuchar antes de hablar (*listen before talk*, LBT). Antes de que un paquete de información sea trasmitido, el dispositivo inalámbrico primero va a escuchar si algún otro dispositivo está transmitiendo, si es así, el dispositivo va a esperar un periodo de tiempo aleatorio y después de haber pasado este lapso de tiempo volverá a escuchar en el medio. En el momento en que nadie este ocupando el medio empezará a transmitir mientras que los otros dispositivos están esperando un lapso de tiempo aleatorio.

Para minimizar el riesgo de que dos dispositivos utilicen el medio al mismo tiempo para trasmitir (lo que causaría una colisión) se emplea el mecanismo llamado *Request To Send/Clear To Send* (RTS/CTS).

Funciona de la siguiente manera cuando un dispositivo intenta comunicarse con otro lo hace por medio del punto de acceso, el cual recibirá la información que tiene como destino otro dispositivo inalámbrico, entonces el punto de acceso le envía al equipo destino un paquete del tipo RTS que le pide un intervalo de tiempo para entregarle la información, por que el nodo destino responde con un paquete CTS el cual le dice que va a estar esperando únicamente la información del punto de acceso. Mientras esta comunicación se está llevando a cabo los demás equipos van a estar escuchando esta conversación y no harán ninguna transmisión por el momento, de esta manera se minimiza el riesgo de colisiones en el medio.

Sin embargo los riegos que se corren en pérdidas de información en un medio inalámbrico podrían darse debido a las interferencias; para asegurarse que las comunicaciones no se pierdan se introdujo el concepto de *acknowledgment* (ACK), que significa que cuando un equipo fue destino de paquetes de información envía una notificación al emisor que ha recibido los paquetes con éxito (ACK), por lo que mientras el emisor no reciba esta notificación se dará por hecho que no llegó la información y procederá a reenviarla de nuevo. Cabe hacer notar que mientras no se reciba la confirmación del receptor de que ha recibido la información, el emisor estará ocupando el medio de transmisión lo que permite recuperarse de cualquier interferencia sin que el usuario final se preocupe de que si ocurrió algún error en la comunicación.

1.4.4 TOPOLOGÍAS DE REDES INALÁMBRICAS

Las redes 802.11 toman como fundamento la idea de un conjunto de dispositivos lógicos agrupados que a través del medio de propagación son capaces de transmitirse información. Llamado Conjunto de Servicio Básico (*BSS, Basic Service Set*) es como se conoce a este conjunto de dispositivos que tendrán un área definida para intercambiar información, el espacio que comprenderá para poder interactuar dependerá de cómo se propague la información en el medio físico de transmisión.

Una estación receptora podrá estar recibiendo diferentes señales dentro del área de servicio emitidas por dispositivos que están al alcance del su radio de cobertura. Los transmisores de la información podrán identificar hacia qué área de servicio dirigirán su transmisión mediante un identificador del conjunto de servicio (*SSID, Service Set Identifier*). De esta forma las estaciones receptoras podrán filtrar las señales por medio del SSID, por lo que sólo se estará escuchando las señales que provengan del área de servicio a la cual pertenezcan. Las tres topologías que se pueden desarrollar con el protocolo 802.11 son:

1.4.4.1 REDES INDEPENDIENTES (*IBSS, Independent Basic Service Sets*)

Una red independiente (IBSS) consiste en un grupo de dispositivos 802.11 comunicándose directamente una con otra, estando todas ellas en un área de alcance de la señal. Este tipo de redes inalámbricas son conocidas como redes Ad-Hoc ya que la simplicidad de la topología hace que básicamente sea una red punto a punto, por lo que la red independiente más pequeña está formada por sólo dos dispositivos.

Una red Ad-Hoc se crea cuando se necesita tener la capacidad de comunicarse con otros equipos con el objetivo de compartir información sin hacer uso de un punto de acceso AP (*Access Point*), usualmente estas redes son creadas para uso temporal con algún fin especifico por un periodo corto de tiempo, como por ejemplo para una sala de videoconferencia, y la mayoría de los casos no necesitan de una planeación para la implementación.

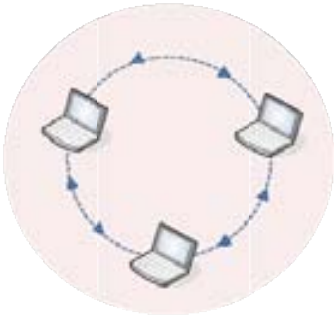


FIGURA 1.6 Red Independiente

1.4.4.2 RED DE INFRAESTRUCTURA (*BSS, Basic Service Sets*)

Las redes de tipo infraestructura tienen como característica la utilización de un punto de acceso AP necesario para la comunicación entre los nodos pertenecientes a la red. El punto de acceso proporcionará servicios y un determinado rango de cobertura dependiendo del fabricante, siendo este el punto central de comunicación para todos los equipos. Por medio del punto de acceso los dispositivos pertenecientes a esa red podrán comunicarse teniendo que pasar por el punto de acceso, la comunicación puede ser hacia equipos que se encuentren dentro del rango de cobertura del AP o a equipos que se encuentren en otra localidad más lejana haciendo uso del sistema de distribución de la red para llegar al destino de la información.

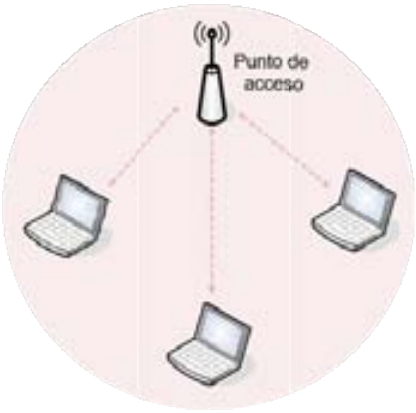


FIGURA 1.7 Red Infraestructura

1.4.4.3 ÁREAS DE SERVICIO EXTENDIDAS (*ESS, Extended Service Sets*)

Para crear redes inalámbricas con una mayor extensión se usan varias redes del tipo infraestructura para ampliar el área de cobertura utilizando un sistema de distribución que las conecte; destacando que este sistema de distribución puede ser mediante un medio físico cableado o inalámbrico.

En este tipo de topología de red inalámbrica se debe asegurar que la cobertura en el área extendida exista señal de algún punto de acceso perteneciente a la red, es decir que el solapamiento de los rangos de cobertura pertenecientes a los puntos de acceso que la conforman cubran con precisión cada resquicio del área, para que así las estaciones móviles puedan comunicarse aun cambiando de área básica de servicio a otra.

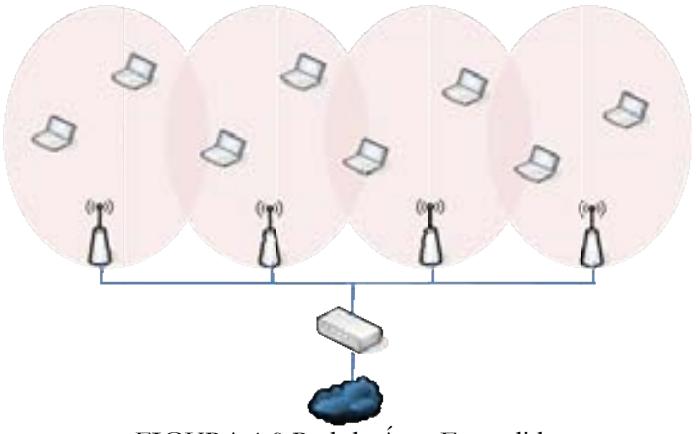


FIGURA 1.8 Red de Área Extendida

1.4.5 COMPONENTES DE UNA RED INALÁMBRICA

1.4.5.1 PUNTOS DE ACCESO (*AP, Access Point*)

Los paquetes de información en las redes 802.11 necesitan ser convertidos a otro tipo de paquetes para poder ser entregados a Internet, los dispositivos encargados de esta tarea de transformación de la información de la red inalámbrica a información que se transmite por redes cableadas son los Puntos de Acceso (AP's), no sólo realizan esta función, sin embargo es la que se considera la más importante.

Un punto de acceso puede gestionar diferentes tipos de datos mediante operaciones como "puentear" (Conectar redes - Puente), retransmitir (Repetidor), distribuir (Concentrador), direccionar paquetes de información (*switching* o ruteo) o para adaptar los formatos de los paquetes de información para otras redes (*Gateway*). Una característica más es que por ejemplo un conjunto de puntos de acceso pueden dar la función de *roaming*, en donde los usuarios se conecten al punto de acceso más cercano para hacer uso de la red, y si el usuario se mueve a otra área de cobertura donde esté al alcance de otro punto de acceso, el dispositivo automáticamente se conecta al nuevo punto de acceso sin perder la comunicación.

Un punto de acceso puede soportar dos tipos de topología, la de punto-punto y la de punto-multipunto. En un sistema donde se tiene una configuración del punto de acceso como punto-punto son permitidas las comunicaciones entre puntos de acceso a puntos de acceso o a una computadora directamente. En la otra disposición, los puntos de acceso son capaces de comunicarse con más de un cliente ya sea usuario u otro punto de acceso.

FIGURA 1.9 Puntos de Acceso

1.4.5.2 TARJETAS DE RED (*NIC, Network Interface Card*)

Las tarjeta de red (NIC's) proveen la comunicación entre la computadora y la red inalámbrica. Las tarjetas de red se encuentran dentro de los dispositivos de los clientes, sin embargo existen adaptadores para

poner tarjetas de red externas. El estándar 802.11 define como deben operar estas tarjetas de red, por ejemplo una tarjeta de red inalámbrica puede tener soporte para el protocolo IEEE 802.11b, en donde sólo funcionará para redes que tengan implementado ese protocolo.

Una tarjeta de red es un transductor (envió y recepción) que convierte las señales de radiofrecuencia a señales digitales que pueden ser procesadas por las computadoras. Por medio de estas tarjetas de red inalámbricas los dispositivos acceden al punto de acceso que recibe y envía paquetes de información hacia otros dispositivos o hacia otras redes.

Las tarjetas de red que son conectadas a los dispositivos como laptops o PDAs requieren del software necesario para controlar el dispositivo y para comunicarlas con el sistema operativo. Parte de la configuración del software que controla la tarjeta de red, puede implicar realizar configuraciones como fijar el SSID de la red, la clave de cifrado WEP, o el canal que ocupará.

Figura 1.10 Tarjetas de Red

1.4.5.2 ANTENAS

Uno de los elementos más importantes de las redes inalámbricas son las antenas, ya que se encargan de hacer la transformación de las señales electromagnéticas en señales eléctricas y viceversa. Existen de dos tipos, las antenas direccionales y las omnidireccionales, las direccionales son capaces de recibir y emitir señales sobre un volumen específico del espacio, por lo contrario las antenas omnidireccionales reciben y envían señales desde cualquier dirección del espacio en donde se encuentra.

Los diferentes tipos de antenas tienen diferentes coberturas de área en dirección horizontal y vertical, por ejemplo las antenas omnidireccionales tienen una cobertura horizontal de 360° y de manera vertical de 7° a 80° de cobertura.

Dentro de las antenas omnidireccionales podemos encontrar dos tipos de antenas que tienen patrones de radiación basándose en las omnidireccionales, las antenas multitrayectoria que son como su nombre lo dice, irradian señales en todas direcciones; por otro lado existen las antenas semidireccionales que son las que irradian señales a media trayectoria. Una antena de este tipo puede tener al menos el doble de alcance que una antena de tipo omnidireccional. De manera efectiva una antena semidireccional puede tener un aumento de 10 veces la amplitud de la señal.

Las antenas direccionales tienen una cobertura muy estrecha pero con un alcance de cobertura muy largo. Para alcanzar este grado de direccionalidad, se necesita usar antenas de plato que enfocan la emisión de las ondas de radio mayoritariamente en una sola dirección, este tipo de antenas son caras comparadas con las antenas omnidireccionales.

Figura 1.11 Antenas

1.5 SEGURIDAD EN REDES INALÁMBRICAS

Las redes inalámbricas en particular las redes 802.11 han ganado mucha popularidad en un breve lapso de tiempo. Sin embargo, esta popularidad se ha visto afectada por temas de seguridad.

En la comunicación inalámbrica, el emisor emite una señal diciendo que quiere comenzar comunicación con otros dispositivos móviles de manera inalámbrica envía los datos a manera de ***broadcast*** esperando que el receptor se encuentre dentro del mismo radio cobertura de la señal y la reciba, la desventaja en este procedimiento es clara, cualquier dispositivo móvil que se encuentre dentro de esta área de cobertura recibirá la señal de datos.

Sin un mecanismo de seguridad cualquier estación con el protocolo 802.11 puede procesar la información que ha sido enviada a una red inalámbrica dentro de su área de cobertura. Para proveer de un nivel mínimo de seguridad en una red inalámbrica es necesario tomar en cuenta dos aspectos muy importantes:

Decidir quién y cómo puede usa la red inalámbrica: este aspecto lo cubren los mecanismos de autenticación para el control de acceso de una red inalámbrica.

Proveer privacidad de los datos que se transmiten en una red inalámbrica: este otro aspecto lo cubren los algoritmos de cifrado implementados para la red inalámbrica.

Autenticación y cifrado de datos son aspectos que hacen de una red inalámbrica una red segura, por si sólos estos mecanismos no proveen seguridad.

El estándar 802.11 en sus especificaciones define un proceso de autenticación de llaves abierto y compartido, además del método de cifrado WEP (*Wireless Encryption Process*) para proveer a los dispositivos métodos de autenticación y cifrado respectivamente. Los mecanismos de cifrado están basados en algoritmos que dan a los datos una apariencia aleatoria. Existen dos tipos de cifrado de datos: Cifrado de Flujos y Cifrado de Bloques. Ambos tipos operan generando una llave de flujo a partir de un valor de una llave secreta. La llave de flujo es mezclada con los datos para que el proceso de cifrado proporcione una salida cifrada o texto cifrado. Estos dos tipos de cifrado son diferentes en cuanto a tamaño de los datos que pueden ser procesados.

Un flujo de cifrado genera una llave de flujo continua a partir del valor de la llave. Los flujos de cifrado son algoritmos pequeños y eficientes por lo que no consumen muchos recursos de la unidad de procesamiento. Un algoritmo comúnmente usado para cifrar datos es el RC4 (*Rivest Cipher 4*) el cual es la base para el algoritmo de seguridad de redes inalámbricas WEP.

Por el otro lado un bloque de cifrado genera una llave de flujo cifrada de un tamaño fijo. El texto plano es fragmentado en bloques y cada uno de ellos es mezclado con el valor de la llave de flujo de manera

independiente. Si el bloque de texto plano es menor al tamaño que el tamaño del bloque de la llave de flujo, se le añade relleno al bloque de texto plano para hacerlo del tamaño apropiado, este tipo de cifrado consume más recursos del CPU (Unidad Central de Procesamiento) que el cifrado de flujos.

El proceso de cifrado es conocido como modo de cifrado *Electronic Code Book* (ECB), el cual tiene la característica que el mismo texto plano cifrado siempre genera la misma salida cifrada, lo cual lo vuelve inseguro porque espías pueden ver los patrones en el texto cifrado y empezar a hacer combinaciones para encontrar el texto original. Algunas técnicas de cifrado pueden solventar este problema: Vectores de Inicialización (*IV, Initiation Vectors*) y la técnica de Modos de *Feedback*.

Los vectores de inicialización es un bloque de bits que se concatena a la llave antes de que el flujo llave sea generado, cada vez que el IV cambia lo hace el flujo llave.

Los modos de *Feedback* son modificaciones al proceso de cifrado para evitar que durante el proceso de cifrado se generen las mismas salidas de un texto plano, son usados generalmente en el cifrado de bloques.

1.5.1 MECANISMOS DE AUTENTICACIÓN

Las especificaciones del estándar 802.11 proporcionan dos mecanismos de autenticación para los clientes de una red inalámbrica. El primero de ellos es autenticación abierta en donde los puntos de acceso aceptan cualquier petición de autenticación, esto permite un rápido acceso a la red, ya que su algoritmo es nulo.

A diferencia del modo abierto, en el mecanismo de autenticación de llave compartida se requiere que el punto de acceso y los clientes tengan habilitado el protocolo WEP y que sus llaves coincidan, este es un proceso que se describe a continuación:

1. El cliente envía una petición de autenticación para autenticar las llaves compartidas al punto de acceso.
2. El punto de acceso responde con un paquete en texto claro de desafío.
3. El cliente cifra el desafío y lo envía de regreso al punto de acceso.
4. Si el punto de acceso puede descifrar correctamente el paquete y recibe el desafío original, se le envía un mensaje de éxito.
5. El cliente puede acceder a la red.

1.5.1.1 AUTENTICACIÓN POR DIRECCIÓN MAC

La autenticación por medio de dirección física de los dispositivos no está contemplada dentro del protocolo 802.11, sin embargo muchos de los fabricantes de los puntos de acceso manejan esta forma de filtrar a los usuarios utilizando listas de control de acceso (*ACL, Access Control List*). En este tipo de autenticación se verifica las direcciones físicas MAC contra las listas de control de acceso configuradas en el punto de acceso o algún servidor de autenticación externo. Esta forma de autenticar usuarios se basa en el uso de llaves abiertas y compartidas, reduce de manera significativa los dispositivos no autorizados para acceder a la red. Por ejemplo se pueden emplear filtros en los puntos de acceso de dos formas, la primera seria dejar pasar todo el tráfico de las direcciones MAC configuradas o la otra seria no dejar pasar el tráfico de las direcciones físicas MAC configuradas.

1.5.2 PROTOCOLOS DE SEGURIDAD

1.5.2.1 WEP (*Wired Equivalent Privacy*)

Las especificaciones del protocolo 802.11 provee privacidad a los datos mediante el método de cifrado WEP, el cual se basa en el algoritmo de cifrado simétrico RC4; esta simetría requiere una relación en las llaves WEP, ya sean de 40 ó 104 bits en longitud, que deben de ser configuradas en los clientes de manera estática, así como en los puntos de acceso.

Se pueden definir hasta cuatro llaves en un dispositivo pero sólo se puede usar una para realizar el proceso de cifrado de la información. El cifrado WEP es usado sólo con paquetes de datos y durante la autenticación de llaves compartidas, WEP cifra los campos de los datos o (*payload*) y el campo del valor del chequeo de integridad (*ICV, Integrity Check Value*) de la trama 802.11, todos los demás campos son transmitidos sin cifrar, el vector de inicialización debe de enviarse sin cifrar para que la estación que reciba la trama pueda usarlo y descifrar los campos que han sido cifrados.

Usa un vector de inicialización IV de 24 bits (uno diferente para cada paquete de información) el cual se concatena a la llave para después ser procesados por el algoritmo de cifrado RC4, con este valor se inicia una secuencia pseudoaleatoria para cifrar los paquetes de información.

Las especificaciones del protocolo 802.11 proveen para valores de 32 bits que funcionan como chequeo de integridad para las tramas, este chequeo le dice al receptor que el paquete de información ha llegado sin haber sido corrompido durante la transmisión. El ICV es calculado para todos los campos usando el Chequeo Cíclico de Redundancia (CRC)-32.

El emisor calcula los valores y coloca los resultados en el campo ICV, este campo es incluido en el proceso de cifrado WEP. Cuando el receptor descifra el paquete calcula el ICV y lo compara con el valor que viene en el paquete en el campo del ICV, si estos coinciden el paquete es considerado como genuino e íntegro, de lo contrario el paquete es rechazado.

El algoritmo aplica una XOR entre el paquete a cifrar (con el ICV) y la secuencia pseudolaeatoria y finalmente se manda el paquete cifrado. La operación XOR es una operación bit a bit de suma en base 2, no se puede (en teoría) encontrar la secuencia inicial si no se sabe cuál es la secuencia usada con la XOR.

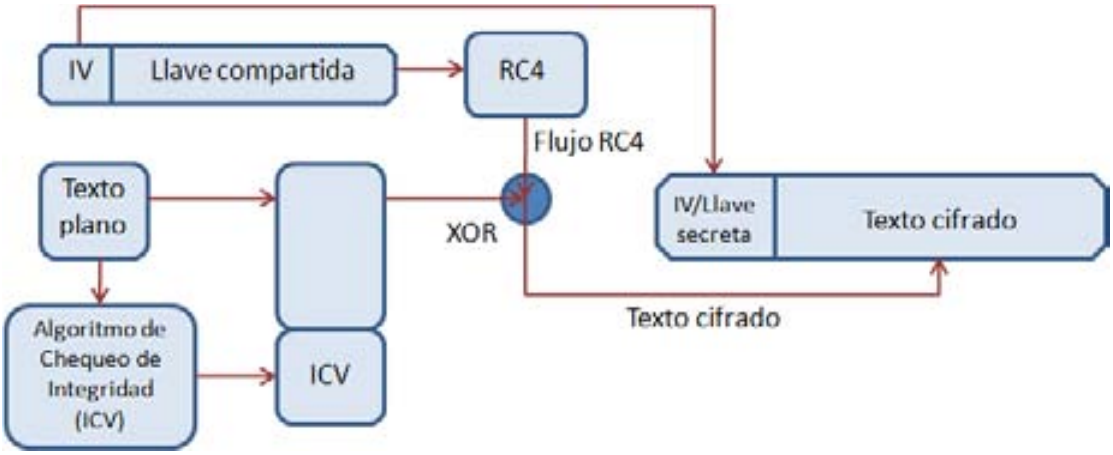


FIGURA 1.12 Cifrado WEP

Ejemplo: 1 XOR 1 =0 ; 1 XOR 0= 1 ; 0 XOR 1=1 ; 0 XOR 0=0;
Si: A=110110 B=011101 la operación XOR tiene la siguiente característica:

A XOR B = 101011 = C C XOR A = 011101 = B C XOR B = 110110 = A

Del ejemplo anterior se observa que para descifrar sólo es necesario obtener la secuencia pseudoaleatoria (IV + llave secreta) y se podrá recuperar el paquete original a través de un XOR entre el paquete cifrado y la secuencia. Entonces una vez que se ha obtenido la clave WEP es posible alterar los datos de algún paquete cifrado y obtener el mensaje original utilizando el mismo algoritmo, de la misma manera el atacante con la clave WEP puede enviar paquetes de información alterados por el mismo con lo que la integridad de los datos se pierde. Por la misma razón de la clave WEP comprometida, es necesario cambiar la clave WEP de la red inalámbrica de manera manual en cada dispositivo configurado.

1.5.2.2 WPA (*Wi-Fi Protected Access*)

Wi-Fi Alliance es una asociación de la industria conformada por más de 200 compañías incluyendo fabricantes de equipos 802.11, fabricantes de chips, compañías de software y muchas otras, su función es promover 802.11 y certificar la interoperabilidad de los productos. Desarrollaron el protocolo *Wi-Fi Protected Access* (WPA) como alternativa a las vulnerabilidades de seguridad presentadas por el protocolo WEP que especifica el 802.11, mientras tanto se desarrollaba 802.11i protocolo de seguridad inalámbrica (WPA2). Para la mayoría de los productos 802.11 que funcionaban con WEP sólo basta con una actualización del firmware para utilizar WPA.

Las especificaciones de WPA es en esencia un subconjunto de especificaciones de 802.11i, que en primer lugar implementa TKIP (*Temporal Key Integrity Protocol*) cada paquete está cifrado por una llave única y basada en sesión (significa llaves diferentes por todos los usuarios y por paquete), autenticación 802.1x y manejo de claves. WPA también incluye el requerimiento para usar autenticación de clave abierta y clave inicial compartida (*Shared-Key authentication*), se puede utilizar 802.1x o claves iníciales compartidas que pueden ser configuradas usando 64 caracteres hexadecimales o una cadena ASCII obtenida de algún algoritmo. Como 802.11i, WPA tiene las capacidades de hacer pruebas de respuesta, peticiones de asociación y peticiones de reasociación.

Como ya se mencionó anteriormente WPA usa TKIP un procedimiento de cifrado más robusto que el esquema que se usaba en WEP, usa una longitud de clave de 48 bits, además de que implementa el uso de *key hashing* conocido como (*KeyMix*) y utiliza el algoritmo no lineal de Chequeo de Integridad del mensaje (*MIC, Message Integrity Check*) generando un bloque de 4 bytes a partir de la dirección MAC de origen, de destino y los datos, añadiendo el MIC calculado a la unidad de datos a enviar. Posteriormente los datos (que incluyen el MIC) se fragmentan y se les asigna un número de secuencia. La mezcla del número de secuencia con la clave temporal genera la clave que se utilizará en el cifrado de cada fragmento.

WPA puede trabajar en dos formas diferentes dependiendo del tipo de red. En redes pequeñas (casa, oficina, etcétera) puede utilizar el uso de claves iníciales compartidas (*PSK, Pre Shared Key*) configuradas en las estaciones y en el punto de acceso, la cual sólo se utiliza para tener acceso a la red, no cifra los datos. En el otro modo de operación, normalmente para redes de mayor tamaño (empresas, universidades, etcétera) se utilizan servidores que realicen autenticación, autorización y contabilidad (*AAA, Authentication Authorization Acounting*) como por ejemplo un servidor RADIUS; además se requiere soporte para 802.1x y EAP que darán la posibilidad de que un usuario de la red haga la negociación vía punto de acceso con el servidor usando canales cifrados para las transmisiones de intercambio de las llaves que harán posible el inicio de sesión.

Una red puede mezclar WPA con el estándar WEP sin embargo el nivel de seguridad de esta red podrá ser comprometido con las vulnerabilidades de WEP, pero WPA no es compatible con WPA2 porque las especificaciones para usar 802.1x son diferentes.

1.5.2.3 WPA2 (802.11i)

Wi-Fi Protected Access 2 está basado en el estándar de seguridad de 802.11 y está especificado en el estándar IEEE 802.11i. WPA2 incluye el algoritmo de cifrado AES (*Advanced Encryption Standar*) desarrollado por *National Institute of Standards and Technologies* (NIST), es un algoritmo de cifrado de bloque con claves de 128 bits, mucho más seguro que el algoritmo utilizado por WEP, que usaba algoritmo RC4.

WPA2 es totalmente compatible con WPA pero requiere de hardware potente para realizar las operaciones de sus algoritmos, por lo que se requiere nuevo hardware para dispositivos que no tuvieran esa capacidad de procesamiento.

Para asegurar la integridad de los datos y la autenticidad de los mensajes utiliza el Protocolo de Código de Autenticación de Mensajes en Cadena para el Bloque de Cifrado (*CCMP, Counter Mode / Cipher Block Chaining / Message Authentication Code Protocol*).

Puede funcionar al igual de WPA de las 2 formas mencionadas anteriormente, para redes pequeñas con claves iníciales compartidas y para redes grandes con la utilización de servidores AAA. El estándar IEEE 802.11i define una red con seguridad robusta (*RSN, Robust Security Network*) en donde los dispositivos clientes y puntos de acceso deben de cumplir con habilidades especificas para brindar esta seguridad requerida. IEEE 802.11i brinda los siguientes servicios: asociación y reasociación, control de acceso, autenticación y re-autenticación, confidencialidad, administración de claves y autenticidad del origen de los datos.

TABLA 1.3 Comparación WEP-WPA-WPA2

	WEP	**WPA**	**WPA2**
Algoritmo de cifrado	RC4	RC4 con TKIP	AES con CCMP
Longitud de la llave	Cifrado: 40 ó 140 bits	Cifrado: 128 bits Autenticación (integridad del mensaje): 64 bits	Cifrado y Autenticación (integridad del mensaje): 128 bits
Llave por paquete	Concatena el IV y la clave secreta	Mezclado por paquetes	No necesita
Llaves únicas	Llave secreta por red. IV cambia por paquete	Llave por sesión, paquete y usuario	Llave por sesión, paquete y usuario
Integridad de Datos	CRC-32	MIC	CCM
Integridad de cabeceras		MIC	CCM
Contador se secuencia		IV	IV
Gestión de las llaves		IEEE 802.1x EAP	IEEE 802.1x EAP
Pre-autenticación			Si
Mecanismo de autenticación	Sistema abierto y llaves compartidas	Sistema abierto y capas superiores	Sistema abierto y capas superiores

1.5.2.4 802.1X

Mecanismo de control de acceso para las redes inalámbricas, que da acceso al usuario para poder ser autenticado con una autoridad central, el control de acceso basado en puertos fue diseñado en una capa superior de mecanismos de autenticación a la capa 2. Básicamente 802.1X tiene tres entidades:

- Solicitante: el dispositivo que desea unirse a la red, en este caso los dispositivos 802.11.
- Autenticador: el dispositivo que controla el acceso, en el caso de las redes inalámbricas 802.11 puede ser el punto de acceso o un router inalámbrico.

- Servidor de Autenticación: Es el encargado de la decisión de la autenticación, puede ser por ejemplo un servidor Radius.

El punto donde el Solicitante se conecta a la red vía el autenticador es llamado la Entidad de Puerto de Acceso (*PAE, Port Access Entity*). Existen básicamente dos puertos controlados por el autenticador, cuando el suplicante se conecta se va a través del puerto del autenticador hacia el servidor de autenticación, una vez que la autenticación es exitosa para el solicitante el puerto de servicio se habilita para el suplicante. Ahora el solicitante puede acceder a los servicios a través del autenticador.

1.5.2.4.1 EAP (*Extensible Access Protocol*)

El protocolo que puede ser usado para esta comunicación es el Protocolo de Autenticación Extensible EAP, se ha convertido en una parte muy importante de las redes inalámbricas, ya que es ocupado para transportar la información de identificación del usuario. EAP pude ser usado sobre la capa 2, sobre la capa de IP o cualquier capa superior, fue diseñado como una extensión de protocolo punto-punto (*PPP, Point to Point Protocol*).

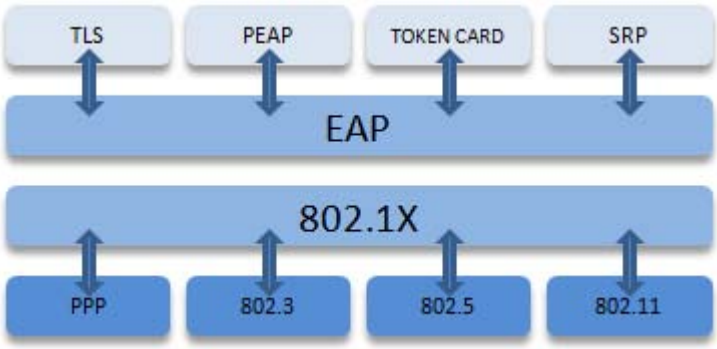


Figura 1.13 802.1X / EAP

EAP no provee autenticación, es sólo como un encapsulado que da flexibilidad en el uso de cualquier tipo de protocolo de autenticación, pero las variantes que existen de EAP dictan como los clientes son autenticados. De esta forma un punto de acceso no necesita saber todos los tipos de autenticación. Algunos métodos de autenticación que soporta son: *Token Cards*, Kerberos, Autenticación por llave pública, Certificados, *Smart Cards*. El proceso que sigue EAP es el siguiente:

1. El cliente se asocia con el punto de acceso.
2. El punto de acceso bloquea a los clientes en el momento que intentan acceder a la red.
3. El cliente provee su información de usuario y contraseña.
4. Un servidor remoto de autenticación AAA y el cliente se autentican.
5. El servidor AAA y el cliente coinciden con la clave de acceso.
6. La autenticación se completa.

1.5.2.4.2 EAP-TLS

EAP con capa de trasporte seguro (*TLS, Transport Layer Security*) requiere que ambas estaciones y el servidor RADIUS se autentiquen así mismos usando criptografía de llave pública, como *smart cards* o certificados digitales.

Esta conversación entre los dispositivos es asegurada con un túnel cifrado TLS, este es la única autenticación cifrada. Después de que este proceso se completó, WEP, WPA o WPA2 proveen a los

usuarios cifrado de sus datos, esto hace que EAP-TLS resista el conocido ataque de *man-in-the-middle* que se describirá en el tema de Inseguridad en capítulo II. A continuación se presenta el proceso de EAP-TLS

1. El cliente se asocia al punto de acceso.
2. El punto de acceso bloquea al cliente para acceder a la red.
3. El cliente autentica el servidor con un certificado.
4. El servidor AAA autentica al cliente con un certificado.
5. El servidor AAA y el cliente coinciden con la clave de acceso.
6. Un túnel seguro es establecido entre el cliente y el servidor.

1.5.2.4.2 PEAP

La falta de privacidad a la hora de enviar la identidad del usuario en EAP-TLS es el primer objetivo que intenta mejorar PEAP. Establece un túnel para trasmitir las credenciales del cliente. Se requiere de dos fases para el funcionamiento de PEAP:

Fase 1. Del lado del servidor empieza la autenticación TLS, y un túnel cifrado se crea. Esto crea un sistema de autenticación del lado del servidor. En esta fase el cliente no envía sus credenciales de acceso, envía alguna información arbitraria con el fin de iniciar una comunicación cifrada. Cuando se completa esta fase todos los datos de autenticación serán cifrados.

Fase 2. .Una vez terminada la fase 1 el protocolo inicia automáticamente la siguiente fase en donde se autenticará el usuario mediante comunicación cifrada usando las llaves creadas durante la fase 1. El cliente es autenticado usando ya sea MS-CHAP versión 2 o algún otro esquema de autenticación.

PEAP provee autenticación mutua, protección de la identidad del solicitante y generación de llaves.

1.5.2.4.2 EAP-FAST

EAP-flexible con autenticación por medio de un túnel seguro es un protocolo relativamente nuevo, pretende evitar el uso de certificados. El establecimiento del túnel de EAP-FAST se basa en acceso protegido de credenciales (*PAC, Protected Access Credential*) que pueden ser administradas dinámicamente por EAP-FAST a través de un servidor AAA. También se maneja en dos fases y la opcional fase 0, en donde las credenciales del usuario son generadas de manera segura entre el usuario y la red, esta credencial conocida como PAC es la que se usa en la fase 1.

Fase 1. Establece un túnel entre las estaciones y el servidor AAA. PAC es usado con el propósito de autenticar al usuario.

Fase 2. Una vez establecido el túnel, el usuario envía sus credenciales de acceso como nombre de usuario y contraseña.

EAP-FAST es el único protocolo que está diseñado para acelerar la re-autenticación entre estaciones cliente y el punto de acceso, a diferencia de EAP-TLS y PEAP que tardan un mayor tiempo en el intercambio de mensajes entre las estaciones y el servidor AAA; para aplicaciones que requieren que este proceso sea más rápido es ideal.

Usa claves secretas compartidas para acelerar el proceso de re-autenticación, en donde el uso de claves públicas es conveniente ya que el punto de acceso y los clientes pueden autenticarse mutuamente sin tener que conocer a otros dispositivos, esto requiere que las claves secretas compartidas ya estén en los dispositivos. EAP-FAST provee protección contra ataques al vector de inicialización, ataques de diccionario, ataques de *man-in-the-middle*.

1.5.2.4.2 VPN (*Virtual Private Network*)

Una VPN (*Virtual Private Network*) conecta componentes y recursos de una red sobre otra red a través de un túnel sobre redes públicas o Internet, permitiendo así al usuario la misma seguridad y características que se tienen en las redes privadas. Las VPN´s permiten a empresas y usuarios remotos conexiones de forma segura a algún servidor de la empresa en otra red lejana usando enrutamiento proveído por una red pública. Para los usuarios la perspectiva que tienen es de una conexión punto a punto entre el usuario y el servidor de su empresa.

Las conexiones seguras a través de redes públicas hacen que los usuarios de las VPN´s vean las comunicaciones como en las redes privadas. Algunos de los usos más comunes de las VPN´s son:

- Acceso a usuarios remotos sobre Internet.
- Conexión de redes sobre Internet.
- Conexión de computadoras sobre Internet.

Los requerimientos para una VPN son los siguientes:

Autenticación de usuario: La solución debe de verificar la identidad del usuario y restringir el acceso a usuarios no autorizados, además debe de proveer conteo y auditoría de registros para mostrar quién acceso, a qué información y cuándo.

Administración de direcciones: La solución debe de asignar a los clientes direcciones sobre la red privada, además de asegurarse que estas direcciones se mantengan privadas.

Cifrado de datos: El transporte de datos sobre redes públicas debe de ser incapaz de ser leído por clientes no autorizados sobre la red.

Administración de claves: La solución debe de generar y refrescar las claves de cifrado para los clientes y servidores.

El canal de comunicación que proveen las VPN´s podrá asegurar conexiones para usuarios de una red inalámbrica. Hoy en día las VPN´s son muy utilizadas en las corporaciones, no se necesita ningún hardware especial, el software de VPN´s es suficiente. El protocolo más utilizado para las VPN es IPSEC aunque existen otros como PPTP, L2TP, SSL/TLS, SSH, entre otros.

1.6 GESTIÓN DE RECURSOS INFORMÁTICOS (ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN)

En la actualidad los aspectos relacionados con la administración y gestión de los recursos informáticos han tenido gran auge debido a que las organizaciones (públicas o privadas) se han preocupado por obtener los resultados esperados, reducir costos y satisfacer sus necesidades con base en las inversiones en materia de tecnología, ya que de nada sirve tener una base tecnológica ampliamente desarrollada si no es organizada eficientemente y encausada en alcanzar los objetivos de las organizaciones.

Cualquier tecnología capas de ayudar a producir, manipular, almacenar comunicar y/o esparcir la información son conocidas como Tecnologías de información (TI). Las TI son herramientas aplicadas con creatividad a los procesos estratégicos, como por ejemplo tareas como administración de datos, redes, ingeniería de hardware, diseño de programas y bases de datos, así como la administración y dirección de

los sistemas completos; le dan a las organizaciones capacidades de respuesta frente al cada vez mas competido mundo global.
Pero para que las aplicaciones de las TI hagan los procesos para los que fueron diseñados de una manera eficiente, es necesario hacerlo usando principios, estrategias, métodos y procedimientos administrativos que integren los recursos humanos, tecnológicos y materiales. La Gestión de Tecnologías de información viene a ser la disciplina que le da sentido y rumbo a la tecnología en las organizaciones, con un enfoque que la integra a los recursos humanos y materiales, para hacerla productiva e innovadora.

La administración de TI contempla el manejo efectivo de los recursos tecnológicos mediante actividades de dirección de personal y la toma de decisiones tecnológicas que vayan de acuerdo a los objetivos de la organización. La amplia gama de sistemas de información y aplicaciones han propiciado que la administración de estas tecnologías resulte una tarea compleja debido a que cada TI tendrá sus soluciones a problemas técnicos y de gestión de su servicios, hoy en día en una organización se pueden encontrar gran variedad de sistemas en donde cada uno se administra de manera diferente, por lo que es difícil unificar criterios y políticas de administración importantes para conservar la seguridad e integridad de la información.

Sin embargo mantener los servicios proporcionados por las TI como pueden ser acceso a red, correo electrónico, bases de datos, acceso a archivos, etcétera, son necesidades que han llevado a buscar herramientas de administración útiles para resolver y prever problemas, capturar los eventos de los sistemas, facilitar parámetros de rendimiento, analizar el desempeño de nuestros sistemas y dispositivos, administrar usuarios, definir accesos a recursos y servicios, y muchas tareas más mediante un sólo punto de administración.

Algunas tareas que se incluyen dentro de un esquema de gestión de tecnologías de información podemos tener:

- Organizar y efectuar la planeación tecnológica en las organizaciones, acorde a la misión y los planes estratégicos de la organización y adquisición de soluciones tecnológicas.
- Definición de políticas y procedimientos a realizar con base tecnológica.
- Definición de planes de contingencia.
- Respaldo y recuperación de información.
- Análisis de rendimiento.
- Afinación de procesos.
- Generación, distribución y almacenamiento de información.
- Monitoreo de sistemas y aplicaciones.
- Aseguramiento de sus recursos de cómputo.
- Soluciones integrales de seguridad.
- Asimilar, adaptar y optimizar tecnología con técnicas como Administración Total de la Calidad, Tecnologías de información, Reingeniería, etcétera.

Hoy en día existen modelos para ayudar con la administración de tecnologías de información, uno de ellos es el modelo COBIT que significa Objetivos de Control para Tecnología de Información y Tecnologías Relacionadas (Control Objetives for Information Systems and Related Technology) fue creado como resultado de la investigación de expertos de varios países, desarrollado por ISACA (Information Systems Audit and Control Association) en 1996.

COBIT es un modelo para auditar la gestión y control de los sistemas de información y tecnología, se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales y las redes. Está basado en la filosofía de que los recursos TI necesitan ser administrados por un conjunto de

procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

El conjunto de lineamientos y estándares internacionales conocidos como COBIT, define un marco de referencia que clasifica los procesos de las unidades de tecnología de información de las organizaciones en cuatro "dominios" principales, a saber:

- Planificación y organización. Estrategia y tácticas, identificación de la forma en que las TI's contribuyen al logro de los objetivos de la organización.
- Adquisición e implantación. Las soluciones de TI's deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso de la organización cubre los cambios y el mantenimiento realizados a sistemas existentes.
- Soporte y Servicios. Entrega de los servicios requeridos, con el fin de proveer servicios se deberán establecer los procesos de soporte necesarios.
- Monitoreo. Evaluación de los procesos para verificar calidad y suficiencia.

Estos dominios agrupan objetivos de control de alto nivel, que cubren tanto los aspectos de información, como de la tecnología que la respalda. Estos dominios y objetivos de control facilitan que la generación y procesamiento de la información cumplan con las características de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Otro modelo es el de Biblioteca de Infraestructura de Tecnologías de la Información (*Information Technology Infraestructure Library*, ITIL) surgió durante los años 80´s en el Reino Unido como un modelo orientado a la gestión de las operaciones y servicios de los sistemas y tecnologías de la información y comunicación.

Está específicamente desarrollado para los servicios de mantenimiento y operación de TI, y proporciona objetivos de servicio además de actividades e indicadores clave de servicio. Nos presenta un modelo muy completo el cuál documenta las técnicas, herramientas y considera el factor tecnología como algo a valorar dentro de sus esquemas, además de detallar el conjunto mínimo de roles necesarios para el desarrollo con garantías de los procesos.

Entre las características más importantes de ITIL están: que es un marco de procesos IT no propietario, es independiente de la tecnología y que está basado en los resultados de las mejores prácticas. Provee de una terminología estándar, independencia entre los procesos, lineamientos para su implementación, lineamientos para la definición de roles y responsabilidades de los procesos, lista de chequeo de madurez, que hacer y qué no hacer, entre otras actividades.

CAPÍTULO

2

PROBLEMÁTICA ACTUAL EN LA FACULTAD DE INGENIERÍA

Una vez que se conocen los conceptos básicos es tiempo de entender cuál es la situación actual de la Facultad de Ingeniería con respecto a las redes inalámbricas, en el desarrollo de este capítulo se establecerá un panorama de la problemática que se vislumbra hacia el uso de estas tecnologías así como una estrategia de solución dirigida hacia una mejor gestión de estos recursos.

2. 1 ANTECEDENTES

Las redes inalámbricas ofrecen muchos beneficios que las han hecho populares hoy en día; la comodidad de acceso, la reducción del cableado en los edificios y el potencial aumento de la productividad son los principales impulsores de esta tecnología que hacen que las personas encargadas de tomar las decisiones relacionadas a las tecnologías de información se decidan por implantar redes inalámbricas, sin embargo es importante estudiar las expectativas que han creado este tipo de tecnologías, junto con los problemas asociados a su uso.

En la actualidad se ha hecho evidente que la venta de los dispositivos móviles está aumentando de manera considerable y que el precio del hardware necesario para instalar una red inalámbrica va disminuyendo año con año. Aunado a esta situación se le suma el impulso que traen las empresas fabricantes de los dispositivos por crear tecnología que esté al alcance de un mercado económico en donde les permitan vender más equipos. Aun así habrá que resolver los problemas de instalación y configuración que un usuario normal pueda tener.

En la Facultad de Ingeniería de la UNAM se cuenta con la capacidad tecnológica y operativa para la utilización de redes inalámbricas como recurso de aprendizaje e investigación así como complemento de servicio para varias actividades. Sin embargo como parte de la base tecnológica de la Facultad deberá considerarse una planeación estratégica que permita propiciar el desarrollo de la institución con el aprovechamiento de las redes inalámbricas.

La administración efectiva de los recursos de las Tecnologías de Información en la Facultad de Ingeniería resulta importante para el cumplimiento de las labores de servicio, académicas y de investigación. Por lo referente a las redes inalámbricas existentes en la Facultad es necesario hacer un análisis de cómo se están utilizando estos recursos. Hoy en día existen un gran número de redes inalámbricas de las cuales no se tiene mucha información y por este motivo no se puede asegurar si estén funcionando de acuerdo a los objetivos por los cuales fueron creadas.

La omisión de administración de redes inalámbricas puede llegar a ser punto de partida para el posible mal uso de estos recursos, por lo que llevar el control de las redes inalámbricas requiere de una fuerte cooperación y coordinación entre las distintas entidades y áreas que tienen a cargo la administración de estos.

Los servicios tecnológicos que ofrece la Facultad de Ingeniería como parte de su infraestructura de Tecnologías de Información no deben de ser descuidados de ninguna forma; a medida que las redes inalámbricas van creciendo en la institución, se deberá ir teniendo un control sobre ellas para asegurar que su utilización este justificada, además de asignar responsabilidades sobre los servicios inalámbricos así como la administración de la red.

En la situación en la que se encuentra la Facultad de Ingeniería, las consecuencias que podría causar la omisión del control de las redes inalámbricas pueden verse reflejadas en problemas de seguridad en cómputo de diversas índoles, que pueden llegar a ser tan graves como filtraciones de información privada, alteración en el funcionamiento de la red a tal grado de dejar de funcionar por lapsos de tiempo, hasta pérdida de sistemas completos. En contraparte, tener la información de quién administra los puntos de acceso, qué configuraciones de seguridad tiene, en dónde se localizan físicamente, entre otros, son datos que podrían llegar a ser de utilidad en casos de emergencia y que ayudarían a una pronta solución de los problemas que pudieran llegar a presentarse.

2.2 PROLIFERACIÓN DE LAS REDES INALÁMBRICAS

La tecnología de las redes inalámbricas como ya se mencionó anteriormente está viviendo un crecimiento en cuanto a popularidad y uso, existen varios factores que son la causa de esta situación:

- El costo de la infraestructura ha ido cada vez disminuyendo (puntos de acceso, tarjetas de red, ruteadores inalámbricos).
- Cuando se implementa una red de este tipo la instalación del cableado estructurado no existe.
- Tienen alcance a lugares en donde no sería posible poner cables de red.
- La movilidad de los usuarios.
- Pueden tener las mismas funcionalidades que una red cableada.
- Son de rápida instalación

Actualmente en la Facultad de Ingeniería podemos darnos cuenta de esta situación con sólo tener una tarjeta de red inalámbrica y dar un paseo por los edificios para detectar su existencia, de las cuales se sabe poco de ellas y mucho menos de quién está a cargo de su administración.

Cualquier persona que cuente con un acceso a la red de la Facultad y que tenga un punto de acceso, puede crear una red inalámbrica sin que el personal encargado de la red tenga conocimiento de ello, y si no se toman las medidas de seguridad necesarias el acceso a la red queda expuesto a personas que no necesariamente tengan derecho a tenerlo en las zonas aledañas a Facultad y dentro de la misma, esto origina múltiples complicaciones tal como el uso inapropiado del ancho de banda, el incumplimiento de

las Políticas de Seguridad en Cómputo y como se mencionó anteriormente el aumento en riesgo de ataques informáticos a la infraestructura de cómputo.

La proliferación de las redes inalámbricas en una misma zona en donde todas ellas están bajo el control de personas o unidades administrativas distintas, invita a problemas de configuración y de inconsistencia en el acceso a la red y que adicionalmente se corre el riesgo de que se pueda producir el colapso del servicio.

Uno de los principales problemas de las redes 802.11 y también una de sus principales ventajas se refiere a la banda de frecuencias que utiliza. Se trata de bandas en las que se está autorizado un uso compartido cumpliendo una serie de requisitos básicos, de entre los que destaca la potencia máxima de emisión. Ese uso más o menos libre permite el establecimiento de redes inalámbricas sin tramitación administrativa alguna, sin embargo tampoco se ofrece ninguna garantía en el sentido de que cualquiera puede ocupar esa frecuencia sin otro requisito que el cumplimiento mínimo que pueda existir referente a la de la normativa básica que se conoce.

De esa forma puede producirse la 'colisión' de diferentes redes inalámbricas en un mismo espacio geográfico y aunque estén definidos varios canales dentro de los rangos de frecuencias de uso común, una expansión masiva de esta clase de redes puede provocar la saturación del medio.

Se deberá atender a la definición, organización y ordenación del espectro de radio de radiofrecuencia con el fin de posibilitar el funcionamiento eficiente de las infraestructuras de telecomunicaciones de la institución.

Otro problema que se vislumbra con la aparición de las redes inalámbricas sin control dentro de la Facultad de Ingeniería es el hecho que muchas de ellas están funcionando de manera abierta, es decir que no se requiere autenticación de ningún tipo para poder usarla, además de tener un identificador de red que pareciera ser el establecido por los fabricantes en los puntos de acceso, lo cual conlleva a deducir que los parámetros de configuración serán conocidos por individuos que conozcan de esos equipos.

2.3 INSEGURIDAD

Las redes inalámbricas nos liberan de la dependencia que impone la red cableada a permanecer en un lugar fijo sin poder movernos, sin embargo esta característica representa a su vez su mayor desventaja, ya que todas las computadoras están irradiando información de forma ininterrumpida, anunciando su presencia a cualquiera que pase dentro del rango de cobertura de su antena, las señales están viajando por el aire al alcance de quien esté dispuesto a escucharlas, entonces se puede espiar la red con relativa facilidad para el intruso, pudiendo este hacer hasta ataques para cometer delitos informáticos sin tener acceso de manera física a las instalaciones de donde se encuentre la red, adicionalmente la intercepción de paquetes de información no será detectada por lo que el atacante podrá actuar premeditadamente, sin tener alguna evidencia de ello.

La seguridad informática está definida en base a tres atributos que deben mantenerse para proteger la seguridad de la información: Integridad, Confidencialidad y Disponibilidad.

- La Integridad de los datos es comprometida cuando la información es modificada por usuarios que no están autorizados.
- La Confidencialidad de los datos se refiere a que sólo las personas facultadas pueden ver la información.
- La Disponibilidad de los datos es cuando los usuarios pueden tener acceso a la información en cualquier momento.

La seguridad de la información se refiere a la prevención y protección, por medio de mecanismos de seguridad para evitar que ocurra de manera accidental o intencional alguna transferencia, fusión, modificación o destrucción no autorizada de la información. Estos mecanismos de seguridad son una colección de herramientas diseñadas para la protección de los sistemas a fin de evitar amenazas de confiabilidad, integridad, autenticación, no repudio y la disponibilidad de la información.

La seguridad de las redes inalámbricas ha sufrido su mayor golpe en la parte de la confidencialidad de los datos debido a la forma en que se trasmite la información utilizando como medio el aire, en donde se hace muy fácil la escucha y captura de información; sumada a esta situación, la falta de un mecanismo de autenticación de usuarios lo suficientemente robusto que asegure la confidencialidad en las comunicaciones.

Por ello es necesario garantizar la seguridad cuando estamos hablando de redes inalámbricas que usan ondas de radio. Para poder asegurar una red inalámbrica un administrador debe de conocer que tipos de vulnerabilidades existen, además de cuáles son los tipos de ataques que pueden sufrir este tipo de redes. Antes de comenzar a analizar algunas de éstas se debe de conocer al enemigo, se puede distinguir entre dos posibles tipos de atacantes según las actividades que éste intente realizar sobre la red:

- Intruso Pasivo es aquel que puede monitorear las transmisiones inalámbricas con un equipo que tenga una tarjeta de red inalámbrica, sin poder ser detectado por los administradores de la red. Este hecho hace que la red inalámbrica deberá de contar con medias criptográficas robustas para que la información que circule en la red (como datos y contraseñas) viaje por el medio de trasmisión de una manera segura; la configuración de este tipo de redes requiere de mayor trabajo en su implementación, también es necesario hacer una concientización en los usuarios para que protejan sus cuentas y contraseñas, ya que de esto depende que los intrusos pasivos se mantengan controlados.

- Intruso Activo es todo aquel que intenta de manera constante inyectar paquetes de datos en una comunicación con el fin de obtener una clave de red o de hacer que el servicio sufra de una saturación de información y deje de funcionar; conocido como el ataque de negación de servicio (DoS, Denegación del Servicio). De igual manera una buena infraestructura de seguridad criptográfica puede lidiar con este tipo de situaciones, no obstante existe también la posibilidad de que el intruso emita ruido electrónico en la frecuencia de banda utilizada y se pueda bloquear la comunicación, ante esta situación no hay forma de protección aún.

Cualquier mecanismo de seguridad debe estar basado en el hecho de que los atacantes pueden ver todo, además de que normalmente las organizaciones enfocan su seguridad en defender el perímetro de ataques externos, sin embargo los ataques pueden venir desde el interior de la organización.

Los atacantes pueden tener muchas razones para vulnerar la red, puede ser alguien que sólo busque usar la red para tener acceso a Internet o hasta un atacante que espera mandar miles de correos *spam* desde esa red o un atacante que espera encontrar una locación anónima para soltar un virus y hasta conseguir información para robar identidades o dinero.

La razón por la que se enunciarán algunas de las vulnerabilidades y posibles ataques que puede sufrir una red inalámbrica es con la intensión de que una red inalámbrica debe de considerarse como un sistema complejo, al cual se le deben de proveer las mejores prácticas de gestión y seguridad para que brinden el servicio de red con una mayor confiabilidad, disponibilidad e integridad.

2.3.1 WARDRIVING

Uno de los ataques más conocidos sobre las redes inalámbricas es el *Wardriving*. Este ataque consiste en averiguar donde hay una red inalámbrica abierta, que no cuenta con seguridad ni control de acceso, esto se realiza con una laptop que tenga una tarjeta de red inalámbrica que pueda operar de forma que capture información del ambiente sin asociarse a los puntos de acceso, todo esto con el objetivo de obtener acceso a la red para propósitos de obtener información o solamente obtener una conexión a Internet. Esta actividad se realiza desde un automóvil en movimiento circulando por lugares en donde sería probable encontrar una red inalámbrica vulnerable, aunque también podría realizarse caminando por esos lugares.

Para efectuar este tipo de ataque, primero hay que configurar la tarjeta de red de manera que sea capaz de escuchar y capturar tramas de red, el paso siguiente es cambiar la dirección física de la tarjeta de red del atacante para evitar los sistemas de filtrado por direcciones MAC (*Media Access Control*). Existen herramientas como el software *Kismet* que nos proporciona información variada sobre las redes que va detectando tal como puede ser puntos de acceso, características de la trasmisión, si existe cifrado WEP, entre otras, toda esta información es útil para un intruso. La información obtenida le permitirá saber el rango de direcciones que maneja la red a la que se está intentando acceder (a partir de esta información se puede saber la dirección de la máscara de red, la dirección de *broadcast* y el *gateway*). Con esta información obtenida ya se tiene una descripción de la red y los elementos para explotarla.

Este tipo de ataque se caracteriza por el uso de símbolos mediante los cuales se informa las características de la red identificada, esta actividad es conocida como *WarChalking*.

2.3.2 PUNTOS DE ACCESO NO AUTORIZADOS (*Rogue AP*)

Este tipo de ataque consiste básicamente en colocar un punto de acceso falso cerca de las instalaciones de la víctima, de forma que los clientes asociados o por asociarse a esa red se conecten al falso AP (*Access Point*) en lugar del legítimo. Una vez conseguida la asociación al *Rogue AP*, el atacante puede provocar ataques de tipo *DoS*, robar datos de los clientes como usuarios y contraseñas de diversos sitios Web o monitorizar las acciones del cliente. Este tipo de ataques se ha empleando tradicionalmente para: crear puerta traseras corporativas, espionaje industrial entre otras actividades.

El *Rogue AP* puede consistir en un AP modificado o una laptop con el software adecuado instalado, como por ejemplo: un servidor HTTP (*HyperText Transfer Protocol*), un servidor DNS (*Domain Name System*), un servidor DHCP (*Dynamic Host Configuration Protocol*) y hasta un Portal Cautivo. Todo este proceso de instalación y configuración *Rogue AP* se puede simplificar bastante mediante la utilización de herramientas como *Airsnaf* que es un programa que automatiza el proceso de configuración y arranque de *Rogue* AP.

2.3.3 ATAQUES DE DENEGACIÓN DE SERVICIO (DoS)

Este tipo de ataque es un problema común de seguridad en las redes, se refiere a un intento de perturbar las funciones de servicio que se ofrecen. Puede darse el caso de que el ataque se realice con la destrucción física del equipo de red o inclusive utilizar equipos y software que hagan el ataque consumiendo todo el ancho de banda. Puede darse el caso de que esta denegación de servicio se realice de manera personalizada es decir sobre alguien en particular o que vaya dirigido específicamente a un dispositivo. Este tipo de ataque es particularmente problemático para las redes inalámbricas debido a la facilidad que se tiene para poder acceder a una de ellas. Un atacante puede hacer una Denegación de Servicio simplemente con equipo de radio-interferencias sobre una red en particular, o el ataque más común es mediante tarjetas de red 802.11 que consumen en gran cantidad los recursos de la red.

2.3.4 ATAQUES DE AUTENTICACIÓN

El acceso a la red le puede significar muchos más beneficios a un atacante. Los diseñadores del protocolo 802.11 crearon un mecanismo de autenticación que actualmente ya ha presentado debilidades, la autenticación de llaves compartidas es fácil de vulnerar y presenta fugas de información en el flujo de su cifrado. Es un método de autenticación mutuo en donde cada lado se envía un desafío con sus llaves conocidas WEP. Este método de autenticación puede ser atacado ya que el intruso consigue obtener suficiente información para generar una llave válida que le de acceso a la red. Con una operación simple de XOR del desafío y su respuesta se alcanza a identificar un fragmento del llamado IV (que se definió en el tema de Protocolos de Cifrado del capítulo I); una vez obtenido el IV simplemente puede cifrar cualquier desafío y podrá autenticarse.

Otra forma de evitar el control de acceso que pudieran tener las redes inalámbricas es mediante un *MAC Spoofing*, ya que hay algunas redes que implementan un filtrado por dirección física MAC, en los puntos de acceso se tienen configuradas las MAC permitidas, las cuales puede obtener fácilmente un atacante con sólo obtener información de los paquetes capturados de la red inalámbrica. *MAC Spoofing* se refiere a un cambio de la dirección física de red MAC a una dirección válida para obtener acceso a una red.

2.3.5 ATAQUE SOBRE PROTOCOLO WEP

El protocolo de cifrado WEP desde su aparición demostró debilidades en su implementación que lo ha convertido en el centro de los ataques dirigidos a las redes inalámbricas. Existen múltiples formas de vulnerar este protocolo, a continuación se mencionan algunos de los más conocidos al momento.

2.3.5.1 ATAQUES PASIVOS DE DECIFRADO DE TRÁFICO

Ocurren cuando se intercepta al tráfico de red inalámbrica en busca de una colisión de IV (*Initialization Vector*). Un individuo dedicado a escuchar de manera silenciosa el tráfico, lo intercepta en forma pasiva hasta obtener 2 paquetes que comiencen con el mismo IV. Con el XOR de estos 2 paquetes el atacante puede obtener el XOR de los 2 textos planos. Esto le permite inferir datos acerca del contenido de ambos mensajes. Como el tráfico IP es a menudo predecible y redundante, se utiliza ese conocimiento para descartar posibilidades acerca del contenido de los mensajes. Cualquier otro conocimiento acerca del contenido de los paquetes también se puede utilizar con ese fin.

Cuando tal análisis estadístico es poco concluyente basado solamente en dos mensajes, el atacante puede buscar más colisiones del mismo IV. Una vez que se obtiene un texto plano entero, todos los demás mensajes con el mismo IV se obtienen de forma directa. Una extensión de este ataque utiliza un host en alguna parte de Internet para enviar tráfico desde el exterior a un host en una red inalámbrica. El contenido del texto plano es conocido por el atacante. Cuando el atacante intercepta la versión cifrada de su mensaje, podrá descifrar todos los paquetes que comiencen con el mismo IV.

2.3.5.2 ATAQUES ACTIVOS PARA INYECCIÓN DE TRÁFICO

Ocurre cuando el atacante inserta paquetes propios cifrados en el flujo de datos de una red inalámbrica. Supongamos que un atacante sabe el texto plano exacto para un mensaje cifrado. Entonces puede utilizar este conocimiento para construir paquetes cifrados correctamente. El procedimiento implica la construcción de un nuevo mensaje, calculando el CRC-32, y cambiar los bits necesarios en el mensaje cifrado original para cambiar el texto plano en el nuevo mensaje. Una propiedad básica es que RC4 (X) xor X xor Y = RC4 (Y). Este paquete se puede ahora enviar al AP o a una estación móvil, y será aceptado como paquete válido.

Una modificación leve a este ataque lo hace mucho más complicado. Incluso sin el conocimiento completo del paquete, es posible mover pedazos seleccionados en un mensaje y ajustar con éxito el CRC

cifrado, para obtener una versión cifrada correcta de un paquete modificado. Si el atacante tiene conocimiento parcial del contenido de un paquete, puede interceptarlo y realizar una modificación selectiva en el mismo.

2.3.5.3 ATAQUES ACTIVOS PARA DESCIFRAR TRÁFICO

Ocurre cuando se engaña al AP para descifrar tráfico arbitrario. En este caso, el atacante hace una suposición no sobre el contenido, sino sobre la cabecera de un paquete. Esta información es generalmente fácil de obtener; particularmente, todo lo que es necesario suponer es la dirección IP de destino. Armado con este conocimiento, el atacante puede cambiar partes apropiadas para transformar la dirección IP de destino y enviar el paquete a una máquina que él controla, en alguna parte de Internet. La mayoría de las instalaciones inalámbricas tienen conectividad a Internet; el paquete será descifrado con éxito por el AP y enviado en forma descifrada a la máquina del atacante, revelando el texto plano. Si se puede hacer una suposición también sobre las cabeceras del paquete TCP, puede incluso ser posible cambiar el puerto de destino en el paquete para que sea enviado al puerto 80, lo que permitirá que sea enviado a través de la mayoría de los firewalls.

2.3.5.4 ATAQUES DE DICCIONARIO

El pequeño espacio de IVs posibles permite que un atacante construya una tabla de descifrado. Una vez que aprenda el texto plano para un paquete, el atacante puede calcular el ***keystream*** de RC4 generado por el IV usado. Esta ***keystream*** se puede utilizar para descifrar el resto de los paquetes que utilicen el mismo IV. En un cierto plazo, el atacante puede acumular una tabla de IVs y de ***keystreams*** correspondientes. Esta tabla requiere una cantidad bastante pequeña del almacenamiento (~15GB) y una vez que se construya, el atacante puede descifrar cada paquete que se envíe sobre la red inalámbrica.

2.3.5.5 ATAQUE FMS (FLUHRER-MANTIN-SHAMIR)

El cifrado empleado por las redes inalámbricas WEP como ya se mencionó con anterioridad está basado en el algoritmo de cifrado RC4 del cual se conocen algunas vulnerabilidades. Este ataque estadístico *FMS* se basa en vulnerabilidades derivadas de su implementación específica de RC4 en WEP. El pilar en el que se basa el ataque son los llamados *IV* débiles; identificar este tipo de *IV* consiste en comprobar aquellos que cumplen con cierta condición necesaria para poder realizar el ataque. Estos *IVs* tienen la característica especial de que provocan la no inclusión de información de la clave en el *keystream*. Para cada uno de los paquetes que cumplen esta condición se ha de adivinar el byte que no tiene información de la llave. La probabilidad de adivinar el byte de la llave correctamente es de un 5% para cada paquete con un *IV* débil.

2.3.6 ATAQUE DE HOMBRE ENMEDIO (*Man-In-The-Middle*)

Mediante este tipo de ataque se hace creer al cliente victima que el atacante es el AP y, al mismo tiempo, convencer al AP que el cliente es el atacante. Para llevar a cabo este tipo de ataque es necesario obtener los siguientes datos mediante un *sniffer*: SSID de la red, la dirección MAC del cliente y del punto de acceso. Una vez obtenidos estos datos se rompe la conexión entre el cliente y AP mediante técnicas de DoS, tras esta ruptura el cliente comenzará a buscar un nuevo AP, momento que aprovechará el atacante para suplantar al AP empleando su MAC y SSID en un canal distinto. Para ello el atacante deberá poner su tarjeta de red inalámbrica en modo MASTER.

De forma paralela el atacante ha de suplantar la identidad del cliente con el AP real empleando para ello la dirección MAC del cliente, de esta forma el atacante logra colocarse entre ambos dispositivos de forma transparente.

2.3.7 ATAQUE DE GEMELO MALIGNO (*Evil Twin*)

Este tipo de ataque de redes inalámbricas consiste en poner un punto de acceso inalámbrico el cual aparenta ser un acceso a una red de confianza, sin embargo este punto de acceso no autorizado ha sido instalado por atacantes con el objetivo de interceptar datos que se trasmiten como contraseñas, números de cuentas de banco, información personal, etcétera. Este ataque puede ser instalado en una laptop que cuente con una tarjeta de red inalámbrica que pueda funcionar como punto de acceso, para anular la señal legitima de la red los atacantes aumentan la potencia de su señal para llegar más fuerte a los clientes cercanos ocupando el mismo identificador de red (SSID) y así aparentar ser la red inalámbrica real.

Este gemelo maligno puede ser configurado para monitorear el trafico entre la computadora del usuario y el verdadero punto de acceso sin que el usuario se de cuenta de lo que está sucediendo. Este tipo de ataques típicamente se lleva acabo cerca de lugares donde existen redes inalámbricas abiertas como aeropuertos, hoteles, librerías, etcétera.

2.3.8 ATAQUE ARP POISONING

El objetivo de este ataque consiste en acceder al contenido de la comunicación entre dos terminales conectadas mediante dispositivos inteligentes como un switch. En esta variante del ataque de *Man-In-The-Middle* se recurre a la alteración de la tabla ARP que mantienen de formas *stateless* todos los dispositivos de la red. Para ello el atacante envía paquetes ARP REPLY a un equipo A perteneciente a la red cableada diciéndole que la dirección IP del equipo B perteneciente a la red inalámbrica la tiene la MAC del atacante, de esta manera consigue modificar la cache de ARP´s del equipo A. Luego realiza la misma operación atacando al equipo B y haciéndole creer que la dirección IP del equipo A la tiene también su propia MAC.

Como ARP es un protocolo *stateless*, los equipos A y B actualizan su cache de acuerdo a la información que el atacante ha inyectado en la red. Como el punto de acceso y el switch al que está conectado forman parte del mismo dominio de *broadcast*, los paquetes ARP pasan de la red inalámbrica a la red cableada sin ningún problema. Para realizar este tipo de ataque existes múltiples herramientas, ya que este tipo de ataque no es específico de las redes inalámbricas.

2.3.9 ATAQUE WPA-PSK

El único ataque conocido contra WPA-PSK es el de tipo fuerza bruta o de diccionario; pese a la existencia de este tipo de ataque la realidad es que el rendimiento del ataque es tan bajo y la longitud de la *passphrase* puede ser tan larga, que efectuarlo de forma efectiva es prácticamente imposible. Los requisitos para llevar a cabo este tipo de ataque son: un archivo con la captura de establecimiento de la conexión entre el cliente y el AP, el nombre del SSID y un archivo de diccionario. Se puede auditar por medio de ataque de fuerza bruta sobre las contraseñas empleadas en un sistema, en este último caso empleando herramientas para crear todas las combinaciones de caracteres posibles.

Como se puede observar existe una gran variedad de posibles ataques sobre las redes inalámbricas algunos de ellos de mayor gravedad que otros, sin embargo cada unos de ellos debe de ser tomado en cuenta cuando se implementará un servicio de red inalámbrica. A continuación se presenta un resumen de algunos ataques a las redes inalámbricas, en este cuadro se toman en cuenta aspectos como que vulnerabilidad asociada tiene este ataque, cuál es el uso típico en las redes inalámbricas, sus posibles consecuencias o resultados, cómo detectarlos y prevenirlos. Después se presenta una clasificación de estos ataques según:

Dificultad de Detección: se refiere a una aproximación de dificultad que tendrán las personas encargadas de la red para detectar el ataque. El valor es de menor a mayor escala, es decir, un valor de 1 equivale a que casi es detectable en cualquier situación el ataque, el valor de 5 se refiere a que casi es imposible detectarlo.

Facilidad de Uso: se refiere a que tan complicado es la ejecución de este ataque. El valor de 1 significa que para ejecutar este ataque se requiere de conocimientos avanzados para llevarlo acabo, un valor de 5 significa que atacantes que son novatos pueden realizarlo.

Frecuencia: se refiere a que tan común es este tipo de ataques a la red. Un valor de 1 se refiere a que este tipo de ataque se casi no se realiza, por el contrario un valor de 5 se coloca para ataques que son diariamente vistos.

Impacto: se refiere a cuánto daño puede causar en la red este tipo de ataque, un valor de 1 significa que casi no tiene efecto sobre la red, y un valor de 5 significa que puede ser muy grave.

TABLA 2.1 Principales ataques a las redes inalámbricas

PRINCIPALES ATAQUES A REDES INALÁMBRICAS									
NOMBRE DEL ATAQUE	VULNERABILIDAD ASOCIADA	USO TÍPICO	RESULTADO DEL ATAQUE	DETECCIÓN	PROTECCIÓN	DIFICULTAD DE DETECCIÓN	FACILIDAD DE USO	FRECUENCIA	IMPACTO
Wardriving	Uso o políticas de configuración de dispositivos.	Descubrir AP's mal configurados para acceder a la red.	Mayor número de accesos.	Casi imposible.	Comprobación periódica de los AP's de la red, auditoría de configuración.	5	4	3	5
Sniffer	Ninguna.	Lectura del tráfico de red inalámbrica.	Pérdida de confidencialidad en la información.	Antisniifers.	Criptografía.	5	5	3	3
MAC Spoofing	Ninguna.	Robo de direcciones MAC válidas para poder enviar o recibir información.	Mayor número de accesos y pérdida de confidencialidad en la red.	Ninguna.	Uso de entradas estáticas en los switch con Memoria de Contenido Direccionable (CAM, Content Addressable Memory).	3	5	1	3
AP´S No autorizados	Del uso, políticas de uso y de controles físicos de seguridad.	Ofrecer el servicio de red de manera no autorizada robando datos que pasen a través del AP.	Pérdida de la integridad y confidencialidad de la información.	Inventario lógico de redes inalámbricas	Sistema de detección de intrusos inalámbricos.	3	2	2	5
DoS	Políticas de buen uso.	Alentar o hasta suspender el servicio de red inalámbrica.	Denegación del Servicio.	IDS, Análisis de bitácoras.	Filtros específicos de tráfico de red en Firewalls.	2	2	3	4
PEAP Man-In-the-Middle	Variable.	Captura de tráfico de red y secuestro de sesiones.	Variable (muchos resultados posibles).	Variable.	Criptografía.	4	2	1	5
Virus, Gusanos y Caballos de Troya	Software y uso.	Variable.	Variable (muchos resultados posibles).	IDS.	Aplicaciones de seguridad y software antivirus.	3	4	5	4
Cracking WEP	Inherente al método WEP.	Obtención de la clave WEP para tener acceso a la red.	Mayor número de accesos y pérdida de confidencialidad en la red.	Casi imposible.	Métodos criptográficos más robustos.	5	3	2	3
Saturación del medio inalámbrico	Asociada al medio de trasmisión.	Alentar o hasta suspender el servicio de red inalámbrica.	Denegación del Servicio.	Inventario lógico de redes inalámbricas.	Sistema de detección de intrusos inalámbricos.	1	3	3	4

2.4 FALTA DE NORMATIVIDAD

De manera general una norma es un conjunto de especificaciones de carácter administrativo y técnico que dictan el comportamiento adecuado del proceso tecnológico en este caso, son de aplicación voluntaria y está elaborada (por consenso) por las partes interesadas que participan en el proceso al cual se esté aplicando, estas normas deben de ser de conocimiento público.

Hablando de las redes inalámbricas se ha mencionado de su problemática y peligros que afectan el rendimiento, la seguridad, la calidad en el servicio, etcétera, cuando no se tienen correctamente gestionadas es por ello necesaria la creación de un conjunto de normas que eviten el acceso no controlado a los recursos tecnológicos.

Existen las Políticas de Seguridad en Cómputo de la Facultad de Ingeniería que tocan algunos aspectos que podrían estar relacionados con las redes inalámbricas, sin embargo como tal no existe una normatividad sobre redes inalámbricas para la institución, por lo que se vuelve necesaria la creación e implementación de una reglamentación para este tipo de tecnologías.

La instalación de puntos de acceso no autorizados provoca que personas no facultadas puedan tener acceso a la red, así como problemas de congestión de los canales de comunicación de las redes inalámbricas, por lo tanto es necesario actuar de forma organizada para la creación de normas que regulen estas tecnologías en la Facultad de Ingeniería.

La inexistencia de normatividad en cuestión de redes inalámbricas es causa de problemas como la falta de asignación de responsabilidades en asuntos de administración, configuración y control de los dispositivos de la red como lo son los puntos de acceso. También como consecuencia de esta carencia de normatividad, surge la creación de redes inalámbricas sin justificar su uso ni su localización.

2.5 ESCENARIOS ACTUALES DE USO

La falta de información y control de la infraestructura de la red inalámbrica de la Facultad de Ingeniería es producto del momento actual que se vive en cuanto a la administración de estos recursos tecnológicos de la institución. Como toda Tecnología de la Información de una organización debe de ser plenamente controlada para poder así conseguir el objetivo bajo el cual fue implementada; partiendo de esta premisa nos podemos dar cuenta que el descuido que se tiene sobre las redes inalámbricas puede llegar a desembocar en problemas graves.

Haciendo un análisis de cómo se utilizan las redes inalámbricas en la Facultad de Ingeniera en estos momentos, no se necesita de mucha investigación para darnos cuenta que no existe una base de datos de puntos de acceso ni de las personas quienes tienen las responsabilidades sobre recursos de este tipo, lo que complicaría la solución de posibles problemas de seguridad en cómputo que pudieran llegar a presentarse, tales como ataques a servidores desde redes inalámbricas existentes en la Facultad sin tener manera de localizar la fuente de dicho ataque.

Actualmente para hacer una red inalámbrica dentro de la Facultad de Ingeniería sólo es necesario contar con un acceso o nodo de red, que sea parte de la infraestructura de la institución al mismo tiempo de contar con el punto de acceso que dará el servicio inalámbrico para dicha red, lo que hace evidente la falta de medidas y políticas de control. En la Facultad de Ingeniería existen entidades especializadas en el ramo que podrían tomar partido en la gestión y administración de estos recursos, tales como los Departamentos de Seguridad en Cómputo y el Departamento de Redes y Operación de Servidores que están adscritos a la Unidad de Servicios de Cómputo Académico de la Secretaria General en la Facultad de Ingeniería.

Este escenario actual de uso vislumbra futuros problemas si no se regula la proliferación de las redes inalámbricas dentro de la institución, con anterioridad se han mencionado problemas de seguridad informática que pueden llegar a ser de gravedad, sumado a esta situación podrían presentarse problemas en la calidad del servicio que se ofrece, producto del solapamiento de las redes inalámbricas como ya se mencionó.

Por lo que se considera muy importante regular la implementación de redes inalámbricas siempre con el objetivo de aprovechar al máximo los recursos tecnológicos con que se cuenta.

2.6 ESTRATEGIA DE SOLUCIÓN A LA PROBLEMÁTICA

Como consecuencia de este capítulo resulta imperativo plantear una estrategia integral que permita mejorar la situación actual en la cual está inmersa la Facultad de Ingeniería con relación a la omisión de gestión de las redes inalámbricas. Esta estrategia deberá ser integral, en donde se cubran aspectos de carácter administrativos y técnicos, de manera que se finquen responsabilidades a las personas encargadas de estos recursos en caso de alguna contingencia.

La estrategia que se pretende seguir y que se desarrollará en este trabajo de tesis cubrirá los siguientes aspectos:

- **Análisis de riesgos.** En esta fase de la estrategia se utilizará la metodología OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*) para obtener un análisis puntual de los riesgos y vulnerabilidades en cuanto a la situación actual de la Facultad de Ingeniería. Esta metodología permite la creación de una estrategia y planes de seguridad desarrollados a partir del análisis hecho en las etapas en que está constituida esta metodología:

    1. Construcción de activos basados en los perfiles de amenaza.
    2. Identificación de vulnerabilidades dentro de la infraestructura.
    3. Desarrollo de planes y estrategias de seguridad.

    Como parte del análisis de riesgos y vulnerabilidades, se hará un levantamiento de un inventario lógico de redes inalámbricas dentro de la Facultad de Ingeniería, que descubrirá las configuraciones actuales bajo las que están funcionando los servicios inalámbricos. La información que se obtenga servirá para identificar posibles debilidades y omisiones en configuraciones de redes inalámbricas.

- **Políticas para las redes inalámbricas.** Parte fundamental de esta estrategia de gestión de redes inalámbricas es contar con políticas de seguridad de las redes inalámbricas para la Facultad de Ingeniería. Como se mencionó anteriormente la falta de normatividad en los servicios de red inalámbricos dentro de la Facultad de Ingeniería puede ser razón de un mal uso de las Tecnologías de Información de la institución.

    Las políticas de las redes inalámbricas para la Facultad de Ingeniería que se propongan estarán sustentadas en el análisis hecho con anterioridad y cubrirán aspectos tales como políticas de seguridad, políticas de infraestructura, políticas del buen uso, políticas de la responsabilidad en cuanto a su administración, políticas sobre la autorización, entre otras. Estas políticas deberán ser publicadas para que sean conocidas por la comunidad en general.

- **Herramienta de gestión de redes inalámbricas.** Una parte significativa de la estrategia de gestión de redes inalámbricas está en el desarrollo de una herramienta que permita de manera centralizada un mejor manejo de las redes inalámbricas dentro de la Facultad de Ingeniería. Esta

herramienta consistirá en un desarrollo Web, el cual permitirá la publicación de las políticas que se desarrollaron con anterioridad, así mismo, presentará un procedimiento de registro de redes inalámbricas para que la existencia de estas redes esté justificado por su uso y se tenga pleno conocimiento de los responsables de dichas redes inalámbricas.

Esta herramienta Web permitirá un control de registro y ubicación de las redes inalámbricas dentro de la Facultad de Ingeniería. Además mediante esta herramienta se podrán generar estadísticas de manera automatizada acerca de parámetros de red e información relacionada a la seguridad.

- **Configuraciones adecuadas y buenas prácticas.** Otra parte importante de la gestión de redes inalámbricas son las configuraciones adecuadas y buenas prácticas que son procedimientos y recomendaciones que se emiten para hacer una red inalámbrica más segura y eficiente, esta parte resulta muy importante ya que si los recursos de las Tecnologías de Información de la Facultad de Ingeniería siguieran con este tipo de prácticas el número de incidentes de seguridad en cómputo disminuirán.

- **Monitoreo de redes inalámbricas.** En las redes de datos de manera general, el monitoreo es una actividad que representa el saber cómo se está comportando la red, además de que permite identificar a posibles intrusos y sus actividades que intenten sobre la red, en las redes inalámbricas de igual manera, el monitoreo resulta una tarea elemental para gestiónalas. Por esta razón se elaborarán documentos que describan software y su configuración para monitorear redes inalámbricas los cuales estarán disponibles dentro de la misma herramienta Web.

- **Auditoría.** Al igual que el monitoreo, la auditoría en los sistemas informáticos representa una actividad primordial para verificar que los sistemas de información funcionen bajo el objetivo que fueron creados y que cumplan con las políticas, es por ello que la auditoría en las redes inalámbricas forma parte de las actividades necesarias para gestionarlas. La herramienta Web contará con una sección dedicada a la auditoría en redes inalámbricas con aspectos relacionados a la auditoría de la configuración, auditoría del servicio, auditoría de la seguridad y auditoría del cumplimiento de las políticas de redes inalámbricas.

Mediante estas estrategias se pretende gestionar las redes inalámbricas de la Facultad de Ingeniería y resulta importante señalar que esta tarea es un trabajo en conjunto en donde las responsabilidades sobre las redes inalámbricas recaigan no sólo en una persona encargada de la administración de red sino, desde las personas encargadas de la instalación y configuración de los puntos de acceso hasta los usuarios de las mismas.

CAPÍTULO

3

ESTRATEGIA DE GESTIÓN DE REDES INALÁMBRICAS

En este capítulo se desarrolla un análisis de riesgos de la situación actual de la Facultad de Ingeniería, lo que permitirá la creación de una estrategia de solución a las vulnerabilidades encontradas durante este análisis siendo parte fundamental de la estrategia la creación de políticas de seguridad en redes inalámbricas.

3.1 ANÁLISIS DE RIESGOS

Cuando estamos hablando de gestión de redes inalámbricas estamos hablando de la gestión de tecnologías de información y por lo tanto es necesario considerar implantar esquemas de seguridad que las protejan ya que forman parte de los activos de la organización. Los procesos de protección y resguardo de las TI´s son continuos y retroactivos, parte de este proceso es el análisis de riesgos que debe de ser una tarea que se realice de manera permanente.

Las redes inalámbricas tienen el problema de inseguridad inherente a su naturaleza, el medio de transmisión, como se mencionó con anterioridad la información transmitida por radiofrecuencia corre mayor riesgo de ser interceptada y perder su confidencialidad, integridad y autenticidad. La información que pueda llegar a transmitirse por las redes inalámbricas de la Facultad de Ingeniería puede ser información de la cual dependa la institución, así mismo la información compartida en la red puede ser fácilmente comprometida, ejemplo de ello son los puntos de acceso que pueden ser víctimas de algún tipo de ataque informático, entre otras situaciones que comprometan su funcionamiento, con esto podemos ver como la información y la infraestructura tecnológica pueden ser amenazadas debido a la falta de esquemas de seguridad que las resguarden.

Este tema contempla el análisis de riesgos sobre las tecnologías inalámbricas de la Facultad, para ello empezaremos a definir que el riesgo es la posibilidad de sufrir alguna pérdida o daño sobre algún *activo* de

de la institución, como por ejemplo puede ser información, hardware, software o algún servicio por lo que estos recursos deben de protegerse de la mejor manera, para llegar a ello hay que hacer una valoración de los riesgos que puedan correr, esto se hace mediante un análisis y administración de los riesgos.

El análisis de riesgos implica un proceso mediante el cual se identifiquen las amenazas y vulnerabilidades que pueda presentar la infraestructura de tecnología de información en una organización, de manera que se valore su impacto y la probabilidad de que ocurran, tiene como objetivo verificar que los controles de seguridad existentes de un sistema se adapten según la proporción de los riesgos que se lleguen a encontrar.

Este proceso nos permitirá identificar cualquier riesgo significativo en todos los activos de información, así como calificar el grado del riesgo y saber cómo manejarlos; también nos permitirá saber que tan expuestos están los recursos a amenazas y vulnerabilidades. Con esta información obtenida se podrá contar un informe en el cual se determinen cuales son las medidas de seguridad que solventarán los problemas encontrados para ayudar a la eliminación de riesgos de manera inmediata con un bajo costo y en un breve lapso de tiempo, identificar soluciones alternativas con sus respectivas ventajas y desventajas.

En la actualidad las organizaciones han implementado una amplia variedad de complejas infraestructuras de cómputo, para ello necesita de diferentes enfoques que les permitan entender los riesgos de seguridad con respecto a su información y a partir de ello crear estrategias dirigidas a esos riesgos. Una organización que desea incrementar su postura de seguridad debe estar preparada para tomar en cuenta los siguientes aspectos:

1. Cambio de una posición reactiva a una posición proactiva, basada en problemas con un enfoque de prevención.
2. Considerar la seguridad desde múltiples perspectivas.
3. Establecer una infraestructura flexible en todos los niveles de la organización capaz de responder de manera rápida para cambiar tecnología y necesidades de seguridad.
4. Iniciar un camino de continuo esfuerzo para mantener y mejorar la postura de seguridad.

El proceso de evaluación de riesgos de seguridad en información ayuda a identificar riesgos de seguridad sobre la información, analizar el riesgo para determinar las prioridades, y crear un plan para mejorar el desarrollo de una estrategia de protección para reducir y mejorar la mitigación de riesgos de los activos críticos de las organizaciones. Después de que en la organización se han evaluado los riesgos se deberá de realizar los siguientes pasos:

1. Planear como implementar una estrategia de protección y planes de mitigación de riesgos resultado de la evaluación mediante planes de acción detallados. Esta actividad puede incluir un análisis minucioso de costo-beneficio entre las estrategias y acciones.
2. Implementar los planes de acción detallados seleccionados.
3. Monitorear el progreso y efectividad de los planes. Esta actividad incluye monitoreo de riesgos por cualquier cambio que pudiera surgir.
4. Controlar variaciones en la ejecución del plan tomando las apropiadas acciones correctivas en caso de ser necesarias.

3.1.1 METODOLOGÍA OCTAVE

El programa de *Network System Survivability* (NSS) del Instituto de Ingeniería de Software (*SEI, Software Engineering Institute*) ha desarrollado el método Evaluación de Amenazas y Vulnerabilidades de Recursos Críticos Operacionales (*OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation*) que permite a las organizaciones tener un enfoque para la auto-evaluación de riesgos de seguridad dirigida, está

diseñado para ayudar a identificar y clasificar los principales activos de información, así como sus amenazas además de analizar las vulnerabilidades que impliquen tanto a la tecnología como sus prácticas. OCTAVE permite a cualquier organización desarrollar prioridades de medidas de seguridad basada en sus objetivos particulares, permite también que comprendan temas tecnológicos y sus respectivos riesgos de seguridad de la información.

El concepto del método OCTAVE de auto-dirigido significa que el personal de la propia organización administre y dirija la evaluación de los riesgos de seguridad en la información; en donde se destaca que la seguridad en la información es responsabilidad de todas las áreas en la organización, no sólo del departamento encargado de la seguridad en TI. Con la utilización de esta metodología se involucran diversas áreas del personal formando un pequeño grupo de trabajo que se conoce como el *Equipo de Análisis* con el objetivo de dirigir el proceso de evaluación de los riesgos dentro de la organización.

Esta metodología requiere del *Equipo de Análisis* como se mencionó anteriormente para identificar la información relacionada con los activos (información, sistemas, hardware, etcétera) que sean importantes para la organización y concentrar las actividades de análisis de riesgos en esos activos que surgieron como los más críticos. Cuando el equipo de trabajo completa la metodología OCTAVE se crea una estrategia de protección para el desarrollo de la organización, además de crear planes de mitigación para reducir los riesgos sobre activos críticos de la misma, estos procesos incorporan estrategias para su cumplimiento en tiempos de corto, mediano y largo plazo.

OCTAVE está constituido en tres fases para permitir a las organizaciones tener una perspectiva global de las necesidades de seguridad en la información.

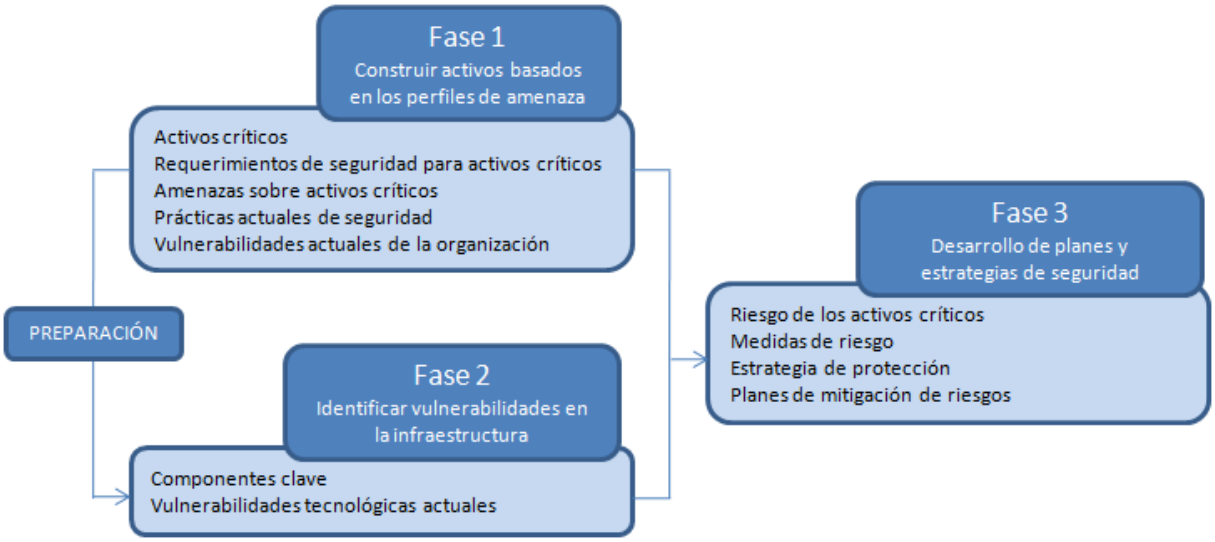


FIGURA 3.1 Metodología de OCTAVE

Después de que la organización ha desarrollado una estrategia de protección y planes mitigación es fácil de implementarlos siempre y cuando se haya analizado bien y a detalle, cuando se llega a este punto la organización ha completado el método OCTAVE.

3.1.2 LEVANTAMIENTO DE INVENTARIO LÓGICO DE REDES INALÁMBRICAS

Para iniciar el análisis de riesgos de las redes inalámbricas en la Facultad de Ingeniería se hará un levantamiento lógico de las redes inalámbricas existentes, esta actividad consiste en obtener la información de las redes 802.11 que están funcionando actualmente mediante un monitoreo del ambiente haciendo recorridos a través del perímetro de la zona donde se desean obtener los datos.

Esta actividad nos permitirá identificar el número actual de redes inalámbricas existentes en la institución y en los alrededores, así como identificar algunas de las vulnerabilidades existentes tales como redes que estén funcionando con los parámetros de fábrica, algunas redes que no implementen mecanismos de seguridad, entre otros aspectos que son de importancia para conocer el estado del vecindario de las redes inalámbricas, así como también de esta manera se observará la problemática de la proliferación de red inalámbrica sin regulación.

Para realizar esta actividad se requirió de algunas herramientas, las cuales se describen a continuación.

TABLA 3.1 Herramientas empleadas para el inventario

Herramienta	Descripción
	HARDWARE
Laptop Dell Latitude.	Computadora portátil que nos brindará la posibilidad de movilidad para realizar el inventario lógico a través de las zonas seleccionadas.
Tarjeta de red inalámbrica PCI CARD con chipset Atheros.	Este tipo de tarjeta de red es requerido para que funcione el software que se empleó para hacer el inventario lógico de las redes inalámbricas de manera que permita la captura de información.
GPS Garmin Etrex Legend.	Este dispositivo hardware es un receptor GPS que permitirá la obtención de las coordenadas de localización de los puntos de acceso. Se eligió este dispositivo debido a la compatibilidad que tiene con el software que se utilizará, además de que en la mayoría de la bibliografía que se consultó para esta actividad se utilizan estos dispositivos.
	SOFTWARE
Sistema operativo Windows XP	Este sistema operativo de Microsoft se eligió con el propósito de poder utilizar la herramienta de Netstumbler.
Netstumbler	Este software que como se mencionó funciona en sistemas operativos Windows tiene la capacidad descubrir las redes inalámbricas que estén a su alcance, obtiene la localización aproximada de los puntos de acceso si se cuenta con un GPS.
Sistema operativo Ubuntu 8.04	Este sistema operativo distribución de GNU/Linux fue seleccionado por la capacidad que tiene para reconocer dispositivos como tarjetas de red inalámbrica y GPS con gran facilidad.
Kismet	Software que funciona para distribuciones GNU/Linux con una gran cantidad de funciones que son de mucha utilidad, puede servir como descubridor de red y hasta como detector de intrusos; también puede funcionar en conjunto con un GPS para obtener la localización aproximada de los puntos de acceso y clientes.
GPSD	Es un software de Linux que monitorea los dispositivos GPS conectados al puerto serial o USB que se encuentren en el equipo. Es necesario para poder utilizar kismet con el GPS.
Google Earth	Software que permite visualizar imágenes satelitales y mapas del mundo. Será utilizado para abrir las bitácoras de captura de datos de los descubridores de red y mostrar una ubicación aproximada de los puntos de acceso detectados.
Knsgem	Es un software libre para Windows que sirve para convertir las capturas de datos de Netstumbler y Kismet en archivos compatibles para Google Earth; genera gráficas de cobertura de las redes descubiertas.

La metodología que se utilizó para el inventario de redes inalámbricas consintió en dos etapas: la primera de ellas fue la recolección de la información y posteriormente la segunda etapa fue el procesamiento de los datos obtenidos.

La recolección de los datos se hizo mediante la técnica de "warwalking", esta técnica es similar a la descrita en el tema 2.3.1 Wardriving sólo que el proceso se hace a pie en lugar de un automóvil. Con esta técnica se hicieron recorridos para obtener mediante varias trayectorias de áreas específicas de la Facultad de Ingeniería en los conjuntos norte y sur los datos necesarios para mapear la situación actual de las redes 802.11. Los puntos de obtención de los datos fueron escogidos en zonas en que se podría obtener una mayor cantidad de redes inalámbricas además de tomar en cuenta el lugar donde el GPS fuera capaz de localizar la ubicación de los puntos de acceso ya que la señal satelital del dispositivo aparecía débil en ciertas zonas.

La toma de datos fue realizada el día Jueves 16 de Octubre en el conjunto norte (Edificio Principal) y el día Martes 21 de Octubre en el conjunto sur (Anexo de Ingeniería) del año 2008.

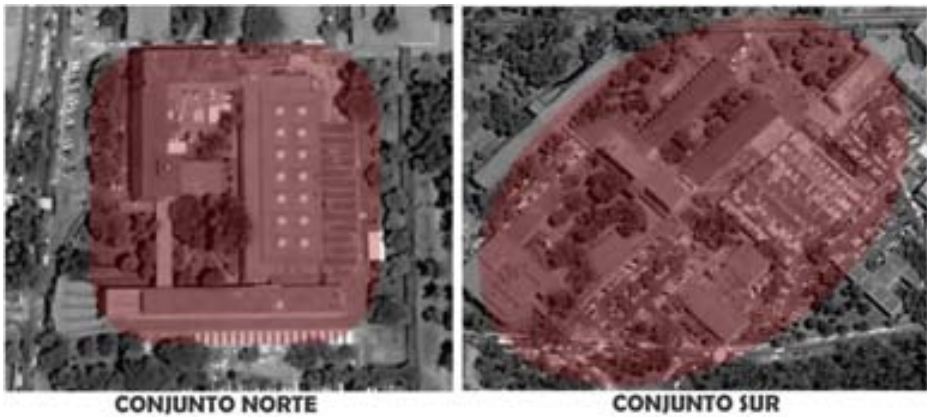


FIGURA 3.2 Área de toma de datos

El proceso de recolección de la información se realizó en dos fases: la primera de ellas se efectuó con el software Windows XP y Netstumbler en donde mediante estas herramientas se obtuvieron datos de la localización de los puntos de acceso. La segunda fase se ejecutó mediante el software *Ubuntu 8.04, GPSD y Kismet* que permitieron la captura de información cómo el cifrado que implementan las redes inalámbricas, estas dos fases se realizaron en los conjuntos norte y sur siguiendo las mismas trayectorias.

La razón por la cual se hizo el proceso de recolección de la información en dos fases se debe a que el software Netstumbler tiene la funcionalidad de poder adjuntar las diferentes tomas de datos en un solo archivo de captura lo que da como resultado una sola bitácora por conjunto, es decir un archivo de captura de datos del conjunto norte y uno del sur.

Adicionalmente la otra razón importante por la cual se hizo también con el software Kismet la toma de datos, es que nos permite una mayor calidad de la información que se recolecta, ya que con Netstumbler sólo proporciona el dato de que si es implementado el protocolo WEP o no, a diferencia de Kismet que hace un pronóstico más preciso del tipo de cifrado de las redes inalámbricas detectadas.

Cuando se tenían las tomas de datos completas se procedió a realizar la segunda fase que se refería al procesamiento de la información. Para ello se obtuvieron dos archivos de Netstumbler, uno por el conjunto norte y otro por el conjunto sur de la Facultad de Ingeniería, los cuales servirían para obtener los mapas de localización aproximada de los puntos de acceso.

Los archivos de Netstumbler que tienen como extensión de archivo ".ns1" debía ser convertido al formato de archivo el cual fuera capaz de interpretar Google Earth (".kml") y establecer la ubicación en un mapa de la zona. Para ello se utilizó el software Knsgem que se instaló en Windows XP para generar estos archivos. Este software además de generar el archivo ".kml" con la ubicación de los puntos de acceso obtenidos, genera un archivo del mismo tipo que permitirá la creación de mapas con la cobertura aproximada de los puntos de acceso detectados. Por otro lado, los datos que se obtuvieron con Kismet se procesaron de manera que se obtuvieron los siguientes datos de todas las redes inalámbricas detectadas:

- SSID.
- Dirección MAC de los puntos de acceso.
- Canal de comunicación.
- Método de cifrado.
- Máxima potencia
- Modo de operación.

La información que se obtuvo permitirá tener un mejor panorama de la situación actual que se vive en la institución con respecto a las redes inalámbricas durante el análisis de riesgos que se realizará en el siguiente tema.

A continuación se ilustran los mapas que exponen la situación actual de las redes inalámbricas en la Facultad de Ingeniería. En la FIGURA 3.3 y FIGURA 3.4 se muestra la localización aproximada de los puntos de acceso detectados durante el inventario lógico, se puede observar que existen redes inalámbricas que no pertenecen a la Facultad de Ingeniería, sin embargo es importante conocer el estado de los alrededores para saber que tan congestionado está el ambiente. Las marcas rosas indican los puntos de acceso que no presentan ningún mecanismo de cifrado, las azules son las redes que implementan el protocolo WEP donde claramente son la mayoría y por último las marcas verdes son redes que implementan algún otro método de cifrado como puede ser WPA, WPA-PSK, etcétera.

FIGURA 3.3 Localización aproximada de los puntos de acceso y su método de cifrado en el conjunto Norte

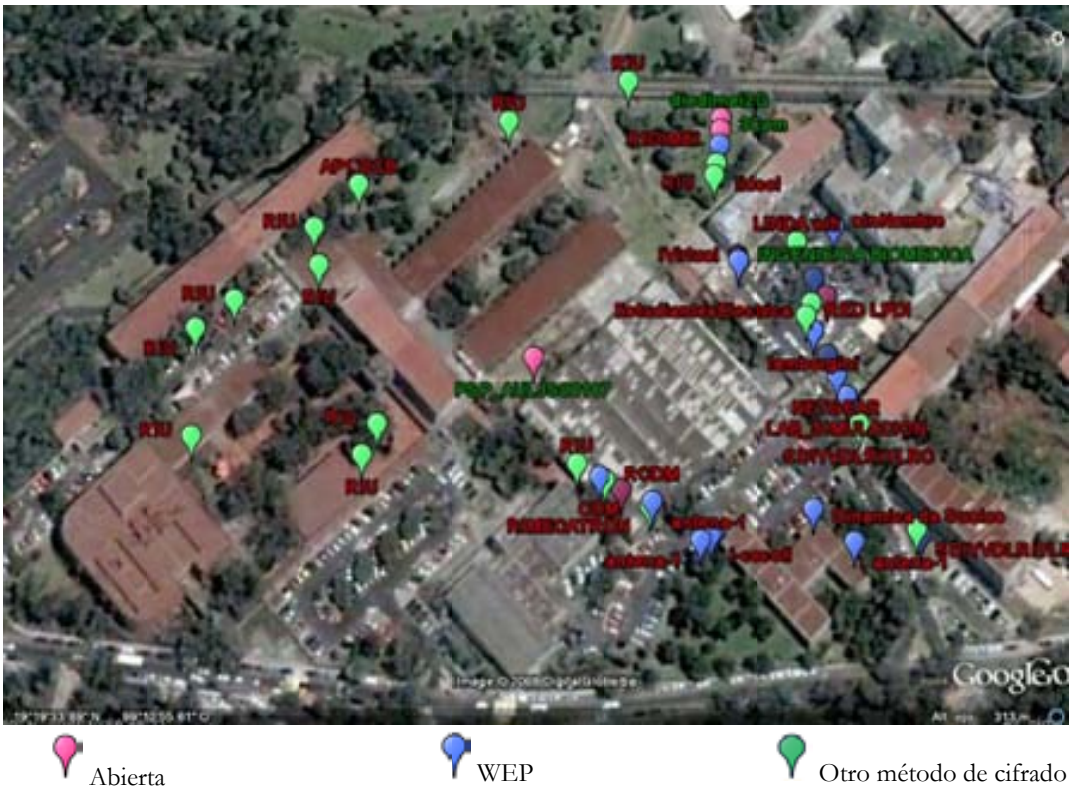


FIGURA 3.4 Localización aproximada de los puntos de acceso y su método de cifrado en el conjunto Sur

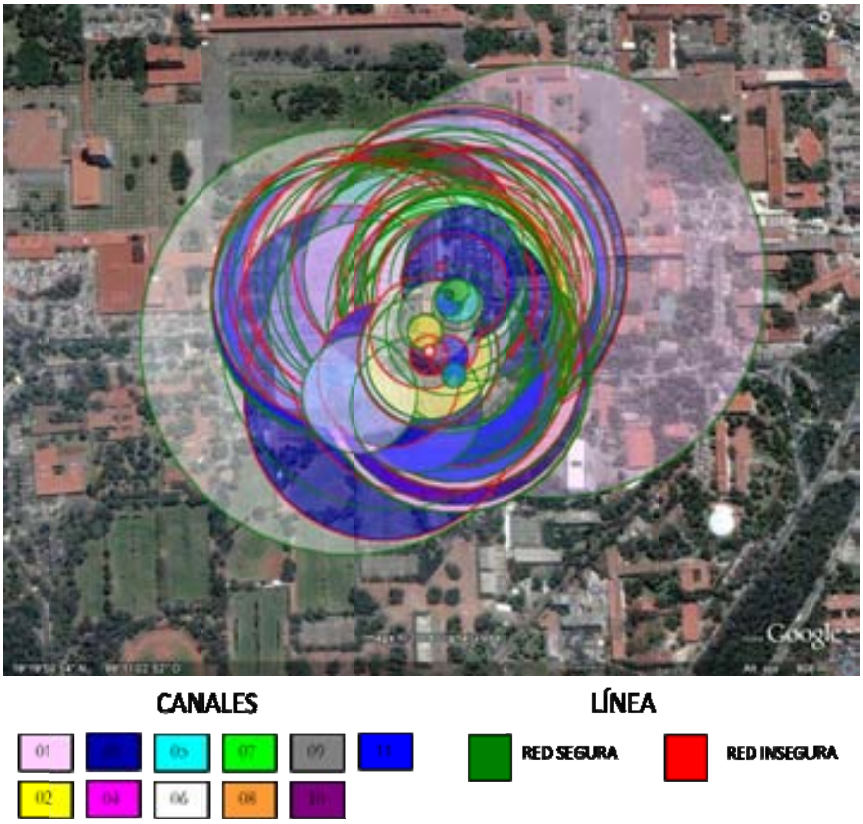
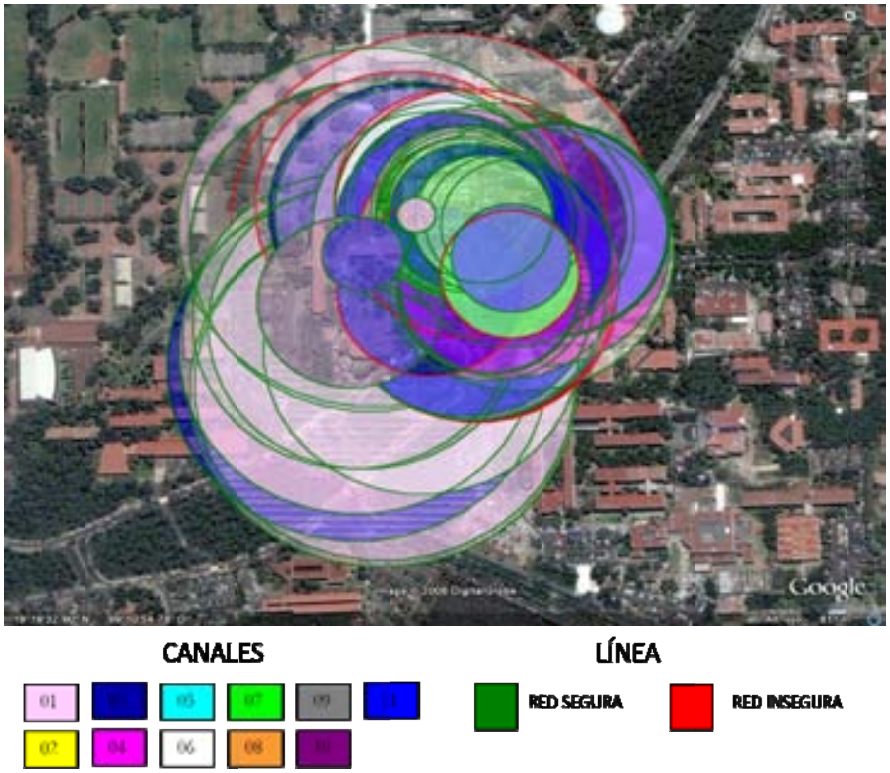


FIGURA 3.5 Área aproximada de cobertura de los puntos de acceso en el conjunto norte



FIGURAS 3.6 Área aproximada de cobertura de los puntos de acceso en el conjunto sur

En las FIGURA 3.5 y FIGURA 3.6 se muestran las aproximaciones de la cobertura de los puntos de acceso en la Facultad de Ingeniería y de las zonas aledañas. A partir de esta imagen se puede ver la gran cantidad de redes por donde está circulando información en el espacio aéreo. Además permite ver en qué canales de comunicación están funcionando, en donde el color de cada canal está establecido por la configuración del software utilizado Knsgem. Adicionalmente cada perímetro de cobertura de las redes inalámbricas está delimitado por una línea de color verde o rojo, para lo que el color verde significa que la red inalámbrica implementa algún mecanismo de seguridad desde WEP hasta WPA2, por lo contrario la línea de color rojo significa que la red inalámbrica no implementa medida de control de acceso, es decir está abierta a los usuarios.

Estas imágenes permiten obtener una perspectiva de las redes inalámbricas existentes dentro de la Facultad de Ingeniería así como de sus alrededores.

3.1.3 RESULTADOS / ESTRATEGIAS

Una vez que se han obtenido los datos del inventario lógico de redes inalámbricas es posible analizar estos resultados con la metodología OCTAVE anteriormente desarrollada.

METODOLOGÍA OCTAVE APLICADA AL CASO DE REDES INALÁMBRICAS DENTRO DE LA FACULTAD DE INGENIERÍA.

FASE 1. Construcción de perfiles de amenaza basados en activos.

En esta primera fase de la metodología se identifican los activos de la institución, áreas de preocupación, requerimientos de seguridad y el conocimiento de la situación actual así como de sus vulnerabilidades. Como primer paso se **identificaron los activos críticos** para la Facultad de Ingeniería:

- Información que se trasmita por las redes inalámbricas.
- Redes inalámbricas.
- Infraestructura de las redes inalámbricas.

La elección se hizo con base al criterio de que en las Tecnologías de Información un activo puede combinar aspectos físicos o lógicos que tengan algún valor para la organización; en este caso como primer punto se colocó a la información que viaja por las redes inalámbricas también como un activo critico por la calidad de información que circula por ellas, ya que no se sabe con certeza el uso que se le da a las comunicaciones de este tipo no podemos aseverar que tan relevante es esta información, por lo que se considera de carácter sensible la información que llegue a transmitirse.

Se consideró en segundo lugar a las redes inalámbricas que son de valor para la institución ya que a través de ellas se comunican una gran cantidad de usuarios ya sean estudiantes, académicos, investigadores y demás personal con diversos objetivos.

Por último se identificó a la infraestructura tecnológica que hace posible la implementación de redes inalámbricas como un activo crítico ya que pueden ser vulnerados de diversas maneras por lo que se debe de considerar para generar una estrategia que permita su protección, esta infraestructura se refiere al hardware y software que forman parte de la red inalámbrica, cómo puntos de acceso, antenas, sistemas de información como servidores o aplicaciones que se utilicen en la Facultad.

TABLA 3.2 Activos críticos

Activo Crítico	Descripción
Información que se transmita por las redes inalámbricas	Las redes inalámbricas pueden servir como medio de comunicación con muchos objetivos ya sean de investigación, de consulta, financieros, entre otros tipos de información.
Redes inalámbricas institucionales	La red de datos de la Facultad de Ingeniería representa una Tecnología de Información fundamental en el funcionamiento de la Facultad, que se utiliza con fines de investigación, consulta, como herramienta de trabajo para compartir sistemas institucionales, etcétera.
Infraestructura de las redes inalámbricas	Los dispositivos como puntos de acceso, antenas, routers inalámbricos entre otros equipos son parte de la infraestructura tecnológica de la Facultad de Ingeniería.

Después es necesario analizar las cualidades que son importantes a proteger de los activos críticos identificados, existen tres requerimientos básicos de seguridad que se deben de considerar que son: la confidencialidad, la integridad y la disponibilidad. Estos aspectos son muy importantes de analizar ya que darán la pauta para desarrollar la estrategia de protección a estos activos que se han seleccionado. Los activos de la organización no deben de ser accesibles a personal no autorizado (confidencialidad), de la misma manera deben de ser modificados únicamente por el personal autorizado (integridad) y además deben de estar disponibles en cualquier momento que sean requeridos (disponibilidad).

A continuación se hace un cuadro que resume los **requerimientos de seguridad para los activos críticos** que se han detectado en esta primera fase de la metodología.

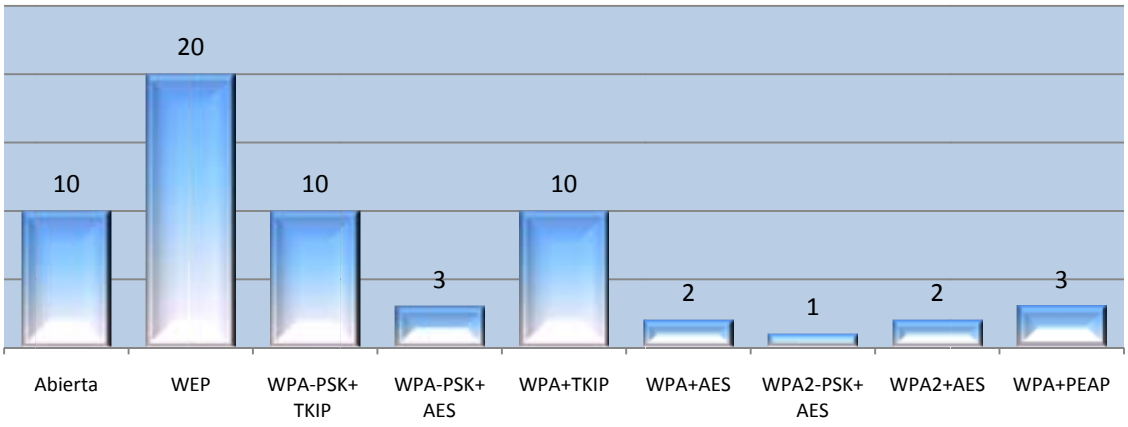
TABLA 3.3 Requerimientos de seguridad de los activos críticos

Activo Crítico	Requerimientos de Seguridad		
	Integridad	Disponibilidad	Confidencialidad
Información que se transmita por las redes inalámbricas	Independientemente del tipo de información que se transmita por el medio inalámbrico ninguna debe ser modificada si no es por los usuarios indicados.	La disponibilidad de la información que viaja por el medio inalámbrico	Uno de los grandes retos para las redes inalámbricas es lograr que la información que viaja por el aire tenga la confidencialidad que se necesita para considerar la red inalámbrica segura.
Redes inalámbricas institucionales	Las redes inalámbricas transmiten información sensible que debe ser sólo manipulable por sus usuarios.	Brindan servicio de conectividad con diversos fines y este servicio debe de ser continuo y óptimo.	La información que viaje por medios inalámbricos deberá ser completamente confidencial debido a la sensibilidad de la información.
Infraestructura de las redes inalámbricas	Los equipos son puestos en funcionamiento cumpliendo configuraciones que deben de ser sólo modificadas por el personal autorizado.	El servicio de red se estableció con objetivos que deben de cumplirse en todo momento por lo que la disponibilidad debe de ser continua.	La infraestructura de las redes inalámbricas deben de poder ser administradas por el personal encargado de estas actividades.

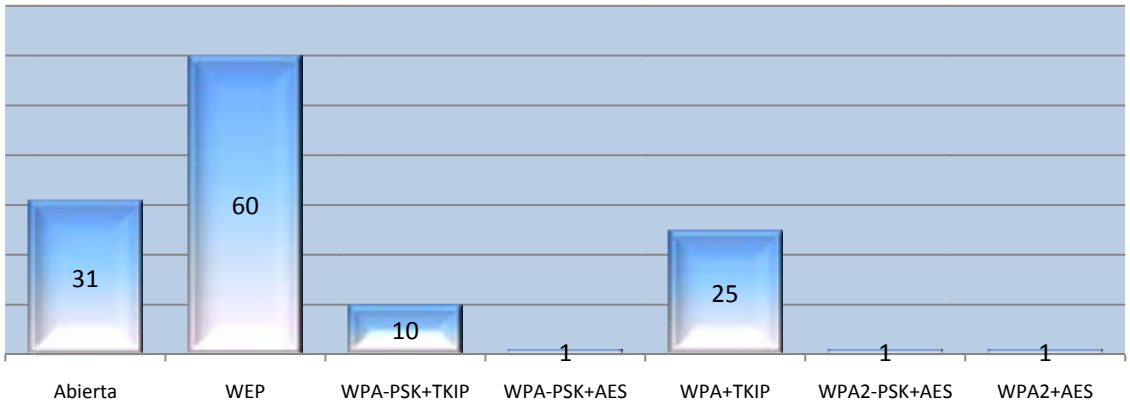
El análisis de riesgos debe ser dirigido con base a las prioridades de necesidad de protección de estos activos, la prioridad es plantear una estrategia que mitigue la situación actual que se vive en la Facultad de Ingeniería con respecto a los requerimientos de seguridad para tener controlado la proliferación de redes inalámbricas que va en aumento.

La actividad del inventario lógico de las redes inalámbricas dentro de la Facultad de Ingeniería permite visualizar **la actualidad de uso de comunicaciones inalámbricas así como las prácticas de seguridad implementadas**, con los resultados es posible hacer un análisis para establecer la estrategia a seguir para hacer que la utilización de los recursos institucionales se haga de manera responsable, considerando que una red inalámbrica mal configurada es una puerta a posibles ataques o intrusiones hacia los activos críticos ya descritos. Los resultados que se obtuvieron son los siguientes:

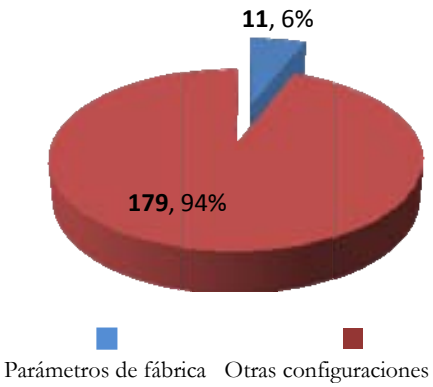
MÉTODOS DE CIFRADO DETECTADOS EN EL CONJUNTO SUR



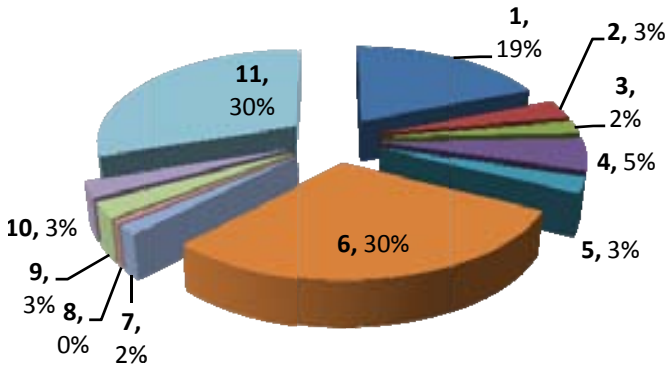
MÉTODOS DE CIFRADO DETECTADOS EN EL CONJUNTO NORTE



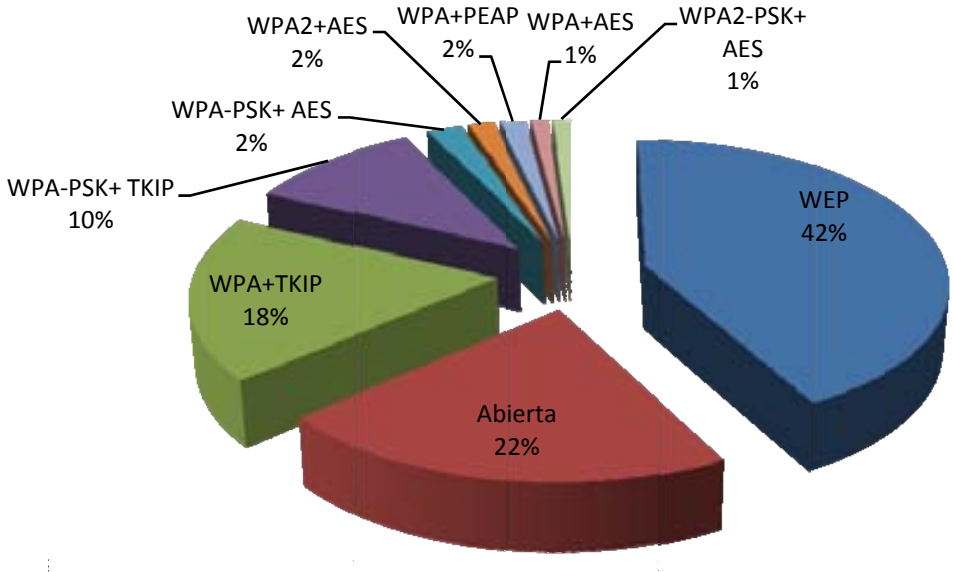
REDES CON PARÁMETROS DE FÁBRICA EN LA FACULTAD DE INGENIERÍA



USO DE LOS CANALES DE COMUNICACIÓN INALÁMBRICA EN LA FACULTAD DE INGENIERÍA



MÉTODOS DE CIFRADO IMPLEMENTADOS EN LA FACULTAD DE INGENIERÍA



- El 22% de las redes detectadas no implementan ninguna medida de seguridad de acceso a la red, lo que implica que cualquier persona con una tarjeta de red inalámbrica puede conectarse a ellas y estar dentro de la red institucional o en redes locales en donde se comparte información de diversas índoles.
- Así mismo, el 42% de las redes inalámbricas implementan el protocolo de cifrado WEP, que como se mencionó en el Capítulo II en el tema de Inseguridad, es un protocolo de cifrado muy fácil de vulnerar y no representa garantía de seguridad en la red inalámbrica.
- Se detecto un 6 % de redes inalámbricas que presentan las configuraciones de fábrica en los puntos de acceso y esto puede ser utilizado por intrusos que conozcan estos dispositivos y los utilicen para vulnerar la red institucional.
- La implementación de redes inalámbricas dentro de la Facultad no está controlada en ningún aspecto y sin el conocimiento del personal encargado de la administración de la red de la Facultad.
- El uso de los canales de comunicación está saturado y sin control alguno. El solapamiento de las redes inalámbricas afecta directamente a su funcionamiento que puede llegar hasta causar la interrupción en el servicio.

Las conclusiones que se obtuvieron son razones muy poderosas para elaborar un plan de mitigación de los riesgos actuales que corren los activos de la Facultad de Ingeniería. Este plan de protección deberá ser desarrollado con base a estas amenazas encontradas en la actividad del inventario lógico de redes inalámbricas dentro de la Facultad de Ingeniería y en este análisis de riesgos.

TABLA 3.4 Activo crítico, Amenazas y Vulnerabilidades

ACTIVO CRÍTICO	AMENAZAS	VULNERABILIDADES
Información transmitida por las redes inalámbricas	Qué los intrusos se aprovechen de la naturaleza del medio de trasmisión para interceptar la información.	• Medio de transmisión. • Métodos de cifrado de datos. • Medidas de seguridad de la red.
Redes inalámbricas institucionales	Qué las redes inalámbricas representen un acceso a la red institucional. Que ocupen la red para perpetrar ataques a nuestras propias redes y sistemas o al exterior.	• Métodos de cifrado. • Control de acceso. • Medio de transmisión.
Infraestructura de red institucional	Qué los dispositivos de red sean comprometidos y modificados por intrusos de redes inalámbricas.	• Configuraciones mal establecidas. • Configuraciones de fábrica.

FASE 2. Identificar Vulnerabilidades en la Infraestructura

En esta fase se identifican los componentes de cómputo clave para obtener un panorama de que vulnerabilidades los afectan, para este caso la infraestructura de las redes inalámbricas.

Analizando la infraestructura de las redes inalámbricas dentro de la Facultad de Ingeniería se puede observar que cuando los puntos de acceso dan conexión a Internet necesariamente se conectan a la red institucional, lo que infiere directamente en la seguridad de toda la red. Cuando no se configura de manera adecuada la red inalámbrica puede ser vulnerada por intrusos y al tener un acceso a la red inalámbrica corren riesgos los sistemas de información, la información académica así como la propia infraestructura de la red. Este plan y estrategia de seguridad deberá incluir acciones a tomar para asegurar el perímetro de la red institucional.

TABLA 3.5 Componentes clave de infraestructura Vulnerabilidades

COMPONENTES CLAVE	DESCRIPCIÓN	AMENAZAS
PC / Laptops	Los equipos de cómputo que estén conectados a la red de la Facultad, así como las laptops que estén conectadas de manera inalámbrica.	• Que estos equipos sean comprometidos en sus configuraciones y funcionamiento. • Que la información que manejan sea visible a personas no autorizadas para ello. • Que se pongan en riesgo el funcionamiento de la red de la Facultad por alteraciones en sus configuraciones. • Que estos dispositivos sean utilizados de manera inadecuada violando las políticas de la institución. • Que sean utilizados como origen de ataques informáticos internos y externos.
Puntos de acceso	Los dispositivos que dan el servicio de redes inalámbricas que están conectados a la red de la Facultad.	
Servidores	Todos los equipos que dan algún servicio como correo electrónico, web, servidor de aplicaciones, etcétera que se encuentran conectados a la red de la Facultad.	
Firewalls, IDS's, Monitores de ancho de banda	Todos los componentes que brindan monitoreo y seguridad a la red de la Facultad.	
Switches	Los dispositivos que distribuyen el servicio de red dentro de la Facultad.	

FASE 3. Desarrollo de planes y estrategias de seguridad

Con la información obtenida hasta este momento se puede empezar a realizar una estrategia que permita mitigar estos problemas de seguridad y funcionamiento de las redes inalámbricas. En esta parte es donde se toman en cuenta las amenazas detectadas en las fases previas del análisis. Una vez identificadas las amenazas la estrategia deberá ser dirigida en función de estos riesgos y su prioridad de resolución.

TABLA 3.6 Amenazas y su descripción

TIPO DE AMENAZA	DESCRIPCIÓN	RESULTADO
Redes inalámbricas sin métodos de control de acceso (abiertas).	Redes inalámbricas que están dando servicio sin tener un control de quienes se conectan a la red inalámbrica, sólo es necesario tener una tarjeta de red inalámbrica para conectarse.	• Acceso • Pérdida, destrucción • Modificación • Interrupción
Configuraciones de puntos de acceso con parámetros de fábrica.	Los puntos de acceso tienen configuraciones que son de fábrica que son estándares y que un intruso las puede utilizar.	• Acceso • Pérdida, destrucción • Modificación • Interrupción
Método de cifrado WEP.	Uno de los puntos débiles de las redes inalámbricas es el método de cifrado WEP que es el más común que se implementa, este método puede ser vulnerado de manera muy rápida y sencilla por los intrusos.	• Acceso • Pérdida, destrucción • Modificación • Interrupción
Proliferación de redes inalámbricas sin control ni autorización del administrador de la red.	El no gestionar la existencia de redes inalámbricas en la misma área geográfica puede llegar a resultar un problema en la calidad del servicio que brindan, así como pueden ser utilizadas como una puerta a la red de la institución.	• Acceso • Pérdida, destrucción • Modificación • Interrupción
Saturación de los canales de comunicaciones inalámbricas.	El uso de los canales de comunicación sin control puede causar que los servicios de red inalámbrica bajen la calidad de su servicio, incluso hasta la pérdida temporal.	• Acceso • Pérdida, destrucción • Modificación • Interrupción

Tabla 3.7 Perfil de Riesgo de las Redes Inalámbricas de la Facultad de Ingeniería

ACTIVO	ACCESO	ACTOR	MOTIVO	RESULTADO	IMPACTO	PROBABILIDAD	PLAN DE MITIGACIÓN DE RIESGOS
REDES INALÁMBRICAS DE LA FACULTAD DE INGENIERÍA	Inalámbrico	Interno	Accidental	Acceso	Medio	Alta	• Elaboración de Políticas de Seguridad de redes inalámbricas. • Configuraciones de seguridad como cifrado de datos, control de acceso, servidor de autenticación, etc. • Reducción de potencia de la antena de la red.
				Modificación	Alto	Media	
				Pérdida, Destrucción	Alto	Media	
				Interrupción	Alto	Media	
			Deliberado	Acceso	Medio	Alta	• Elaboración de Políticas de Seguridad de redes inalámbricas. • Monitoreo regular de las redes inalámbricas • Auditoría de seguridad de los servicios de red inalámbrica.
				Modificación	Alto	Alta	
				Pérdida, Destrucción	Alto	Alta	
				Interrupción	Alto	Alta	
		Externo	Accidental	Acceso	Alto	Alta	• Reducción de potencia de la antena de la red inalámbrica. • Configuraciones de seguridad como cifrado de datos, control de acceso, servidor de autenticación, etc. • Monitoreo de las redes inalámbricas de la Facultad de Ingeniería.
				Modificación	Alto	Media	
				Pérdida, Destrucción	Alto	Media	
				Interrupción	Alto	Media	
			Deliberado	Acceso	Alto	Alta	• Reducción de potencia de la antena de la red inalámbrica. • Configuraciones de seguridad como cifrado de datos, control de acceso, servidor de autenticación, etc. • Monitoreo regular de las redes inalámbricas
				Modificación	Alto	Alta	
				Pérdida, Destrucción	Alto	Alta	
				Interrupción	Alto	Alta	

TABLA 3.8 Estrategia de Protección de Redes Inalámbricas para la Facultad de Ingeniería

Estrategia de Protección de Redes Inalámbricas para la Facultad de Ingeniería	
Estrategia	**Descripción**
Políticas de seguridad.	Creación de una normatividad que regule la instalación, configuración y utilización de las redes inalámbricas dentro de la Facultad de Ingeniería. Estas políticas deberán ser desarrolladas con base en el hecho de proteger las tecnologías de información de la Facultad, deberán cubrir aspectos como Políticas de Uso, Políticas de Seguridad, De la Configuración, etcétera. Una vez que sean creadas y aprobadas estas políticas deberán ser publicadas para el conocimiento de la comunidad.
Procedimiento de registro de redes inalámbricas.	Proponer un procedimiento de autorización de la instalación de las redes inalámbricas. Este procedimiento de registro deberá ser conducido por el administrador de la red y el Departamento de Seguridad en Cómputo. Tendrá como objetivo tener conocimiento de la existencia de redes inalámbricas así como de su uso. El desarrollo de este procedimiento deberá incluir que las personas que solicitan la autorización, entreguen la información relacionada con su red inalámbrica para saber que cumplen con las políticas establecidas.
Información almacenada de redes inalámbricas.	Contar con la información de las redes inalámbricas como configuraciones, direcciones IP, métodos de cifrado, localización, uso, encargado de la red, etcétera. Esta base de datos servida como registro de información para consulta en la toma de decisiones durante el proceso de autorización. Con esta información se tendrá un control de quienes están a cargo de las redes implementadas, para fincar responsabilidades en caso de algún incidente de cómputo relacionado con su red inalámbrica.
Buenas prácticas de las redes inalámbricas.	Creación de buenas prácticas para las redes inalámbricas. La responsabilidad del buen funcionamiento de las redes inalámbricas es directamente del personal encargado de sistemas en los diferentes departamentos y áreas en donde se encuentre instalada, sin embargo, la publicación de buenas prácticas de redes inalámbricas servirán como guía para un mejor funcionamiento de este tipo de servicios.
Monitoreo de redes inalámbricas.	Creación de prácticas de monitoreo de redes inalámbricas. El monitoreo de las redes inalámbricas es una práctica de seguridad que los administradores de las redes deben de utilizar de manera regular, y son ellos quienes tienen la responsabilidad directa de identificar malos usos de sus servicios de red, a menos que sea requerido el apoyo del Departamento de Seguridad en Cómputo. Es por ello que estas prácticas deberán ser tomadas en cuenta por los encargados de las redes inalámbricas.
Auditoría de redes inalámbricas.	Creación de prácticas de auditoría de redes inalámbricas. Una vez que sean publicadas las Políticas de Seguridad de Redes Inalámbricas, todos los involucrados deberán estar auditando sus equipos para saber si están cumpliendo con los lineamientos establecidos. Estas prácticas serán una ayuda a los administradores de las redes inalámbricas.
Sistema Web de gestión de redes inalámbricas.	Creación de un sistema Web que permita conjuntar todas las estrategias anteriores y que esté disponible a la comunidad de la Facultad. Este sistema Web deberá cumplir el objetivo de conjuntar información relacionada con el procedimiento de registro, Políticas de Seguridad, auditoría, monitoreo y buenas prácticas. Este sitio Web deberá presentar la información de la base de datos de manera que se obtengan su localización y configuraciones, de esta manera se tomarán decisiones de autorización en base a la información aquí presentada.
Gestión del espectro electromagnético.	Gestionar los canales de comunicación inalámbrica disponibles para el uso de redes inalámbricas y evitar solapamiento para asegurar el buen servicio. Las comunicaciones inalámbricas deben de ser planeadas antes de ser implementadas, para la toma de decisiones cuando se selecciona el canal de comunicación es necesario saber que tan congestionado se encuentra el ambiente y así elegir un canal que evite al máximo el solapamiento y la congestión de la red inalámbrica.

3.2 POLÍTICAS DE SEGURIDAD DE REDES INALÁMBRICAS

En una organización en donde se quiere tener controlado el uso de sus tecnologías de información es necesario establecer principios que declaren su buen uso y sus posibles penalizaciones en caso de no seguir con estos principios. Para ello es necesario crear un conjunto de reglas o políticas de seguridad y divulgarlas como herramienta de control de la infraestructura tecnológica, en este caso de la Facultad de Ingeniería.

Una política de seguridad es un conjunto de documentos en donde se detallan las reglas de seguridad en cómputo para una organización. Tienen como objetivo informar al personal de la organización (generalmente todas las áreas) las normas y mecanismos que se deben cumplir y poner en práctica para proteger los recursos tecnológicos y la información de la organización.

Las necesidades de la organización y el análisis de riesgos son las principales directrices en la creación de las políticas de seguridad. El documento general que especifique las políticas de seguridad debe de estar formado por tres documentos diferentes:

- Políticas. Elemento esencial de las políticas de seguridad y que generalmente no son tecnológicamente especificas y tienen repercusiones más amplias sobre los aspectos relacionados con la red.
- Guías de uso. Mejores prácticas de la organización.
- Procedimientos. El conjunto mínimo de criterios de operaciones de ciertas tecnologías o activos.

FIGURA 3.7 Ciclo de vida de la Seguridad

Las políticas de seguridad tienen un ciclo de vida en donde se desarrollan varias etapas como lo son de investigación, elaboración, aprobación, divulgación, aceptación por parte de los usuarios finales, darles seguimiento, actualización y como etapa final la eliminación cuando haya quedado obsoleta. Cuando

alguna de estas etapas no se lleva a cabo queda la posibilidad de que no se tomen como válidas estas políticas.

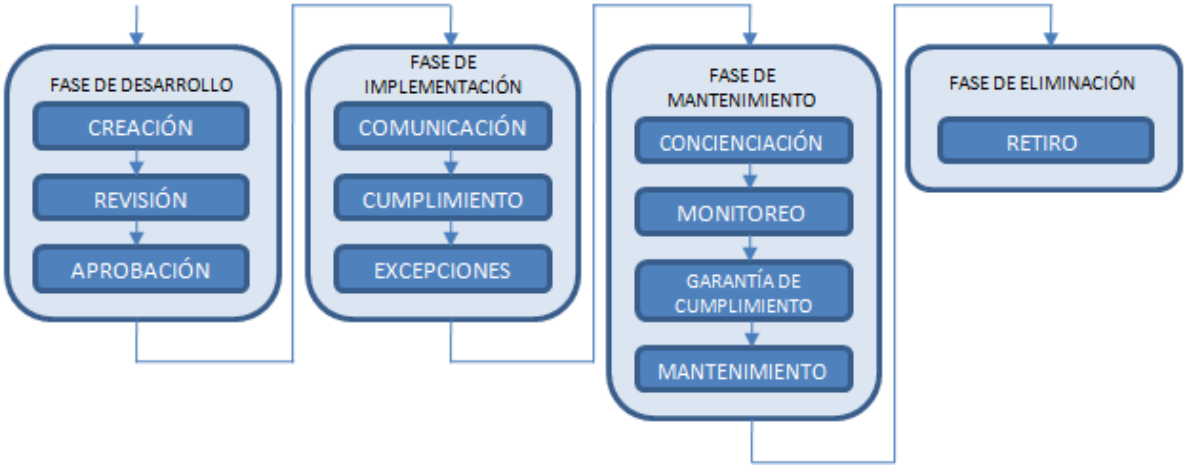


FIGURA 3.8 Ciclo de vida de una política de seguridad

3.2.1 NECESIDADES

Como ya se mencionó anteriormente las necesidades de la organización es una de las dos directrices en el desarrollo de las políticas de seguridad, el impacto de estas necesidades que tienen sobre las políticas de seguridad recaen en:

- Objetivos de la organización

Los objetivos de la organización se deben de entender y tener una plena comprensión de ellos para poder diseñar políticas de seguridad. En este caso los objetivos de la Facultad de Ingeniería que se tienen con respecto a las Tecnologías de Información será lo que marque la dirección para la creación de las políticas de seguridad en las redes inalámbricas de la Facultad, además se debe de conocer el papel y funciones que deben de cumplir los servicios tecnológicos que ofrece la institución.

Entender la relación entre el costo y el beneficio de aplicar políticas de seguridad también arroja herramientas necesarias para la elaboración de políticas que cumplan con las necesidades de la organización, se debe de comprender el costo asociado a los incidentes de seguridad para poder considerar el costo de mitigación de la amenaza, a partir de esta información se podrá hacer el análisis costo/beneficio.

El desarrollo de políticas de seguridad es una tarea en donde se debe de involucrar miembros de diferentes áreas como puede ser un representante del nivel directivo, un miembro del personal jurídico, miembro de la comunidad de usuarios y obviamente personal encargado de la seguridad en cómputo de la organización, en la creación de las políticas se debe de tener una visión amplia que cubra las necesidades a todos los niveles.

Las políticas desarrolladas cubrirán las necesidades de la institución de tener regulaciones legales y técnicas, además servirán como guía para el comportamiento profesional y personal de la comunidad, cubrirán la necesidad de unificar la forma de trabajo de personas en diferentes lugares o momentos que tengan responsabilidades y tareas similares, además de asociar la filosofía de la institución al trabajo.

3.2.2 POLÍTICAS PARA REDES INALÁMBRICAS PARA LA FACULTAD DE INGENIERÍA

A continuación se presentan las Políticas de Seguridad para Redes Inalámbricas en la Facultad de Ingeniería, estas políticas son una propuesta del Departamento de Seguridad en Cómputo de la Facultad de Ingeniería.

Políticas de Seguridad para Redes Inalámbricas en la Facultad de Ingeniería

Objetivo

Definir las políticas relacionadas con la instalación de equipos inalámbricos a la red de la Facultad de Ingeniería y establecer los procedimientos para su instalación, administración y configuración.

Metas:

- **Mantener la integridad y confidencialidad de la información y de la infraestructura de la red.**
- **Establecer normas para la instalación de antenas externas para uso con equipos de red inalámbricos.**
- **Prevenir la interferencia con otros usuarios que utilicen el mismo espectro de frecuencias**.

El mantenimiento de la seguridad e integridad de la red de la Facultad requiere de medios adecuados para asegurar que solamente los usuarios autorizados puedan hacer uso de ella. Los dispositivos de red inalámbricos que utilizan la infraestructura de la red, deben de cumplir con ciertas normas para que solamente usuarios autorizados y autentificados se puedan conectar y que dichos dispositivos no queden expuestos.

Ámbito de aplicación

Estas políticas deberán ser observadas por todos los miembros de la Facultad de Ingeniería, ya sea a nivel individual (estudiantes, investigadores, personal de apoyo, personal administrativo, personal directivo, personal vinculado a proyectos de investigación, etcétera) o colectivo (Centros, Institutos, Departamentos, Grupos, etcétera). También se aplicará a cualquier otra entidad externa que utilice los recursos informáticos de la institución.

Definiciones

- Comité Asesor de Cómputo de la Facultad de Ingeniería: Esta responsabilidad será del Comité de Cómputo de la Facultad de Ingeniería.

- Responsable de la Administración de Red: Es el encargado de la administración y operación de la red institucional. En la Facultad de Ingeniería es el jefe del Departamento de Redes y Operación de Servidores (DROS) adscrito a la Unidad de Servicios de Cómputo Académico (UNICA).

- Responsable de la Seguridad: Es el encargado de dirigir las medidas y acciones para hacer cumplir esta política, así como de su interpretación, control de cumplimiento y resolución de los problemas relativos a la misma. En la Facultad de Ingeniería es el jefe el Departamento de

Seguridad en Cómputo (DSC) adscrito a la Unidad de Servicios de Cómputo Académico (UNICA).

- Responsable de cómputo del área, coordinación, secretaría o división: Es el responsable de los equipos de cómputo que hayan sido instalados en un área, coordinación secretaría o división dentro la Facultad de Ingeniería, esta responsabilidad se limita a autorizar la instalación de los mismos, quien puede utilizarlos y que uso se hace de ellos. Normalmente el responsable de cómputo es el director o jefe del área.

- Administrador de Sistemas: Es el responsable de la gestión y la administración de los equipos de cómputo, responsable de supervisar el cumplimiento de la política de seguridad de los mismos. Será normalmente el encargado de los sistemas tecnológicos de las áreas.

- Usuarios: Toda persona que utilice los recursos de redes inalámbricas de la Facultad de Ingeniería.

- Dispositivo inalámbrico de red: Se entiende como un equipo que permite acceder de forma inalámbrica a la red de datos de la Facultad de Ingeniería. Los dispositivos inalámbricos de red pueden ser de varios tipos:
  - Punto de acceso *(access point)*. Actúa como *Hub* inalámbrico al cual se conectan computadoras.
  - Tarjetas inalámbricas para computadora. Permiten a una computadora conectarse a un punto de acceso.
  - Antena. Dispositivo diseñado para emitir y recibir ondas electromagnéticas.

- Cobertura: área geográfica donde la señal de la red inalámbrica se puede obtener.

- Interferencia: degradación de la señal causada por la radiación electromagnética de otro dispositivo. La interferencia puede causar que la velocidad de transmisión/recepción de datos y/o perdida de la señal.

- Dirección MAC (*Control de Acceso al Medio*): número de seis octetos que identifica el equipo que va a ser utilizado en la red inalámbrica.

- Dirección IP (*Internet Protocol*): número que identifica de manera lógica un dispositivo dentro de una red que utilice el protocolo de Internet (IP).

- SSID (*Service Set Identifier*): Identificador que trasmiten los puntos de acceso referente al nombre dado a la red inalámbrica para identificar el servicio.

Introducción

En este documento se plantea la normatividad para regular el buen uso, disponibilidad y nivel de servicio de los recursos de redes inalámbricas de la Facultad de Ingeniera. El uso de estos recursos inalámbricos deberá respetar los fines con los que fue instalada, evitar la interrupción de los servicios que ofrece o de otros equipos que forman parte de la infraestructura de red, así mismo evitar situaciones que afectan la seguridad de la información y de los usuarios.

El Departamento de Seguridad en Cómputo podrá modificar estas Políticas de Seguridad y Uso de las Redes Inalámbricas en cualquier momento cuando se considere necesario y es responsabilidad de los

usuarios asegurarse del conocimiento de tales cambios. Estas políticas por tal motivo estarán publicadas en Internet para consulta en cualquier momento. Así mismo este documento es un complemento de las Políticas de Seguridad en Cómputo para la Facultad de Ingeniería.

Aquellas personas que ignoren esta normativa de forma reiterada, deliberada, por negligencia o las infrinjan se podrán ver sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) o disciplinarias que se estimen oportunas. En cualquier caso será responsabilidad de los jefes de área, coordinación, secretaría o división; dar la difusión necesaria a esta política para que sea conocida por todos los agentes a los que se aplica. Las sanciones serán emitidas por el responsable de la Secretaría General en caso de ser requeridas.

Políticas de Uso

- Nadie está autorizado a instalar dispositivos inalámbricos de red, sin el visto bueno del administrador de red y previa autorización del responsable del área, coordinación, secretaría o división. Cuando se detecte un equipo instalado sin cumplir lo anterior se procederá a deshabilitar el puerto del switch en donde se detecte, independientemente si existen otros equipos de red conectados a ese puerto.
- Todos los "puntos de acceso" que vayan a ser instalados deberán ser registrados y autorizados por el Departamento de Redes y Operación de Servidores y el Departamento de Seguridad en Cómputo siguiendo el ***Procedimiento de Registro de Redes Inalámbricas*** que se describe al final de este documento.
- Los dispositivos inalámbricos de red están sujetos a las mismas reglas y políticas que se aplican a otros dispositivos electrónicos de comunicación por red de la Facultad de Ingeniería.
- El abuso o interferencia de los canales de comunicación inalámbrica con otras actividades que no sean las establecidas es una violación al uso aceptable. La interferencia o disrupción de otras comunicaciones autorizadas o la intercepción de otros tipos de tráficos constituyen una violación a las políticas.
- Si se requiere una red inalámbrica para laboratorios de redes dedicadas a pruebas y experimentación de los diversos protocolos y estándares, ésta deberá instalarse de forma autónoma e independiente y totalmente desconectada de la red de la Facultad, respetando en todos los casos el espacio radioeléctrico de las redes inalámbricas ya existentes y la previa autorización del Departamento de Redes y Operación de Servidores.
- (Disposición transitoria) Los puntos de acceso existentes e instalados por los usuarios, anteriores a la publicación de estas políticas, serán sustituidos o reconfigurados para su integración en la plataforma de gestión actual y al amparo de esta normativa.

Políticas Sobre la Seguridad

El mantenimiento de la seguridad e integridad de la infraestructura de redes inalámbricas de la Facultad de Ingeniería requiere de métodos que aseguren que sólo los usuarios autorizados puedan tener acceso al mismo. De esta manera, el equipo debe tener las medidas de seguridad necesarias para evitar que se vean afectados los servicios de la red inalámbrica.

- La instalación y configuración de los puntos de acceso deberá ser realizada por personal capacitado con los conocimientos técnicos necesarios, además se deberán modificar los parámetros establecidos por el fabricante del dispositivo para evitar que cualquier individuo tenga acceso a los mismos.
- Los puntos de acceso de las redes inalámbricas deberán contar con las últimas actualizaciones de su *firmware* antes de ser puestos en operación. Una vez que hayan iniciado su uso, también se

deberá de estar actualizando de manera constante con las últimas versiones del *firmware* que llegaran a liberarse.

- Una vez configurado el punto de acceso se deberán deshabilitar las formas de administración que no se vayan a ocupar, por ejemplo la administración vía página Web, etcétera.
- Las contraseñas de los puntos de acceso deberán de ser lo más robustas posibles, ocupando un mínimo de 8 caracteres en una combinación de caracteres alfanuméricos y caracteres especiales. Estas contraseñas sólo serán conocidas por el encargado de la red inalámbrica. Estas contraseñas deberán ser cambiadas como mínimo cada dos meses.
- El SSID de la red inalámbrica deberá de estar oculto al conocimiento público (No *Broadcast*), en caso de ser necesaria la publicación del SSID de red, esta situación se informará durante el procedimiento de registro de la red inalámbrica.
- Ningún individuo debe conectar ni instalar equipo de acceso inalámbrico sin la previa autorización del responsable del área, coordinación, secretaría o división.
- El equipo deberá ser configurado de manera que minimice la interferencia con otros equipos de radiofrecuencia que se encuentren en la misma zona, cuidando que los canales de comunicación no se solapen. Esta información será proporcionada por el administrador de la red durante el procedimiento de registro de red inalámbrica y estará fundamentada en los registros que se tengan de redes inalámbricas en la zona.
- Las redes inalámbricas deberán ser implementadas en segmentos de red diferentes al de la red cableada, es decir se deberán implementar redes virtuales con direcciones IP no homologadas para las redes inalámbricas, queda prohibida la utilización de direcciones IP homologadas para asignar de manera dinámica y estática en una red inalámbrica.
- Los "puntos de acceso" no podrán ser administrados por los clientes inalámbricos. Toda administración de los "puntos de acceso" se realizará por medio de la red cableada.
- Cuando se cuente con una antena externa conectada al punto de acceso, se deberá reducir la potencia de transmisión para sólo cubrir el área en la cual se necesita el servicio de red inalámbrica.

Sobre la Confidencialidad

- Las comunicaciones inalámbricas no proveen un mecanismo de codificación de los datos transmitidos confiable al cien por ciento. La protección de los datos es responsabilidad del usuario y de la aplicación que utilice para transmitir los datos.
- Las redes inalámbricas no deben de ser utilizadas como medio de transmisión de datos para información sensible ya que esta puede ser monitoreada por intrusos, por lo que no se deben de utilizar para transmitir información de servicios críticos o que busquen la alta disponibilidad.
- Los usuarios que trabajen con información confidencial, deben utilizar software que utilice algoritmos de cifrado confiables, por ejemplo: SSL (*Secure Socket Layer*), S*ecure Shell, IPSEC, VPN's* entre otros.
- Las redes inalámbricas existentes en la Facultad de Ingeniería deberán implementar como mínimo el método de cifrado de datos WPA.
- Cuando se implementen métodos de cifrado con llave compartida, estas claves deberán de ser conocidas únicamente por el administrador de sistemas. Deberán ser cambiadas como mínimo cada dos meses y en caso de que un usuario no permitido tenga acceso a esta llave deberán cambiarse inmediatamente para asegurar que sólo el administrador de sistemas la conozca.

Sobre el Control de Acceso

- Una manera de minimizar riegos de accesos no autorizados a la red, es mediante el uso de control de acceso en los AP's, estos dispositivos deberán implementar filtros de direcciones MAC de los dispositivos clientes que tengan permitido el uso de la red inalámbrica, sin embargo la implementación de este método de control de acceso presenta vulnerabilidades, no obstante representa un control administrativo de los clientes que utilizan la red.
- No deberán de existir redes inalámbricas que sean de tipo abiertas, es decir que no tengan un mecanismo de autenticación.

Sobre la Disponibilidad e Integridad

- La disponibilidad de los servicios inalámbricos ofrecidos a la comunidad es responsabilidad del administrador de sistemas así como del responsable de cómputo del área a que pertenece esta red inalámbrica.
- Se recomienda la instalación de Firewalls para filtrar tráfico de red y direcciones IP dentro de la red inalámbrica, esto para asegurar que sólo pase tráfico de red permitido a la red cableada.

Sobre la seguridad física de la infraestructura de red

- El equipo debe ser protegido con medidas de seguridad física para prevenir el robo o acceso no autorizado a los dispositivos.
- Los puntos de acceso deberán estar localizados en un área accesible en donde se les pueda dar mantenimiento y puedan ser configurados sin impedimentos.
- Los puntos de acceso deberán ser colocados alejados de fuentes de interferencias como lo pueden ser hornos de microondas, antenas de radiofrecuencia, entre otros. Para cuando se coloquen al aire libre deberán contar con una protección contra agua, radiación solar, etcétera.

Sobre la Interferencia

- El funcionamiento correcto de una instalación inalámbrica que cubre edificios completos o áreas más amplias, requiere que todo el equipo esté correctamente instalado y configurado para evitar interferencias entre los componentes de otros segmentos de red o entre otros equipos.
- El administrador de red de la Facultad de Ingeniería es el encargado de regular y administrar la configuración de las frecuencias.
- Las interferencias que pudieran resultar serán resueltas por el administrador de la red de acuerdo a las prioridades de equipo de acceso inalámbrico, las cuales son las siguientes: investigación, de académica, administración, y acceso a alumnos.
- El Departamento de Redes y Operación de Servidores responderá a reportes de equipos que puedan estar causando interferencia y de no resolverse la situación, el uso del equipo sospechoso puede ser restringido o retirado.

Sobre el Monitoreo

- Como medida de seguridad y rendimiento de la red inalámbrica se recomienda al área encargada de esa red inalámbrica hacer la solicitud al Departamento de Seguridad en Cómputo para monitorear de manera periódica la red inalámbrica.
- En las redes inalámbricas existentes en donde se asigne IP mediante el protocolo DHCP se deberán de almacenar bitácoras de asignación de direcciones.

- El Departamento de Seguridad en Cómputo tiene la autorización para monitorear las redes inalámbricas cuando se tengan indicios de incidentes o le sea reportada actividad intrusiva sobre la red.

Sobre la Auditoría

- Toda la infraestructura de redes inalámbricas está sujeta a auditorías periódicas realizadas por el DSC para prevenir uso no autorizado y violaciones a las políticas de seguridad, para prevenir actividad intrusiva y otros propósitos similares.

Sobre las Responsabilidades de los Responsables de Cómputo del Área, Coordinación, Secretaría o División

- Los responsables de cómputo del área, coordinación, secretaría o división deberán de autorizar la implementación de redes inalámbricas en sus respectivas áreas.

Sobre las Responsabilidades de los Administradores de Sistemas

- Todas las redes inalámbricas que se pretendan instalar deberán seguir el Procedimiento de Registro de Redes Inalámbricas para la Facultad de Ingeniería.
- Los administradores de sistemas deberán llevar un registro de las tarjetas de comunicación inalámbrica que se utilicen en su red inalámbrica.
- Los administradores de sistemas deberán informar a los usuarios de su red inalámbrica sobre la seguridad, las políticas y procedimientos relacionados al uso de las comunicaciones inalámbricas en la institución.
- Informar al DSC en caso que se requiera la ayuda para la solución de algún incidente de seguridad.

Sobre la Responsabilidad del Administrador de la Red

- Mantener un registro de todas las tarjetas y equipos inalámbricos de la Facultad de Ingeniería.
- Resolver los problemas de interferencia en la comunicación.
- Informar a los usuarios de sistemas inalámbricos sobre las políticas de privacidad y seguridad relacionados con el uso de comunicaciones inalámbricas.
- Resolver cualquier caso no previsto.

Sobre la Responsabilidad del Departamento de Seguridad en Cómputo

- Crear, mantener y actualizar las políticas y las buenas prácticas de seguridad.
- Monitorear la seguridad y los posibles conflictos de redes inalámbricas en las áreas comunes.
- Verificar el cumplimiento de la presente normatividad a través de auditorías y revisiones periódicas.
- Atender los reportes de incidentes de cómputo que hayan sido notificados en las redes inalámbricas existentes.

Sobre el mal uso de los recursos

- El DSC – DROS podrán suspender o desconectar los servicios de red inalámbrica de manera temporal o definitiva según la falta que se haya cometido con el único propósito de dar certidumbre y continuidad a los demás servicios ofrecidos por la institución.

PROCEDIMIENTO DE REGISTRO DE RED INALÁMBRICA DENTRO DE LA FACULTAD DE INGENIERÍA

Con la finalizad de gestionar las Tecnologías de Información inalámbrica de la Facultad de Ingeniería se ha establecido un procedimiento de registro de las redes inalámbricas existentes. La instalación de nuevas redes inalámbricas dentro de la Facultad de Ingeniería requiere de una serie de pasos a seguir para que sea registrada por el Departamento de Redes y Operación de Servidores y el Departamento de Seguridad en Cómputo de la Facultad, este procedimiento permitirá tener conocimiento de la existencia de las redes inalámbricas.

El procedimiento de registro de redes inalámbricas permitirá asegurar que la infraestructura de comunicaciones inalámbricas sea homogénea y uniforme para evitar riesgos de seguridad.

1. Una vez obtenida la autorización del responsable del área, coordinación, secretaría o división para la implementación de la red inalámbrica: acceder al sitio Web Gestión de Redes Inalámbricas de la Facultad de Ingeniería (GRIFI) en la parte de Procedimiento de Registro y descargar el documento que contiene la información solicitada para el registro, para posteriormente llenarlo de manera manual.
2. La solicitud de registro se deberá entregar al encargado de la administración de la red para ser revisado.
3. El administrador de la red una vez que haya revisado el documento de registro, resolverá si se registra o no la red inalámbrica. En caso afirmativo la información será enviada al Departamento de Seguridad en Cómputo para ser registrada en la base de datos de las redes inalámbricas, así mismo se le informará al responsable de la solicitud que ha sido registrada la red inalámbrica. Por lo contrario, cuando algún dato de la red inalámbrica deba de ser modificado se deberá informar de igual manera al responsable de la solicitud para que haga la o las correcciones correspondientes y reiniciar el procedimiento.

Una vez que el DSC tiene la información de la red inalámbrica esta podrá ser consultada en el sitio Web donde se tiene la aplicación de visualización de las redes inalámbricas en la Facultad de Ingeniería siempre y cuando se disponga de una cuenta de acceso al sistema.

FORMATO DE SOLICITUD DE REGISTRO DE RED INALÁMBRICA
FACULTAD DE INGENIERÍA

INFORMACIÓN DEL RESPONSABLE O CONTACTO TÉCNICO DEL EQUIPO

Nombre : _____

División a la que pertenece: _____

Departamento al que pertenece: _____

Puesto que desempeña: _____

Correo Electrónico: _____Tel/Ext._____

INFORMACIÓN DEL EQUIPO (PUNTO DE ACCESO)

Fabricante:_____ Modelo: _____

Dirección MAC:_____ Tipo de Antena: _____

Nombre del Equipo: _____ Alcance: _____

Estándares en que funcionará: _____802.11a _____802.11b _____802.11g

PÁRAMETROS DE LA RED INALÁMBRICA

SSID de red:_____
(Max.15 Caracteres)

Canal(es) propuesto para funcionar: _____

Envía SSID por broadcast: Sí No

CONEXIÓN DEL PUNTO DE ACCESO

Uso de la red inalámbrica:

Acceso a la red Investigación Intranet Otro uso

IP del punto de acceso: _____ IP del Gateway del punto de acceso:_____

Máscara de red:_____

CONTROL DE ACCESO Y SEGURIDAD

Utiliza filtrado MAC: Sí No Utiliza DHCP: Si No

Utiliza servidor de autenticación Sí No Utiliza IPSec Sí No

Método de cifrado: WEP WPA-MIXED PSK-MIXED Otro
WPA+TKIP WPA-PSK+TKIP WPA2+TKIP WPA2-PSK+TKIP
WPA+AES WPA-PSK+AES WPA2+AES WPA2-PSK+AES

Mecanismo de autenticación: EAP EAP-FAST EAP-TLS EAP+TTLS
PEAP LEAP OTRO NINGUNO

Configuración del AP: Consola WEB SNMP Otra

OTRA INFORMACIÓN

Tipo de usuarios de la red inalámbrica: Alumnos Académicos Investigadores Administrativos

Bitácoras de asignación de IP's: Sí No

Observaciones:

CAPÍTULO

4

HERRAMIENTA DE GESTIÓN DE REDES INALÁMBRICAS

Como parte de la estrategia propuesta se encuentra el desarrollo de un sistema Web que permita centralizar la información referente a las redes inalámbricas dentro de la Facultad de Ingeniería, en este capítulo se presenta el análisis, diseño e implementación de dicha herramienta.

4. HERRAMIENTA DE GESTIÓN DE REDES INALÁMBRICAS

La herramienta de gestión de redes inalámbricas permitirá contar con la información y el estado actual de las redes inalámbricas existentes de la Facultad de Ingeniería, será el medio de comunicación para publicación de las políticas además de contar con una plataforma que presentará la información necesaria para gestionarlas, tal como lo es el monitoreo, la auditoría y las buenas prácticas.

Esta herramienta será un desarrollo Web de forma tal que pueda ser accedida desde cualquier computadora conectada a Internet.

4.1 DEFINICIÓN DE OBJETIVOS

Los objetivos que persigue este desarrollo son los siguientes:

- Contar con una aplicación que ayude a la gestión de las redes inalámbricas existentes en la Facultad de Ingeniería, en donde se tenga una base de datos con la información referente a las mismas.
- Contar con una herramienta Web que muestre las políticas sobre las redes inalámbricas.
- Contar con una herramienta en línea que permita llevar a cabo el procedimiento de alta, baja o modificación de una nueva red inalámbrica.

- Tener un sitio Web que permita dar a conocer técnicas y procedimientos para gestionar redes inalámbricas. Esta herramienta deberá presentar información de auditoría, monitoreo y además de buenas prácticas en redes inalámbricas.
- Contar con una herramienta en línea que muestre estadísticas y resultados sobre la gestión de las redes inalámbricas.

4.2 NECESIDADES

Actualmente en la Facultad de Ingeniería existe una gran variedad de servicios de red inalámbricos que son habilitados con propósitos de diversas índoles, tales como investigación, laboratorios de pruebas, acceso a la Red Inalámbrica Universitaria (RIU), entre otros; dichas redes son una extensión a la infraestructura de red de la Facultad de Ingeniería por lo que deben de ser gestionados de la mejor manera posible. Sin embargo en el análisis de riesgos hecho con anterioridad, se demostró que muchas de ellas están funcionando bajo configuraciones inadecuadas que pueden ser aprovechas por usuarios no autorizados y hacer mal uso de ellas.

Es por ello que surge la necesidad de contar con un control de las redes inalámbricas lo que le permitirá a los departamentos encargados de la administración y de la seguridad de la red de la Facultad de Ingeniería contar con una herramienta que sea capaz de identificar los puntos de acceso inalámbricos, así como reducir el tiempo de respuesta a incidentes en caso de contingencias.

El sitio deberá de cumplir también una función informativa, los procedimientos de registro y las políticas de las redes inalámbricas deberán estar públicados, por lo que el mecanismo principal de difusión será el sitio Web.

Actualmente no se cuenta con la información necesaria y suficiente de un registro de redes inalámbricas existentes dentro de la Facultad de Ingeniería, así como también se carece de información relacionada a los responsables de su administración. En estos momentos si se llegara a presentar alguna falla de la red o algún incidente de cómputo provocado por accesos establecidos de manera inalámbrica dentro de la institución no se contaría con la evidencia suficiente para atender con prontitud un incidente, o para establecer las debidas responsabilidades y emitir sanción correspondiente a la falta.

Este sistema Web deberá permitir obtener información de manera rápida y eficiente, datos como quién está a cargo de la red inalámbrica, sus configuraciones de red cómo lo son dirección IP y dirección de Gateway, información de la red inalámbrica cómo su SSID, bajo qué canal inalámbrico funciona y qué tipo de antena utiliza, así como información de configuraciones de seguridad implementadas añadiendo la localización física del punto de acceso.

La gestión de cualquier recurso de Tecnologías de Información involucra una serie de actividades que deben de ser completadas como parte del proceso de gestión, la auditoría y monitoreo deberá ser parte fundamental de la estrategia de gestión de redes inalámbricas dentro de la Facultad de Ingeniería.

La aplicación que se desarrollará deberá ser capaz de administrarse de manera centralizada y contar con la capacidad de manejar diferentes perfiles de usuarios, con el fin de dar la posibilidad de que sólo los usuarios autorizados cuenten con esta información que resultaría muy valiosa para posibles intrusos. Por el contrario información como el procedimiento de registro, las políticas de redes inalámbricas, la información de monitoreo, auditoría y buenas prácticas deberán ser visibles a los usuarios en general.

4.2.1 NECESIDADES DEL SISTEMA

La primera etapa del desarrollo de cualquier aplicación es entender las necesidades del sistema así como las de sus involucrados. Se debe de averiguar cómo es que el sistema debe de funcionar para entenderlo, mediante la tarea de recopilar la mayor cantidad de información que se pueda obtener. Así mismo es trascendental identificar las necesidades y priorizarlas ya que no todos los requerimientos son igualmente importantes para el funcionamiento de la aplicación.

TABLA 4.1 Necesidades y principales involucrados del sistema

NECESIDAD	PRIORIDAD	PREOCUPACIONES	SITUACIÓN ACTUAL	SOLUCION PROPUESTA
Gestión de redes inalámbricas.	**ALTA**	La proliferación de las redes inalámbricas dentro de la Facultad de Ingeniería sin control alguno resulta en una variedad de incidentes de cómputo cómo: • Alteración de información crítica que está disponible o que viaja sobre la red de datos. • Acceso a servicios o documentación de carácter privada. • Intermitencias o hasta suspensiones temporales del servicio de red. • En el caso de incidentes de cómputo, no contar con la información necesaria para mitigar el problema con la mayor rapidez y eficiencia posible.	En la Facultad de Ingeniería se sabe que existe una gran variedad de áreas en donde se cuenta con acceso a la red de manera inalámbrica en diferentes dependencias de la institución. Sin embargo, no se tiene un registro de quien está a cargo de la red inalámbrica, bajo qué condiciones se encuentra operando, etcétera.	• El sistema de gestión de redes inalámbricas deberá almacenar la información correspondiente a las redes inalámbricas existentes dentro de la Facultad de Ingeniería. Información como quién está a cargo de la red, dirección IP, localización, métodos de seguridad implementados, etcétera.
Políticas de redes inalámbricas.	**ALTA**	• Instalación de puntos de acceso bajo ninguna medida de seguridad, administración, etcétera. • Implementación de redes inalámbricas con las configuraciones de fábrica en los puntos de acceso. • No hay responsables de la red inalámbrica en caso de que se presenten incidentes de seguridad. • Uso indebido de los recursos de red de la Facultad de Ingeniería.	No existe actualmente una normatividad sobre la instalación, configuración, seguridad y administración de las redes inalámbricas de la Facultad de Ingeniería por lo que se hace necesaria la creación de políticas de redes inalámbricas así como su difusión.	• Este trabajo contempla la creación de políticas de redes inalámbricas que ya se propusieron en el capítulo 3. Una vez creadas es importante que la herramienta Web sirva como un mecanismo de difusión a la comunidad para su conocimiento.
Procedimiento de registro de redes inalámbricas.	**ALTA**	• Aparición de redes inalámbricas para usos no autorizados de la red. • Cualquier persona con acceso a un nodo de red puede implementar una red inalámbrica sin tener una autorización previa. • Desconocer cómo está conformada la infraestructura de red de la Facultad de Ingeniería.	Como resultado de la falta de un procedimiento de autorización para implementar redes inalámbricas con recursos de la Facultad cualquier persona con acceso a la red de la institución podrá crear su propia red inalámbrica sin que el Departamento de Redes y Operación de Servidores y el Departamento de Seguridad en Cómputo tengan conocimiento de ello.	• Crear un procedimiento de registro de redes inalámbricas dentro de la Facultad de Ingeniería que permita validar el uso adecuado de la red y controlar los parámetros de redes inalámbricas así como de seguridad en cómputo establecidos por las políticas de redes inalámbricas.
Mapa de localización de redes inalámbricas.	**ALTA**	• Desconocer la ubicación física de los puntos de acceso de las redes inalámbricas. • Ubicar varias redes inalámbricas dentro de una misma área geográfica funcionando en los mismos canales de comunicación. • Saturación del medio de transmisión en una zona.	El crecimiento de las redes inalámbricas dentro de la Facultad genera que existan diferentes redes de este tipo dentro de una misma área lo que da como resultado que la calidad del servicio se vea disminuida.	• El sistema Web deberá localizar las redes inalámbricas existentes en la base de datos en una mapa que permita ubicar los puntos de acceso dentro de la Facultad de Ingeniería
Perfiles de usuarios para el sistema Web.	**MEDIA**	• Que el desarrollo Web sea utilizado por usuarios no permitidos y obtengan información de la existencia de redes inalámbricas dentro de la Facultad de	No aplica en este caso.	• El sitio Web deberá manejar perfiles de usuarios en base al rol que maneje dentro del sistema.

		Ingeniería así como de sus configuraciones de seguridad y por ende las posibles vulnerabilidades de seguridad.		• El uso de sesiones deberá implementarse como medida de seguridad de la información que maneje el sitio.
Buenas prácticas de redes inalámbricas.	**MEDIA**	• Intrusiones a la red institucional debido a configuraciones de fábrica que se dejan en los puntos de acceso. • Malas configuraciones de dispositivos de red inalámbrica que lleguen a provocar fallas en los servicios de red.	Después de haber realizado el inventario lógico de redes inalámbricas dentro de la Facultad de Ingeniería se detectaron redes inalámbricas con configuraciones que vienen de fábrica en los puntos de acceso o en algunos casos redes que funcionan sin medidas de control de acceso.	• Se deberá establecer dentro del desarrollo Web una zona en donde se toquen temas de buenas prácticas en las redes inalámbricas, esta información deberá ser visible a los usuarios en general.
Auditoría de las redes inalámbricas.	**MEDIA**	• Que las redes inalámbricas existentes en la Facultad de Ingeniería no estén cumpliendo con las políticas de uso establecidas. • El desconocimiento de las áreas encargadas de la red inalámbrica en cómo realizar auditorías de red inalámbrica.	La existencia de las redes inalámbricas dentro de la Facultad no está regulada, por lo que la auditoría a estos equipos resulta una tarea que no se hace con regularidad, siendo que auditar los servicios de red es una tarea primordial dentro de las medidas de seguridad informática.	• Se deberá establecer dentro del desarrollo Web una zona en donde publique información relacionada con auditoría en redes inalámbricas para que los encargados de los puntos de acceso tengan información al respecto.
Monitoreo de las redes inalámbricas.	**MEDIA**	• Que se estén intentando ataques sobre las redes inalámbricas con regularidad y que no sean detectados por los administradores. • Que haya usuarios no autorizados conectados a los puntos de acceso. • Obtención de información confidencial al estar conectados a las redes inalámbricas establecidas dentro de la Facultad de Ingeniería	Se podrían estar realizando ataques de fuerza bruta sobre redes inalámbricas en estos momentos y no ser detectados debido a que no existe una política que obligue a las áreas correspondientes a estar monitoreado sus redes inalámbricas de manera regular.	• Las técnicas de intrusión pueden ser detectadas mediante herramientas que se presentarán en una sección del sitio Web en dónde se expongan las principales características de estos programas. Esta información deberá estar disponible a todos los usuarios
Estadísticas de redes inalámbricas.	**BAJA**	• No contar con información referente a el número actual de redes inalámbricas dentro de la Facultad de Ingeniería así como cuáles protocolos de seguridad son los más comunes, cuáles son los canales de comunicación inalámbrica más utilizados, etcétera.	No se tiene un registro actualmente de redes inalámbricas.	• El sitio Web deberá generar estadísticas de manera automatizada acerca de datos relacionados a las redes inalámbricas existentes dentro de la Facultad de Ingeniería.

4.2.2 REQUERIMIENTOS DEL SISTEMA

En esta etapa se establece qué tiene que hacer el sistema exactamente, se provee de los requisitos del sistema para tener un mejor entendimiento y así tener una base solida para la fase de análisis del sistema. Los requisitos se dividen en dos grupos, los funcionales que son las operaciones básicas del sistema y los no funcionales que son aquellos atributos que debe exhibir el sistema, pero no son una funcionalidad específica.

4.2.2.1 REQUERIMIENTOS FUNCIONALES DEL SISTEMA

R1. Registro de las redes inalámbricas existentes dentro de la Facultad de Ingeniería. Esta información deberá ser almacenada en una base de datos. La información que se deberá de registrar será comprendida en 6 áreas generales:

- Información del contacto. Esta información será de utilidad para saber quién está a cargo de la red inalámbrica y cómo localizarlo en caso de cualquier situación referente a la red que está a su cargo. La información del contacto que se deberá de almacenar será:
    1. Nombre completo del administrador o encargado de la red inalámbrica.
    2. División a la que pertenece.
    3. Departamento.
    4. Puesto que desempeña.
    5. Correo electrónico.
    6. Teléfono o extensión dentro de la Facultad de Ingeniería.

- Información del equipo. Datos sobre el punto de acceso que estará dando el servicio de red inalámbrica:
    1. Fabricante del punto de acceso.
    2. Modelo del punto de acceso.
    3. Dirección del medio de control de acceso/dirección MAC.
    4. Nombre que tendrá el dispositivo.
    5. Si utiliza antena, qué tipo de antena utiliza así cómo su alcance.
    6. Y bajo que protocolos estará funcionando (802.11a, 802.11b ó 802.11g).

- Parámetros de la red inalámbrica. Estos datos son muy importantes dentro del registro de las redes inalámbricas.
    1. Nombre o SSID de red que tendrá la red inalámbrica.
    2. Canal (es) en los cuales estará funcionando.
    3. Y si esta red anuncia su SSID (*broadcast* del SSID).

- Datos de conexión a la red. Información de cómo estará funcionando en la red de la Facultad de Ingeniería.
    1. Dirección IP del punto de acceso.
    2. Dirección IP del *Gateway* que utiliza.
    3. Máscara de red.
    4. Así como su uso (acceso a la red, investigación, Intranet u otro uso).

- Datos de control de acceso y seguridad. Se deberá incluir información de cómo está funcionando la red inalámbrica, datos cómo:
    1. Método de cifrado que implementa.
    2. Mecanismo de autenticación.
    3. Sí utilizan filtrado de direcciones MAC.

4. Sí utiliza el protocolo IPSec.
5. Sí utiliza un servidor de autenticación.
6. Sí asigna direcciones DHCP en la red.
7. Cómo es configurado el punto de acceso sí por interfaz Web, por medio de la consola de comandos, SNMP u otra.

- Otra información. Datos que pueden ser importantes para llevar un mejor control de las redes inalámbricas.
    1. Tipos de usuarios de la red inalámbrica.
    2. Sí se guardan las bitácoras de asignación de IP's.
    3. Horario de funcionamiento.
    4. Fecha de instalación.
    5. Fecha de inicio de funcionamiento.
    6. Observaciones que deban de tenerse en cuenta.

R2. Ubicación de las redes inalámbricas registradas en un mapa de la Facultad de Ingeniería. La localización de las redes registradas será dividida en dos áreas: conjunto norte y conjunto sur de la Facultad de Ingeniería. Se requiere que el sistema sea capaz de presentar una interfaz en donde el usuario podrá localizar la red que se acaba de registrar. Al igual que la información de la red la ubicación será almacenada en una base de datos.

R3. Presentación de los datos de red así como su ubicación. Una vez registrados los datos de la red inalámbrica se deberá de presentar la información de una manera agradable y funcional, en dónde se localicen las redes inalámbricas existentes al momento en un mapa.

R4. El sistema deberá ser capaz de administrar estos registros, es decir, se deberá poder dar de alta, editar y eliminar registros de redes inalámbricas.

R5. El sistema deberá manejar perfiles de usuarios en dónde sólo un tipo de usuarios podrá ser capaz de administrar los registros de las redes inalámbricas.

R6. El sistema deberá tener zonas para publicar la información del procedimiento de registro de redes inalámbricas, las políticas de redes inalámbricas, información de monitoreo, información de auditoría así como información de buenas prácticas y configuraciones adecuadas.

4.2.2.2 REQUERIMIENTOS NO FUNCIONALES DEL SISTEMA

R7. El sistema deberá generar estadísticas de manera automatizada a partir de los registros en la base de datos de las redes inalámbricas. Estas estadísticas deberán estar visibles para cualquier usuario del sistema.

R8. La interfaz Web deberá ser agradable al usuario.

4.3 ANÁLISIS DE LA HERRAMIENTA GESTORA DE REDES INALÁMBRICAS

Una vez que conocemos los requerimientos funcionales y no funcionales del sistema el siguiente paso es el análisis del sistema en donde se obtiene una visión del mismo. En esta etapa se generan los Casos de Uso con el fin de entender cuáles son las entradas y salidas, así como las variables del sistema Web.

4.3.1 OPERACIÓN PRINCIPAL DEL SISTEMA

1. De los requisitos R1, R2 y R3 que se establecen como la principal funcionalidad del sistema se desprende el siguiente diagrama

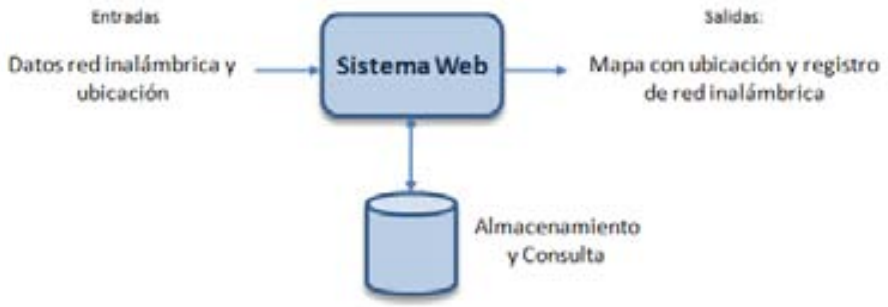


FIGURA 4.1 Diagrama inicial del sistema

4.3.2 OPERACIONES SECUNDARIAS DEL SISTEMA

2. Del requisito R4 que define las operaciones de administración del sistema Web, por lo que estas tareas deberán ser realizadas por el perfil de usuario de mayores privilegios.
3. Del requisito R5 se identifican los roles de usuarios y sus privilegios, por lo que las actividades dentro del sistema Web serán basadas en los perfiles.
4. Del requisito R6 se identifica la operación de las áreas de publicación de información en donde no se requiere de algún perfil de usuario para consultar dichas zonas del sitio.

4.3.3 CASOS DE USO

Caso de Uso 1.	Registro y ubicación de una red inalámbrica
Requerimientos cubiertos	R1, R2.
Descripción	La operación principal de sistema Web consiste en registrar las redes inalámbricas existentes dentro de la Facultad de Ingeniería así como su ubicación física. El sistema deberá ser capaz de presentar una interfaz donde se introduzcan los datos de la red inalámbrica así como un mapa para poder ubicarla.
Actores	Usuarios con privilegios de administrador y el sistema Web.
Precondiciones	Para dar de alta una red inalámbrica no deberá existir una red inalámbrica con el mismo SSID, nombre del punto de acceso y ubicación de la red. Además previamente para registrar una red inalámbrica deberá ser autorizada por el personal encargado de estas tareas.
Pasos	1. Entrar al sistema Web con un usuario que tenga los privilegios de administrador. 2. Dirigirse a la página en donde se podrán dar de alta los datos de redes inalámbricas. 3. Llenar el formulario con los datos requeridos de manera obligatoria para poder registrar la red inalámbrica. 4. Una vez registrados los datos de la red inalámbrica se deberá pedir la ubicación de la red, ya sea en el conjunto norte o sur de la Facultad de Ingeniería. 5. Localizar en un mapa de la zona la ubicación del punto de acceso de la red inalámbrica. 6. Dirigirse al mapa para verificar la existencia de la nueva red inalámbrica.
Validaciones	• Validar que el usuario tenga privilegios de administrador del sistema. • Que la sesión no haya expirado. • El sistema deberá validar cada campo del formulario como campos de nombre, teléfono, direcciones IP, etcétera. Además se deberá verificar que el nombre del punto de acceso y SSID no existan ya en una red inalámbrica.

Caso de Uso 2.	Visualización de los datos
Requerimientos cubiertos	R3.
Descripción	Un usuario del sistema podrá ingresar a la aplicación para visualizar las redes inalámbricas registradas en el sistema.
Actores	Usuarios con cuenta del sistema y el sitio Web.
Precondiciones	Tener cuenta del sistema.
Pasos	1. Dirigirse al sistema Web a la parte donde se ingresa al sistema. 2. Validar las credenciales de los usuarios. 3. Si son usuarios podrán ingresar a la aplicación que les permita ver en las redes inalámbricas del sistema Web.
Validaciones	• Validar que el usuario tenga privilegios de administrador del sistema. • Que la sesión no haya expirado.

Caso de Uso 3.	Operaciones de administración de registros de redes inalámbricas
Requerimientos cubiertos	R4.
Descripción	Un usuario que cuente con privilegios de administrador del sistema podrá registrar, modificar información y eliminar registros de redes inalámbricas.
Actores	Usuarios con privilegios de administrador y el sistema Web.
Precondiciones	Tener privilegios de administrador.
Pasos	1. Entrar al sistema Web con un usuario que tenga los privilegios de administrador. 2. Dirigirse a la página en donde se podrán dar de alta, modificar y eliminar los datos de redes inalámbricas. 2.1 Insertar: Caso de Uso 1. 2.2. Modificar. Ir a la página de editar datos de red inalámbrica, seleccionar de un menú de edición de datos la red inalámbrica a la que se editarán los datos. Una vez modificados los datos, enviarlos para que sean actualizados. 2.3 Eliminar. Ir a la página de edición de datos de red inalámbrica, seleccionar del menú de eliminar red inalámbrica el registro. Al seleccionar y enviar esa información, la red se deberá eliminar de la base de datos. 3. Regresar a la página inicial de administrador del sistema.
Validaciones	• Validar que el usuario tenga privilegios de administrador del sistema. • Que la sesión no haya expirado. • El sistema deberá validar cada campo del formulario como campos de nombre, teléfono, direcciones IP, etcétera. Además se deberá verificar que el nombre del punto de acceso y SSID no existan ya en una red inalámbrica.

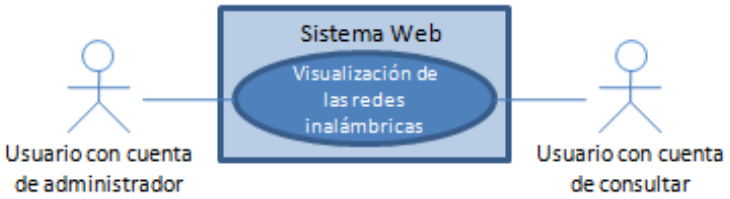
Caso de Uso 4.	Perfiles de Usuarios
Requerimientos cubiertos	R5.
Descripción	Las cuentas del sistema deberán tener ciertos privilegios que les permitan hacer uso del sistema según el perfil de usuario.
Actores	Usuarios y el sistema Web.
Precondiciones	Tener cuenta del sistema.
Pasos	4. Dirigirse al sistema Web a la parte donde se ingresa al sistema. 5. Validar las credenciales de los usuarios y según sea el perfil de usuario desplegar el sistema. 5.1 En caso de ser un usuario con privilegios de "sólo consulta de la información" desplegar el sistema donde aparecen registradas las redes inalámbricas. 5.2 En caso de ser un usuario con privilegios de "administrador" desplegar el sistema con los privilegios de administrador.
Validaciones	• Validar que el usuario exista en la base de datos. • Que la sesión no haya expirado.

Caso de Uso 5.	Publicación de información
Requerimientos cubiertos	R6.
Descripción	Una parte muy importante de este desarrollo será la publicación de información relativa a las redes inalámbricas dentro de la Facultad de Ingeniería.
Actores	Usuarios y el sistema Web.
Precondiciones	Ninguna.
Pasos	1. Dirigirse a la dirección Web del sitio. 2. Seleccionar del menú principal el área de información a consultar.
Validaciones	Ninguna

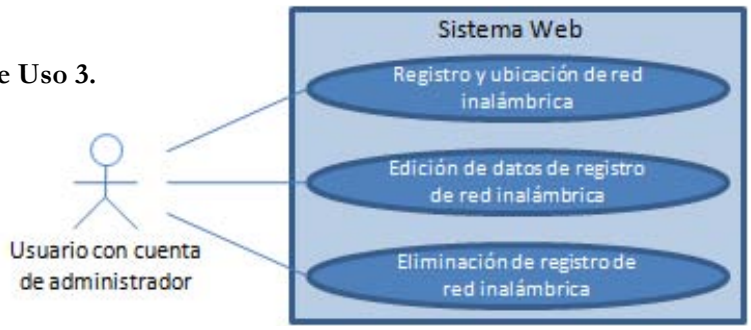
4.3.4 DIAGRAMAS DE CASOS DE USO

Caso de Uso 1.

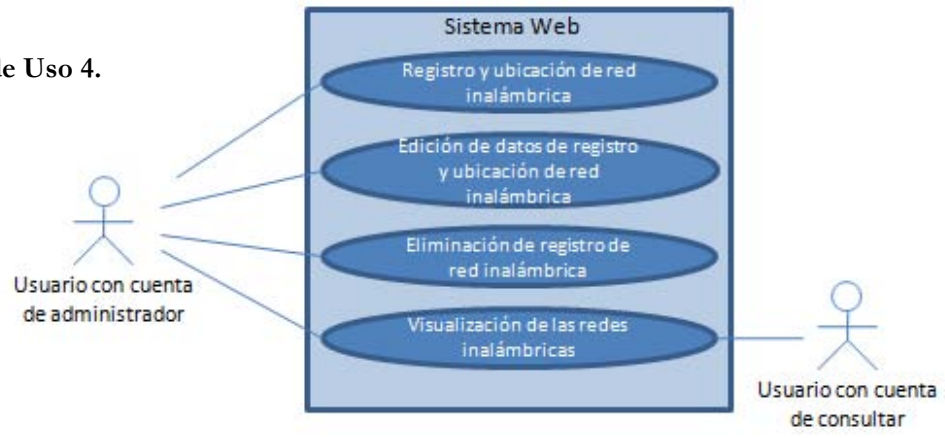
Caso de Uso 2.



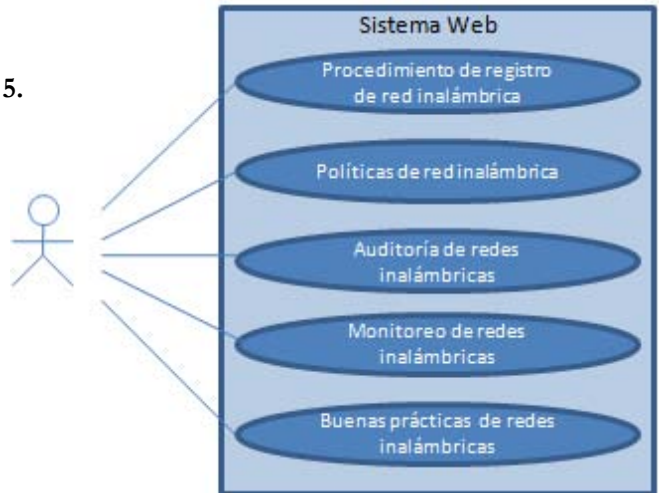
Caso de Uso 3.



Caso de Uso 4.



Caso de Uso 5.



4.3.5 DEFINICIÓN DEL ALCANCE DEL SISTEMA

Una vez conocidos los requerimientos funcionales y no funcionales se puede llegar a analizar cuáles son las tareas específicas de deberá cubrir el sistema y cuáles no. A continuación se listan las actividades que se requieren para el sistema:

1. Registro de redes inalámbricas mediante un formulario de introducción de datos.
2. Localizar la ubicación de la red inalámbrica en un mapa para que posteriormente sea visible en una aplicación donde se visualicen los datos y ubicación de manera conjunta.
3. Aplicación Web que permita visualizar las redes inalámbricas registradas así como su ubicación en un mapa de la zona.
4. Administración del sitio mediante operaciones de alta, cambios de información (datos o ubicación) y eliminación de registros de redes inalámbricas.
5. Manejo de perfiles de usuarios.
6. Publicación de información relacionada a las redes inalámbricas:
    - Procedimiento de alta.
    - Políticas de redes inalámbricas.
    - Auditoría en redes inalámbricas.
    - Monitoreo en redes inalámbricas.
7. Generación de estadísticas de información de redes inalámbricas de manera automatizada a partir de la información almacenada en la base de datos.
8. Deberá tener una interfaz agradable al usuario y procedimientos sencillos.

El sistema no manejará la creación de las cuentas de los usuarios desde el sitio Web en una primera etapa, la administración de estas cuentas se realizará de manera manual en la base de datos de usuarios por parte de los administradores del sistema Web.

4.4 DISEÑO DE LA HERRAMIENTA GESTORA DE REDES INALÁMBRICAS

La siguiente fase del desarrollo del sistema es el diseño, en esta etapa se deberá separar en componentes el sistema.

4.4.1 COMPONENTES DEL SISTEMA

Se empezarán a diseñar los componentes del sistema Web a partir del análisis hecho de los requerimientos del sistema. Se identificaron principalmente 5 Casos de Uso que podrán ser vistos como componentes del sistema.

C1. Componente de registro y ubicación de redes inalámbricas dentro de la Facultad de Ingeniería.
C2. Componente de visualización de redes inalámbricas dentro de la Facultad de Ingeniería.
C3. Componente de administración de registros de la base de datos de las redes inalámbricas.
C4. Componente de autenticación de usuarios y sesiones.
C5. Componente de publicación de información de las redes inalámbricas.

4.4.2 DISEÑO DE COMPONENTES

C1. Componente de registro y ubicación de redes inalámbricas dentro de la Facultad de Ingeniería.

El C1 es el componente que se encargará de la funcionalidad de registrar las redes inalámbricas dentro del sistema, para ello se empezará a diseñar el componente a partir del diagrama del componente.

FIGURA 4.2 Módulo de registro y ubicación de redes inalámbricas

Del diagrama se desprenden varias observaciones que servirán en la fase posterior de implementación del sistema:

- El componente deberá ser un proceso de dos fases, en la primer fase se guardarán los datos de la red inalámbrica, posteriormente en la segunda fase se ubicará la red inalámbrica dentro del mapa.
- Los datos deberán ser validados antes de ser enviados a la base de datos. Cada campo del formulario deberá llenarse correctamente para asegurar que la información que se almacene corresponda a los campos que contendrá la base de datos.
- La ubicación podrá estar dentro de las dos zonas existentes para colocar la red inalámbrica. Esta ubicación deberá ser almacenada como un dato más de la red inalámbrica para que posteriormente pueda ser consultada.
- Esta operación sólo podrá ser utilizada por la cuenta con privilegios de administrador. Todas las páginas del sistema deberán verificar el perfil de la cuenta.

C2. Componente de visualización de redes inalámbricas dentro de la Facultad de Ingeniería.

El componente C2 será el encargado de visualizar las redes inalámbricas existentes en la base de datos. La visualización de estas redes se realizará de forma que se ubiquen los puntos de acceso en un mapa de la Facultad de Ingeniería, para las dos áreas conjunto norte y sur de la Facultad de Ingeniería.

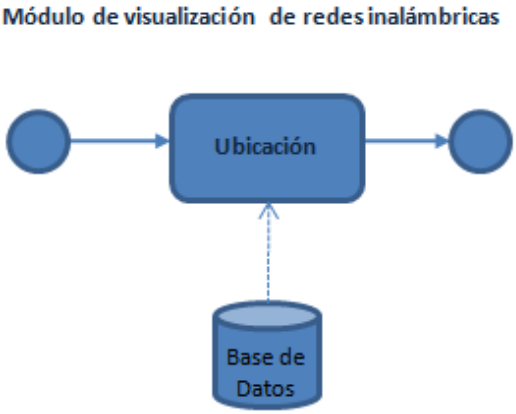


FIGURA 4.3. Módulo de visualización de redes inalámbricas

- El sistema visualizará en una aplicación las redes inalámbricas existentes en dos zonas.
- La visualización de las redes inalámbricas se realizará dependiendo de los registros que haya en la base de datos.
- Además de su ubicación en el mapa, se presentará información referente a las redes inalámbricas registradas.

C3. Componente de administración de registros de la base de datos de las redes inalámbricas.

Este componente será el encargado de manipular la información que se encuentre almacenada en la base de datos. Las funcionalidades de este componente están ligadas a la base de datos, estas operaciones que son ingresar registro, modificar registro y eliminar, serán tareas específicas de la cuenta de administrador.

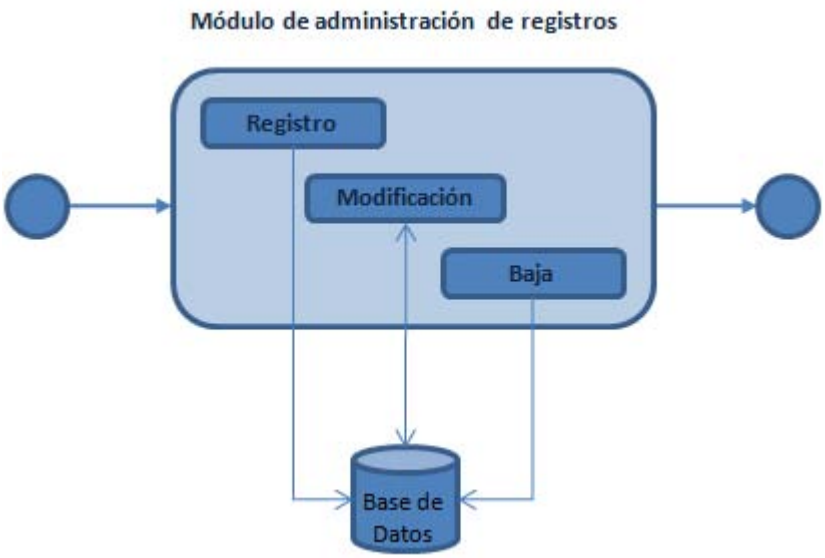


FIGURA 4.4. Módulo de administración de registros

Observaciones:

- El módulo de administración deberá tener la funcionalidad de alta, baja y cambios de los registros de la base de datos de la red inalámbrica.
- Sólo la cuenta de tipo administrador será la que podrá operar estas tareas.
- La operación de registro se consideró en el C1 (Componente 1).
- Para la operación de modificación de información de los registros de igual manera, se deberán validar los datos que se estén actualizando, así como verificar que si se cambia el SSID y el nombre del punto de acceso no existan ya dentro de la base de datos.
- Se podrá modificar la información de la red inalámbrica y la ubicación de la red inalámbrica.
- La operación de eliminar un registro de la base de datos será irreversible, una vez realizada esta operación no quedará rastro en el sistema.

C4. Componente de autenticación de usuarios y sesiones.

Este componente se encargará de autenticar a los usuarios del sistema así como su perfil. Las cuentas de usuarios deberán estar almacenadas en una base de datos en donde se almacene el usuario, su contraseña y el tipo de usuario que es. Las cuentas del sistema deberán de ser administradas de manera local en la base de datos. Este sistema no contempla la funcionalidad de la administración de las cuentas de usurarios desde el sitio Web. Se manejarán 2 tipos de cuentas del sistema, las de tipo administrador y las de consulta.

Una vez que se haya autenticado el usuario se deberá comprobar que una sesión de tipo administrador o consulta se ha iniciado, por lo que el uso de la sesiones en cada una de las páginas del sistema será obligatorio, de esta manera mientras la sesión no haya expirado se tendrán los privilegios para realizar las operaciones que pueden realizar con este tipo de cuenta.

C5. Componente de publicación de información de las redes inalámbricas.

El módulo de publicación no requiere del uso de una cuenta del sistema, la publicación de información será con fines informativos. En esta parte de la funcionalidad de sistema se deberá presentar en el sitio Web la información referente al procedimiento de registro de redes inalámbricas, las políticas de redes inalámbricas, información de monitoreo, auditoría así como buenas prácticas de redes inalámbricas.

La información deberá ser presentada de manera que el usuario pueda navegar con facilidad dentro del sitio Web. Como una opción de la publicación de esta información se podrá colocar archivos *PDF* que puedan descargase del sitio Web.

4.4.3 FLUJO DE PANTALLAS DEL SISTEMA

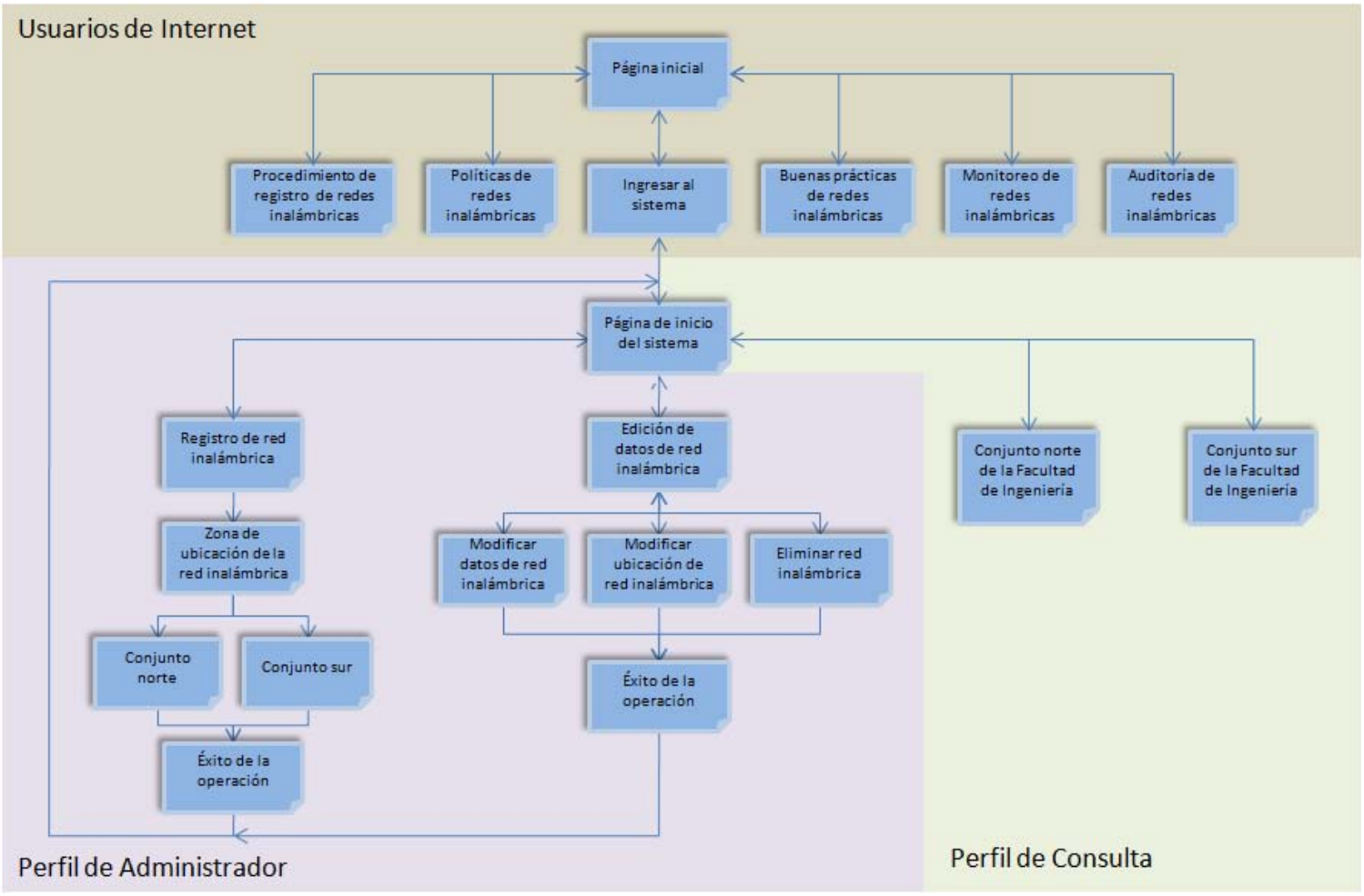


FIGURA 4.5. Flujo de pantallas del sistema

4.4.4 DIAGRAMA DE SECUENCIAS

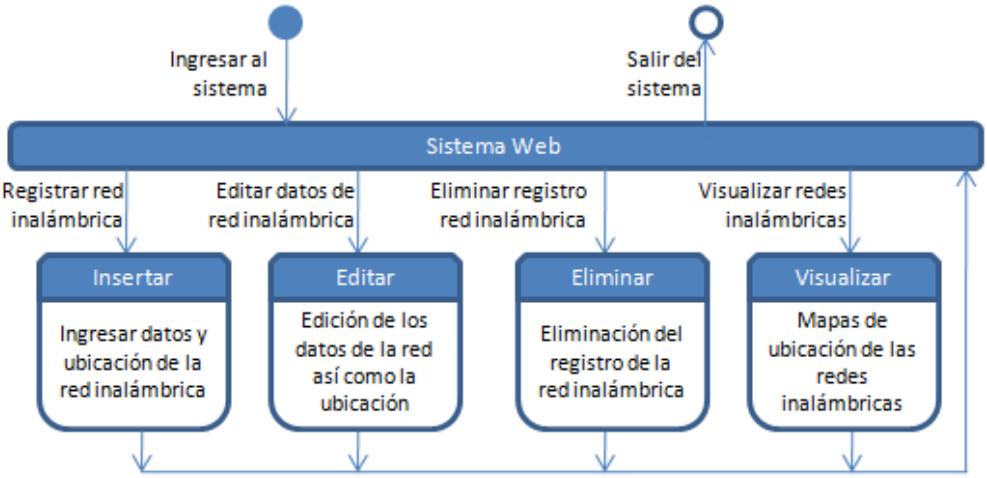


FIGURA 4.6 Diagrama de secuencias 1

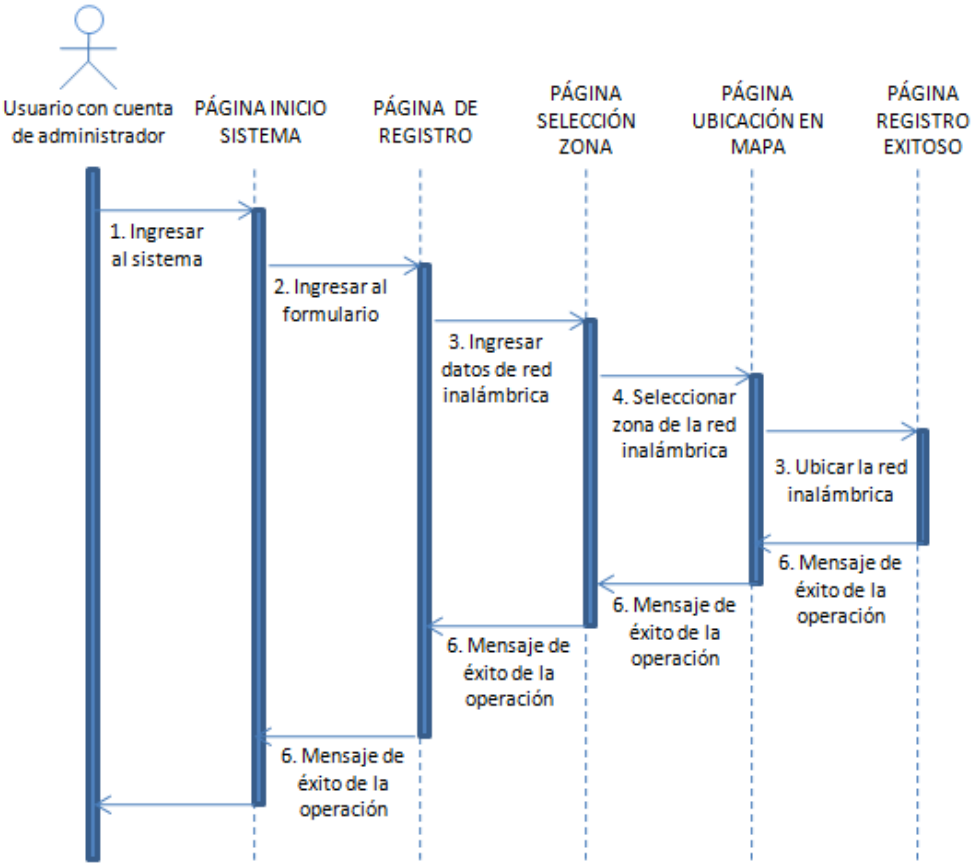


FIGURA 4.7 Diagrama de secuencias 2

4.4.5 DICCIONARIO DE DATOS

NOMBRE DE LA TABLA	NOMBRE DEL ATRIBUTO	DESCRIPCIÓN	TIPO	FORMATO	ES PK?
redesInalambricas	idRed	Id de red, será único e irrepetible	INT	00	NO
	nombre	Nombre y apellido de la persona encargada de la red inalámbrica	VARCHAR		NO
	division	División a la cual pertenece la persona encargada de la red inalámbrica	VARCHAR		NO
	departamento	Departamento donde labora la persona encargada de la red inalámbrica	VARCHAR		NO
	puesto	Puesto que desempeña la persona encargada de la red inalámbrica	VARCHAR		NO
	correo	Correo electrónico de la persona encargada de la red inalámbrica	VARCHAR		NO
	telefono	Teléfono donde se podrá localizar a la persona encargada de la red inalámbrica	INT	00000000	NO
	fabricante	Nombre del fabricante del punto de acceso	VARCHAR		NO
	modelo	Modelo del punto de acceso	VARCHAR		NO
	direccionMAC	Dirección física o MAC del punto de acceso	VARCHAR	00-00-00-00-00-00	NO
	tipoAntena	En caso de tener conectada una antena, el tipo de antena que es.	VARCHAR		NO
	nomAP	Nombre del equipo del punto de acceso	VARCHAR		SI
	alcance	Alcance de la antena en caso de existir	INT	00.00	NO
	wifia	Si el punto de acceso tiene soporte para el protocolo 802.11a	VARCHAR		NO
	wifib	Si el punto de acceso tiene soporte para el protocolo 802.11b	VARCHAR		NO
	wifig	Si el punto de acceso tiene soporte para el protocolo 802.11g	VARCHAR		NO
	ssid	Nombre del identificador de la red inalámbrica	VARCHAR		SI
	canales	En que canales de comunicación inalámbrica está configurada la red	VARCHAR		NO
	broadcast	Si la red irradiara el nombre de la red a manera de broadcast	VARCHAR		NO
	uso	El uso que para cual fue creada la red inalámbrica	VARCHAR		NO
	gateway	Dirección IP del Gateway de red que utiliza la red inalámbrica	VARCHAR	000.000.000.000	NO
	ipap	Dirección IP del punto de acceso	VARCHAR	000.000.000.000	NO
	mascara	Máscara de red que utilizara la red inalámbrica	VARCHAR	000.000.000.000	NO
	filMAC	Si la red inalámbrica utiliza un filtrado de direcciones MAC	VARCHAR		NO
	dhcp	Si la red inalámbrica utiliza un servicio DHCP para asignar direcciones	VARCHAR		NO
	ipsec	Si la red inalámbrica utiliza el protocolo IPSec	VARCHAR		NO
	servAut	Si la red inalámbrica utiliza un servidor de autenticación	VARCHAR		NO
	cifrado	Que método de cifrado de datos utiliza la red inalámbrica	VARCHAR		NO
	mecanismo	Que método de mecanismo de autenticación utiliza la red inalámbrica	VARCHAR		NO
	confAP	De qué forma fue configurado el punto de acceso	VARCHAR		NO
	usuarios	Que tipos de usuarios tiene la red inalámbrica	VARCHAR		NO
	bitácoras	SI la red inalámbrica guarda bitácoras de asignación de direcciones IP	VARCHAR		NO
	horarioI	Horario de inicio de funcionamiento de la red inalámbrica	VARCHAR	00	NO
	horarioT	Horario de termino de funcionamiento de la red inalámbrica	VARCHAR	00	NO
	fechaInst	Fecha en la cual fue instalada la red inalámbrica	VARCHAR	00/00/0000	NO
	fechaFunc	Fecha en la cual comenzó a funcionar la red inalámbrica	VARCHAR		NO
	Observaciones	Observaciones a tomar en cuenta para la red inalámbrica	VARCHAR		NO
	lugar	Lugar de la localización de la red inalámbrica (Principal / Anexo)	VARCHAR		NO
	posx	Posición x que ocupa el punto de acceso en el mapa	VARCHAR		NO
	posy	Posición y que ocupa el punto de acceso en el mapa	VARCHAR		NO
usuariosRI	login	Login del usuario del sistema	VARCHAR		NO
	password	Contraseña del usuario del sistema	VARCHAR		NO
	Tipo	Tipo de cuenta de usuario del sistema	VARCHAR		NO

4. 4.6 DIAGRAMA DE FLUJO DE DATOS

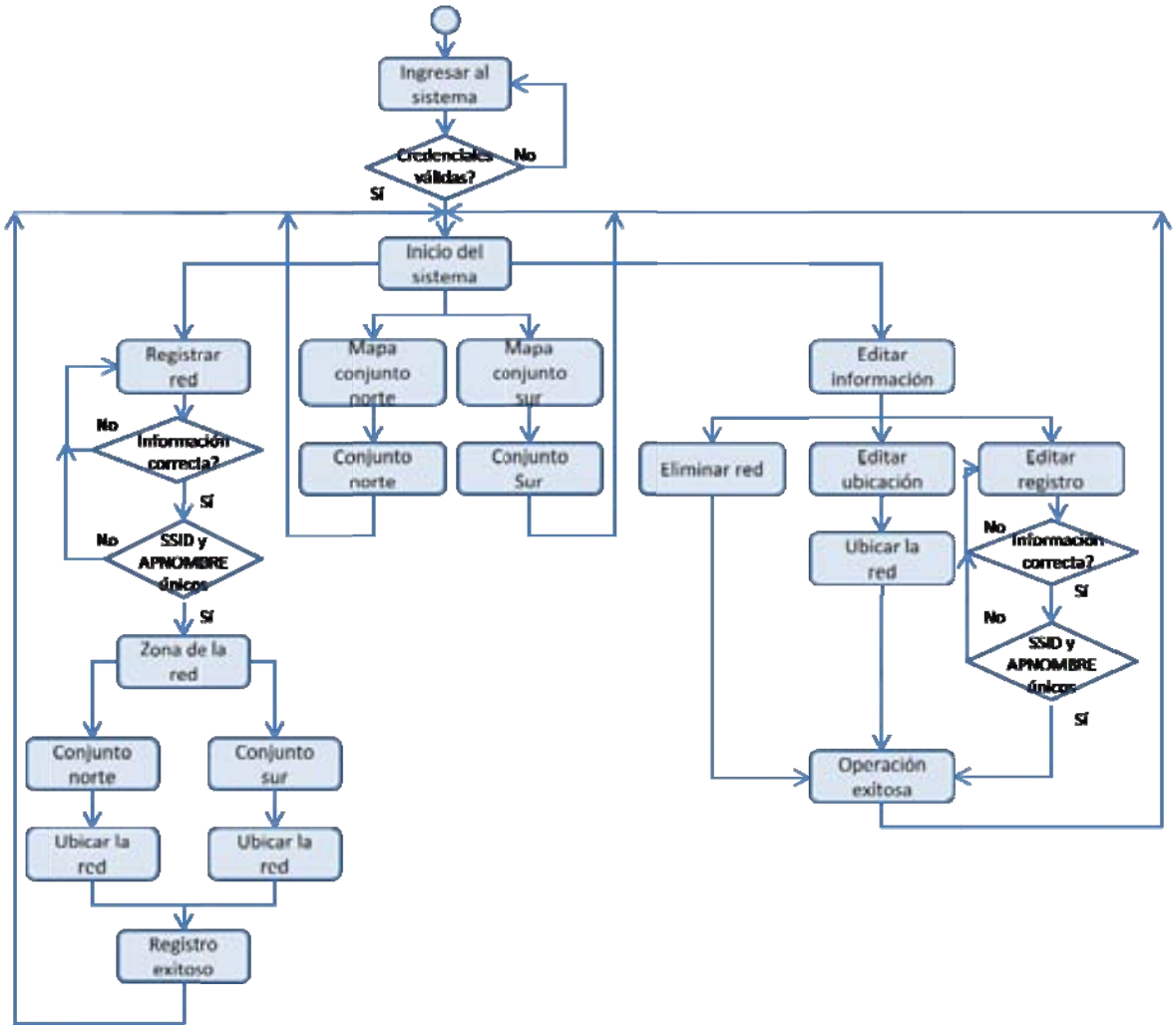


FIGURA 4.8 Diagrama de flujo de datos

4.4.7 TECNOLOGÍAS DE PROGRAMACIÓN A IMPLEMENTAR

El desarrollo del sistema Web para la gestión de redes inalámbricas de la Facultad de Ingeniería deberá ser una herramienta que permita de manera fácil y controlada llevar el registro de las redes inalámbricas existentes en la institución, para ello se deberá de crear un sistema que sea totalmente funcional. De la etapa anterior y del análisis de los requisitos del sistema se puede concluir que esta herramienta deberá presentar programación Web y algunos recursos de programación gráfica, por lo que a continuación se hace una descripción de los componentes elegidos para el desarrollo del sistema.

- PROGRAMACIÓN WEB

Para el sitio Web que se desarrollará se eligió el lenguaje de programación Web de *Java Server Pages*. Esta tecnología de programación dinámica para Web fue desarrollada por *Sun Microsystems*, y que por sus características de lenguaje de programación de propósito general actualmente tiene una fuerte presencia en

el desarrollo de sitios Web a nivel mundial, brinda la posibilidad de heredar las clases de *Java* que lo hace muy poderoso, además de ser multiplataforma.

- PROGRAMACIÓN GRÁFICA

Para el desarrollo de la parte gráfica del sitio Web se utilizará *Macromedia Flash 8*, debido a la calidad del procesamiento de animaciones y contenido interactivo que tiene. *Flash* es de licencia propietaria de *EULA*, este software permite la creación de animaciones multimedia e interactivas para Internet, razón por la cual se ha elegido como parte de las herramientas del desarrollo del sitio Web.

Las animaciones que se pueden desarrollar con *Flash* darán la posibilidad de que el sitio Web presente una interfaz interactiva entre el usuario y la base de datos, los requisitos de visualización de las redes inalámbricas podrán cubrirse completamente con esta herramienta.

- BASE DE DATOS

Para el manejo de los datos se utilizará *MySQL*, que presenta un manejo de bases de datos relacionales, multihilo y multiusuario. Tiene controladores de base de datos para *JSP*, además se recomienda su uso para sistemas pequeños como es el caso. Es de licencia *GNU GPL* por lo que no es necesario adquirir el software.

4.5 DESARROLLO DE HERRAMIENTA GESTORA DE REDES INALÁMBRICAS

En esta etapa del proceso de desarrollo de la herramienta Web es donde se comienza la programación del sistema, se crearán los archivos *jsp* y archivos de flash que darán la funcionalidad al sistema. El desarrollo se hará de manera como se haya diseñado en la etapa previa, haciendo un desarrollo modular y una vez que se hayan terminado de desarrollar los *jsp´s* se deberán hacer pruebas por cada módulo que se implemente para que al final resulte un sólo sistema Web integrando los componentes.

4.5.1 IMPLEMENTACIÓN DEL C1. COMPONENTE DE REGISTRO Y UBICACIÓN DE REDES INALÁMBRICAS DENTRO DE LA FACULTAD INGENIERÍA

Para empezar con el desarrollo de este componente se analizará el flujo de la información.

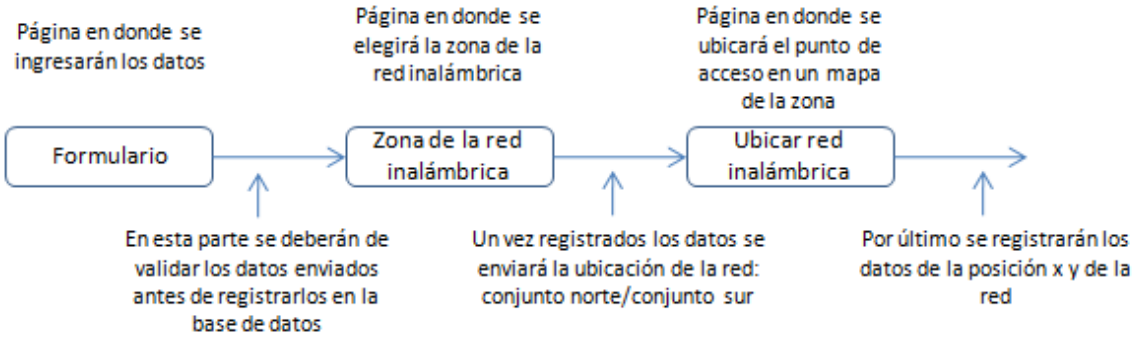


FIGURA 4.9 Modelo del flujo de información

formulario.jsp

Esta página presentará un formulario que muestre los campos necesarios de información para registrar a la red inalámbrica. La página se desarrolla con código HTML y deberá tener el código necesario que valide la sesión del usuario.

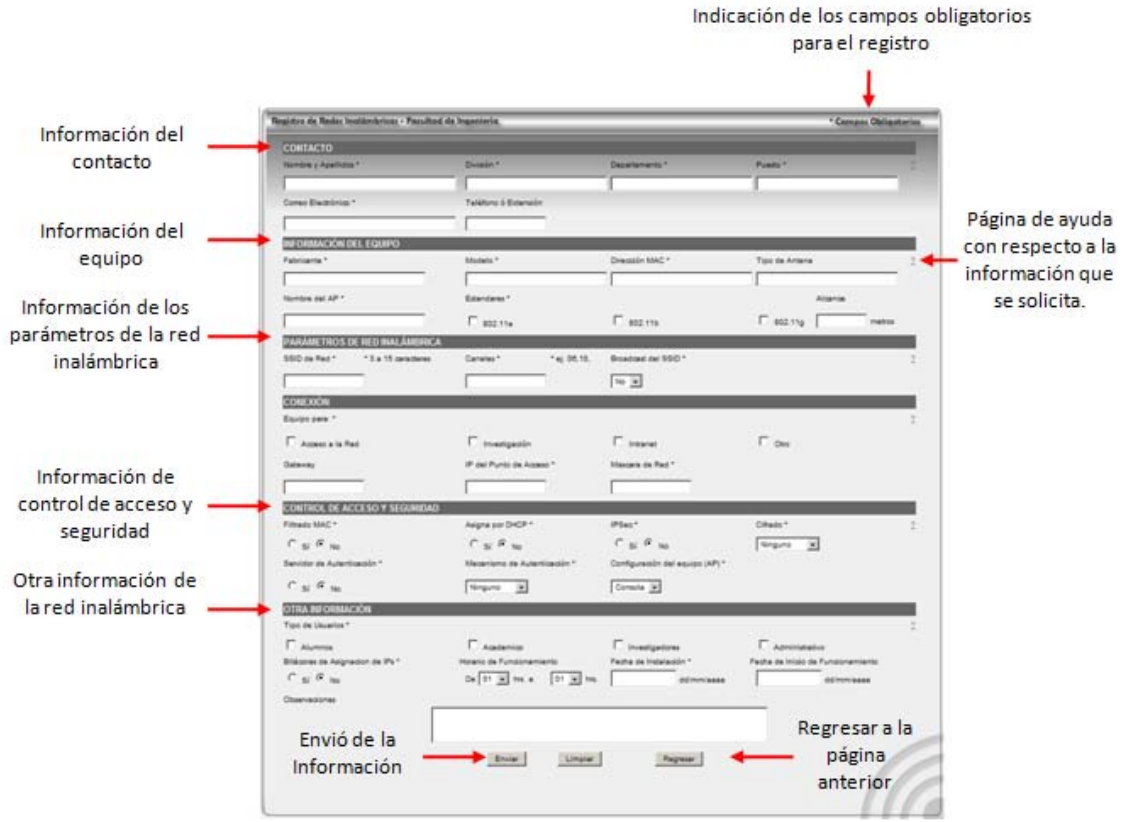


FIGURA 4.10 Formulario

recibe.jsp

El *jsp* que recibirá los datos enviados por el formulario deberá de validar cada campo, es decir que el campo de nombre sean sólo cadenas, el campo teléfono sean sólo números, etcétera. Una vez que se validaron los campos se indicará con una bandera si todos los campos enviados corresponden al tipo de dato esperado, una vez que esta bandera indicó que si son correctos entonces se procede al envió de los datos a la base de datos. Se debe verificar antes si no existe registrada una red inalámbrica con el mismo SSID y nombre de AP, ya que son los identificadores únicos.

PSEUDOCÓDIGO DEL JSP QUE RECIBE Y REGISTRA LOS DATOS

```
/* Cabeceras */
<%@ page import="java.sql.*"%>
/* Código HTML que desplegará la cabecera de la página de respuesta*/
/* Función que se ocupará para validar campos de direcciones IP, recibe una cadena de direcciones IP y regresa verdadero o falso si es
o no válida*/
<%!
      boolean esDireccionValida(String dir)   {   Código de la función   }
%>
```

```
<%
/*Declaración de las variables */
String nombre="";
/* Validación de los parámetros recibidos */
if((request.getParameter("nombre")!=null) && (request.getParameter("nombre").matches("(([a-zA-Z]+|[a-zA-Z]+\\s)*)" )))
{  nombre= request.getParameter("nombre")  }
else{
            cadenaError="Nombre no valido";
            fallo=true;                }

Connection conn2 = null;
Statement st2 = null;
ResultSet rs2 = null;
try{
            Class.forName("com.mysql.jdbc.Driver").newInstance();
            conn2 = DriverManager.getConnection("jdbc:mysql://localhost/*****);
            st2 = conn2.createStatement();
            rs2 = st2.executeQuery("select * from redesinlamabricas where ssid='" + ssid  + "' and apnombre='" + apnombre  + "'");
            while(rs2.next())       {                       bandera=rs2.getString("ssid");    }
            if(!bandera.equals("")){
                        cadenaError="Existe una red con ese SSID y AP Nombre iguales, escoger otros parámetros";
                        fallo=true;                         }
}//try
catch (Exception ex) {   out.println(ex);   }
finally {     }

/*Una vez validados los parámetros checar la bandera de fallo, si es falso entonces enviar los datos a la base de datos*/
if(fallo==false)
{
    Connection conn=null;
    try{
          Class.forName("com.mysql.jdbc.Driver").newInstance();
          conn=DriverManager.getConnection("jdbc:mysql://localhost/pruebas?user=root&password=QwAsZx");
         PreparedStatement pst=conn.prepareStatement("INSERT INTO redesinlamabrica (valores) values(?)");
         pst.setString(1,nombre);
             .
   }
   catch(Exception e)    {     }
   finally {    if(conn != null) conn.close();    }
}
else {    }
/* Código HTML que desplegará el resto de la página de respuesta*/
```

Una vez registrada la red inalámbrica en la siguiente página se deberá elegir la zona en donde se ubicará el punto de acceso, como se mencionó desde los requisitos se manejarán dos zonas inicialmente, la zona del conjunto norte y la zona del conjunto sur de la Facultad de Ingeniería. Cuando se elija la zona se deberá guardar en la base de datos la zona en que se ubicará y a continuación desplegar la página donde se encuentre la aplicación que será capaz de obtener la posición exacta.

FIGURA 4.11 Selección de zona

```
Class.forName("com.mysql.jdbc.Driver").newInstance();
conn = DriverManager.getConnection("jdbc:mysql://localhost/********");
PreparedStatement pst=conn.prepareStatement("update redesinlamabricas set lugar=? where lugar='' ");
pst.setString(1,vlugar);
pst.executeUpdate();
pst.close();
```

localizacionRedInalambrica.jsp

Esta página deberá mostrar la aplicación que sea capaz de obtener una ubicación sobre un mapa de la zona, esta parte de desarrollo está con Flash y *ActionScript*. La aplicación muestra un punto que se podrá movilizar sobre el mapa, mediante *ActionScript* se estarán obteniendo las coordenadas del punto y se estarán visualizando en las etiquetas *x* y *y* mostradas en la aplicación, una vez fijado el punto se enviarán los datos mostrados en la aplicación: ssid, apnombre y las posiciones x y y.

Código *ActionScript*

```
onClipEvent (enterFrame)  {       localizacion();    }
onClipEvent (load)
{    function localizacion()   {
               if(_root.mouse_mc._x<600) {    _root.box1=_root.mouse_mc._x;    }
               else {        _root.box1="Fuera de Rango";  }
               if(_root.mouse_mc._y<600){     _root.box2=_root.mouse_mc._y;    }
               else{    _root.box2="Fuera de Rango";  }
               }
}
```

```
on (release)
{
               datos = new LoadVars();
               datos.ssid = ssid;
               datos.apnombre = apnombre;
               datos.posx = box1;
               datos.posy = box2;
               datos.send("send.jsp","_self" );
}
```

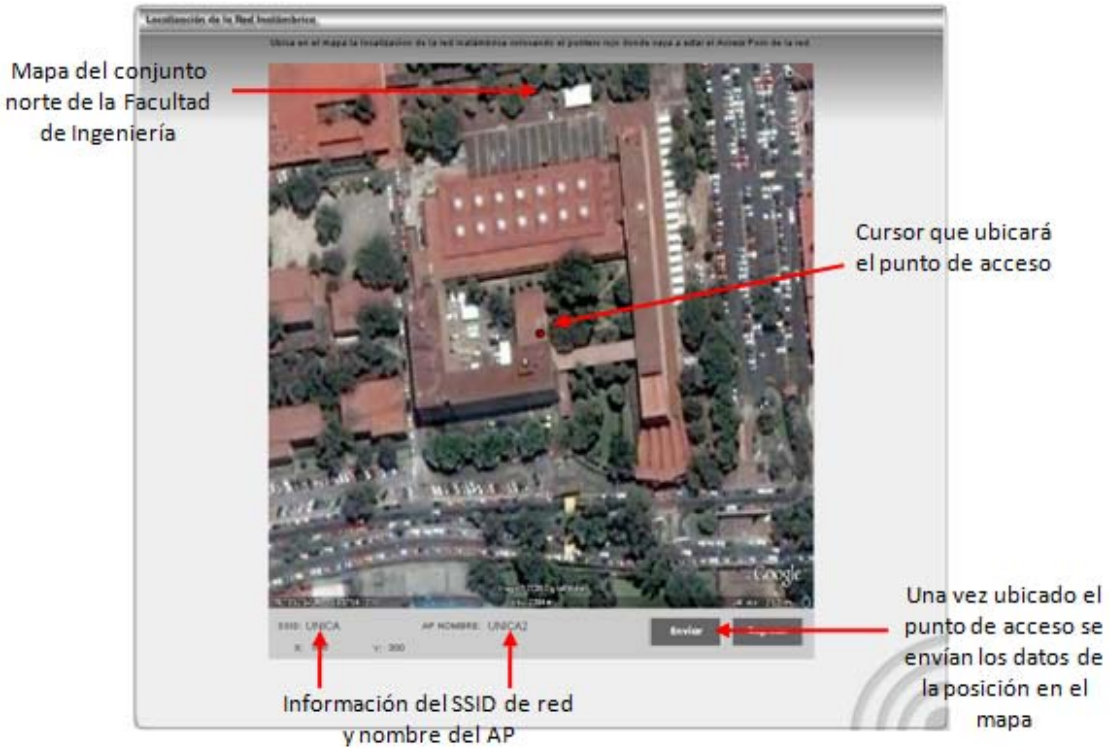


FIGURA 4.12 Mapa de localización

send.jsp

Este archivo se encargará de recibir los datos enviados por la aplicación flash para actualizar los datos de *posicionx* y *posicióny* en la base de datos.

```
String vssid=request.getParameter("ssid");
String vapnombre=request.getParameter("apnombre");
String vposx=request.getParameter("posx");
String vposy=request.getParameter("posy");

Connection conn = null;
try {
        Class.forName("com.mysql.jdbc.Driver").newInstance();
        conn = DriverManager.getConnection("jdbc:mysql://**********");
        PreparedStatement pst=conn.prepareStatement("update redesinlamabricas set posicionx=?, posiciony=? where ssid=?
and apnombre=? ");
        pst.setString(1,vposx);
        pst.setString(2,vposy);
        pst.setString(3,vssid);
        pst.setString(4,vapnombre);
        pst.executeUpdate();
        pst.close();
    }
response.sendRedirect("exitoAlta.jsp");
```

Con esta información se completa el registro de la red inalámbrica y se re-direcciona a la página del mensaje de éxito de registro de red inalámbrica.

4.5.2 IMPLEMENTACÍON DEL C2. COMPONENTE DE VISUALIZACIÓN DE REDES INALÁMBRICAS DENTRO DE LA FACULTAD DE INGENIERÍA

La implementación del componente C2 se desarrolló en *ActionScript*. Este componente tiene la funcionalidad de obtener la información de las redes inalámbricas y mapearlas en el mapa de la zona. En el diseño de este componente se declaró que esta aplicación flash obtendrá los datos de las redes y los mostrará en los campos de información. Deberían aparecer todas las redes inalámbricas de la zona, con la opción de mostrar la información de cuál es el SSID de red en la parte inferior de este desarrollo. Al momento de querer visualizar la información de determinada red se seleccionará con un clic sobre el gráfico que representa el punto de acceso y automáticamente se llenarán los campos con la información de la red seleccionada.

Para el desarrollo de esta aplicación se utilizará un archivo XML (*Extensible Makeup Language*) del cual la aplicación Flash podrá obtener la información y presentarla al usuario. Este archivo deberá ser creado en el momento que se registre una red inalámbrica para poder tener actualizados los datos. Mediante el uso de archivos XML la aplicación gráfica podrá interactuar con el archivo y así obtener los datos. *ActionScript* permite la lectura de archivos XML mediante el manejo de la jerarquía de objetos dentro del archivo XML.

El funcionamiento de esta aplicación de visualización está dividido en dos fases, la primera fase se encarga de leer la información del archivo XML para obtener el número de redes inalámbricas y su posición para poder dibujarlas en el mapa; la segunda fase consta de leer nuevamente el archivo para obtener la información y mostrarla conforme a las redes ubicadas en el mapa.

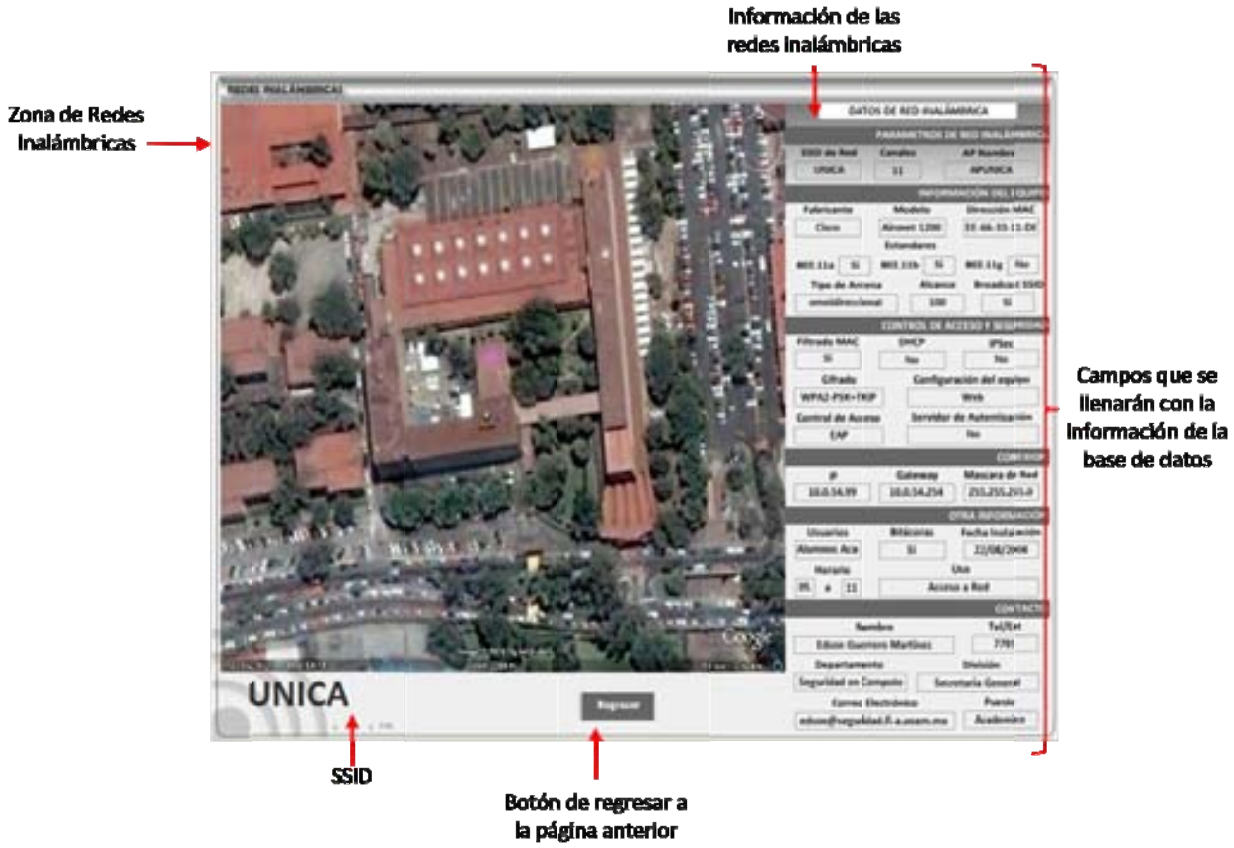


FIGURA 4.13 Aplicación de redes inalámbrica

La primera fase dibujará un objeto *MovieClip* de flash por cada red encontrada y lo dibujará en el mapa. Cada red inalámbrica será representada por este objeto de Flash que tendrá un color aleatorio para diferenciar cada punto de acceso. A continuación se muestra el código *ActionScript* que logra esta funcionalidad:

```
#include "lmc_tween.as"
oXml = new XML();
oXml.ignoreWhite = true;
oXml.load("redInaP.xml");
oXml.onLoad = function (success)  {
   if(success)  {
numRedes = oXml.firstChild.childNodes.length;
                        var datosRedesI:Array = new Array();
                        for (var i:Number = 0; i<numRedes; i++){
                        datosRedesI.push([
                                                oXml.firstChild.childNodes[i].attributes.id,
                                                oXml.firstChild.childNodes[i].attributes.posxm,
                                                oXml.firstChild.childNodes[i].attributes.posym,
                                                oXml.firstChild.childNodes[i].attributes.ssid ]);
                                                }
for(var k:Number = 0; k < numRedes; k++)   {
                        var mc:MovieClip = punto.duplicateMovieClip("item"+k, k);
                        color = Math.round(Math.random()*0xFFFFFF);
                        mc.colorTo(color,0);
                        var mposx:Number=datosRedesI[k][1];
                        var mposy:Number=datosRedesI[k][2];
```

```
                                    if( ((mposx>10) and (mposx<610)) and ((mposy>30)and(mposy<630)))  {   mc._x = mposx;
            mc._y = mposy;          }
                        else {      mc._x = 0; mc._y = 0;   }
            }//for
}//if

else{trace("No se pudo cargar el XML");}
}//function
setProperty("punto",_visible,0);
```

La segunda fase se encarga de consultar el archivo XML para obtener la información relacionada con el punto de acceso dibujado en el mapa. Esta información será mostrada cada que se seleccione el punto de acceso en el mapa, de esta manera se hace una consulta al archivo para traer los datos que coincidan con la ubicación del mapa. En esta etapa se estarán esperando eventos del mouse, es decir que cada que se seleccione un punto de acceso o se pase por encima del objeto de flash que indica el punto de acceso habrá una acción. Cuando se seleccione se traerán los datos y se mostrarán en los campos de información, cuando se pase sobre él se mostrará el SSID de red en la parte inferior izquierda de la aplicación.

Esta aplicación podrá ser visualizada por usuarios con cuenta de tipo administrador y usuarios que tengan cuenta de consulta, por lo que el *jsp* que publique esta aplicación deberá verificar la sesión de usuario que esté abierta.

```
on(press){
            var oXml:XML = new XML();
            oXml.ignoreWhite = true;
            oXml.load("redInaP.xml");
            oXml.onLoad = function(exito) {
                        var posxp:Number=getProperty(_target,_x);
                        var posyp:Number=getProperty(_target,_y);
                        if (exito) {
                                    for(var i:Number=0; i< oXml.firstChild.childNodes.length;i++){
                                                var posxpm:Number=oXml.firstChild.childNodes[i].attributes.posxm;
                                                var posypm:Number=oXml.firstChild.childNodes[i].attributes.posym;
                                                if((posypm==posyp) and (posxpm==posxp)){
                                                            _root.ssidD.text =oXml.firstChild.childNodes[i].attributes.ssid;
                                                            _root.canalesD.text=oXml.firstChild.childNodes[i].attributes.canales;
                                                           .
                                                            .
                                                            _root.posx.text = osxpm;oXml.firstChild.childNodes[i].attributes.posxm;
                                                _root.posy.text = osypm;oXml.firstChild.childNodes[i].attributes.posym;}}}//if
                        else{  trace("Error"); }//else   }//function  }//onpress

on(rollOver) {
            var oXml:XML = new XML();
            oXml.ignoreWhite = true;
            oXml.load("redInaP.xml");

oXml.onLoad = function(exito) {
                        var posxp:Number=getProperty(_target,_x);
                        var posyp:Number=getProperty(_target,_y);
                        if (exito) {
for(var i:Number=0;i<oXml.firstChild.childNodes.length;i++){
                                                var posxpm:Number=oXml.firstChild.childNodes[i].attributes.posxm;
                                                var posypm:Number=oXml.firstChild.childNodes[i].attributes.posym;
                                                if((posypm==posyp) and (posxpm==posxp)) {
                                                            _root.nomRed.text = oXml.firstChild.childNodes[i].attributes.ssid; }}
                        }//if
                        else{  trace("Error");  }//else }//function      }//onrollOver
```

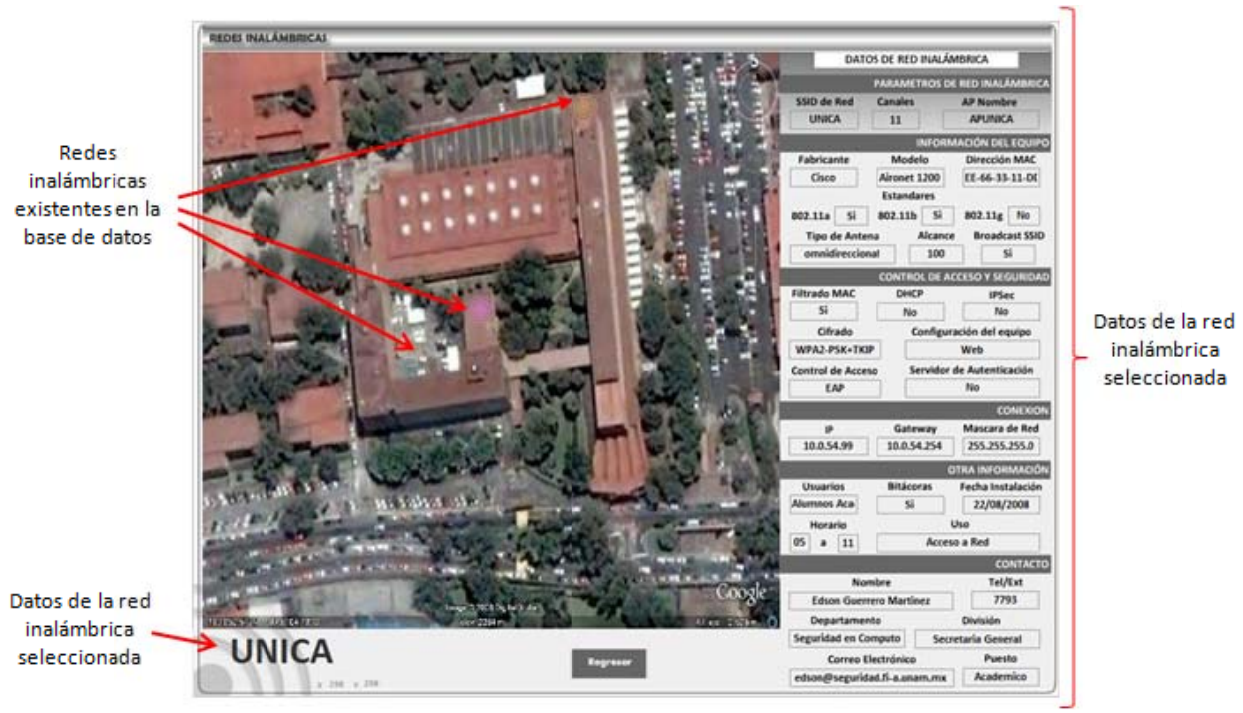


FIGURA 4.14 Aplicación de redes inalámbricas con datos

4.5.3 IMPLEMENTACIÓN DEL C3. COMPONENTE DE ADMINISTRACIÓN DE REGISTROS DE LA BASE DE DATOS DE LAS REDES INALÁMBRICAS

El componente de administración de registros de la base de datos se desarrolló en base a los requerimientos del sistema, se implementó una página que muestre las tres actividades establecidas para el administrador del sitio, estas actividades contemplan la edición de datos, edición de ubicación y la eliminación de registros de redes inalámbricas. Esta página presentará 3 combos de selección que serán llenados con información de los registros de la base de datos, para diferenciar la elección de la red se llenarán con el SSID-AP_NOMBRE-LOCALIZACION de esta manera se identificará con facilidad la red inalámbrica.

FIGURA 4.15 Administración de registros

- La primera funcionalidad de este componente es la edición de datos, como nombre del contacto, parámetros de la red inalámbrica, etcétera. Se seleccionará una red del combo y se llenará el formulario inicial de registro con los datos de la red seleccionada. Una vez que estén los datos en el formulario serán editables los campos, cuando se hayan modificado los campos se enviarán los datos y se volverán a validar de igual manera a como se realizó en el procedimiento de registro.
- La segunda funcionalidad es la de edición de ubicación. Cuando se haya elegido un registro y se pulse el botón de enviar, la siguiente página será la aplicación de ubicación de red inalámbrica en el mapa. De igual manera de cuando se ubicó el punto de acceso en el mapa se enviarán los datos a la base para ser actualizados.
- La tercera funcionalidad es la de eliminación de registro de red inalámbrica. Cuando se elija un registro del combo de selección y se pulse el botón de *Eliminar* se enviará a la página que elimina ese registro de la base de datos, esto se hace de manera inmediata por lo que una vez pulsado el botón de eliminar el registro no existirá más en la base de datos.

Todas estas actividades serán tareas exclusivas del administrador del sistema, por lo que la validación de las sesiones será de manera obligatoria para cada *jsp* que se ejecute en estos procedimientos.

4.5.4 IMPLEMENTACIÓN DEL C4. COMPONENTE DE AUTENTICACIÓN DE USUARIOS Y SESIONES

El desarrollo de este componente está basado en la verificación de una sesión válida del sistema así como del atributo del tipo de usuario de la sesión. Según el requerimiento R5 que hace referencia al uso de perfiles de usuarios, ya se estableció que serán dos tipos de cuenta la de administrador y la de consulta. Estas credenciales serán validadas con la tabla de usuarios en la base de datos, una vez que se haya verificado la existencia del usuario en el sistema se procederá a crear la sesión del usuario.

Una vez identificado el tipo de usuario se mostrará de inicio la página de control del sistema en donde dependiendo del perfil de usuario se mostrarán las tareas que podrán realizar en el sistema.

```
// Cabeceras del jsp
<%@page import = "java.util.*" session="true"%>
<%

//Código de autenticación del usuario en la base de datos

//si es usuario, crear una sesión según el tipo de cuenta

    session.setAttribute("tipoCuenta",tipoCuenta);
    session.setMaxInactiveInterval(480);
    response.sendRedirect("gestionRedesIna3.jsp");

//si el usuario no existe en el sistema
      response.sendRedirect("ingresar.jsp");
%>
```

```
<%
            HttpSession actualSession=request.getSession(true);
            String
tipoUsuario=(String)session.getAttribute("tipoCuenta");
            if(tipoUsuario ==null)
            {
                        response.sendRedirect("ingresar.jsp");
            }
            if(tipoUsuario==”administrador”)
            {
                        //Codigo de jsp de administrador
            }
            else
            {
                        //Codigo de jsp de consulta
            }
```

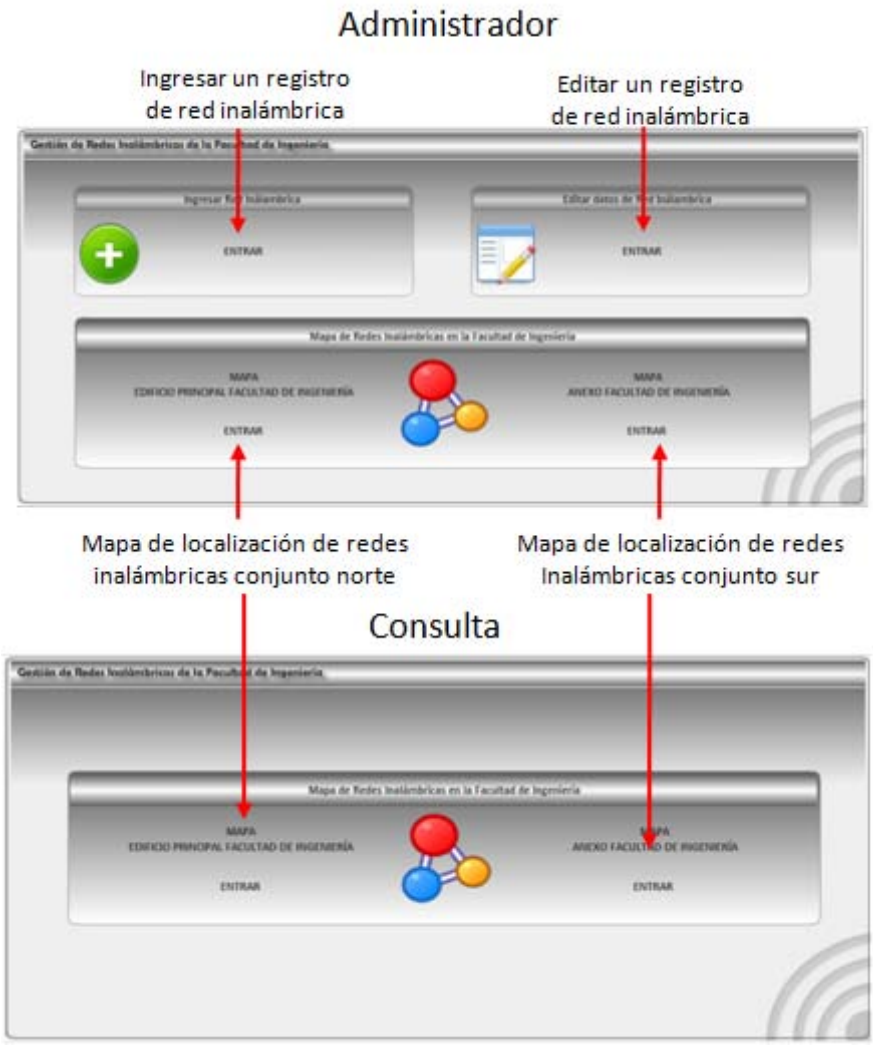


FIGURA 4.16 Perfiles de usuarios

Para ingresar al sistema se presentará una página para ingresar el nombre de usuario y contraseña

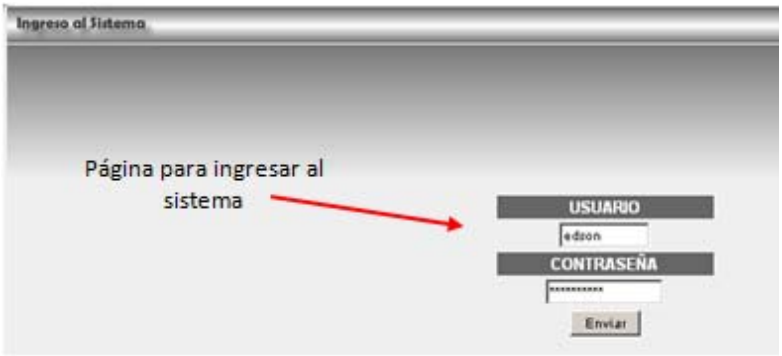


FIGURA 4.17 Ingresar al sistema

4.5.5 IMPLEMENTACIÓN DEL C5. COMPONENTE DE PUBLICACIÓN DE INFORMACIÓN DE LAS REDES INALÁMBRICAS

La implementación del componente C5 de publicación de información que tendrá la tarea de conjuntar al sistema, ya que se desarrollará un sitio Web en donde siempre se tenga la opción de ir a las páginas de publicación de información. Es decir para el desarrollo de este componente se tomará en cuenta la estructura general del sitio. Hasta este momento no se ha mencionado cual es la estructura del sitio, por lo que a continuación se muestra cómo será la estructura del mismo.

Para el desarrollo de la estructura del sitio Web se tomaron en cuenta los requerimientos R6, R7 y R8, en donde se consideran los aspectos relacionados con el diseño del sitio. La publicación de información como lo son las Políticas de Seguridad son un requisito funcional de sistema por lo que esta información deberá siempre estar accesible para el usuario. La manera de lograr que esta información sea accesible todo el tiempo es mediante un menú que esté presente en todo el sistema.

FIGURA 4.18 Estructura del sitio Web

En este menú habrá un enlace a cada página del sitio que presente información que se clasificó como un requisito del sistema, como lo son la página de Estadísticas, Procedimiento de Registro de Red Inalámbrica, la página de Políticas de Seguridad, página de buenas prácticas, página de monitoreo y pagina de auditoría, así como la de ingresar al sistema.

Para complementar la estructura se agregará en la parte inferior del sistema Web una zona de enlaces a sitios de interés como lo es la página de créditos, la página del Departamento de Seguridad en Cómputo, la página de la Unidad de Servicios de Cómputo Académico (UNICA), la página de la Facultad de Ingeniería y la página de la UNAM. La publicación de la información, así como las páginas de administración del sistema quedará en la parte media del sitio Web. De esta manera se logra cumplir el objetivo de tener un sitio Web en donde no represente dificultad al usuario el navegar por él, además de que esta estructura permitirá tener en todo momento un acceso a la información ahí publicada.

La publicación de las Políticas de Seguridad entonces quedará en la parte media de la página, así como se muestra en la siguiente figura. Cabe resaltar que la información ahí publicada será visible a cualquier usuario de Internet, no se necesitará una cuenta de acceso al sistema para poder tener la oportunidad de consultar la información.

FIGURA 4.19 Zona de publicación de políticas

La integración de todos los componentes implementados no representa ningún desarrollo extra debido a la forma en que fue diseñado el sistema Web. Sin embargo el correcto funcionamiento de los componentes funcionando como un sólo sistema se probará en la etapa de pruebas del sistema.

4.6 PRUEBAS DE LA HERRAMIENTA GESTORA DE REDES INALÁMBRICAS

En esta última fase del desarrollo de la herramienta gestora de redes inalámbricas se deberán poner a prueba si los requisitos establecidos en las fases iníciales fueron implementados en la construcción de este sistema. Cabe señalar que en las etapas anteriores se realizaron pruebas de manera individual a cada uno de los componentes desarrollados durante la fase de implementación, por lo que en esta etapa se evaluará al sistema completo ya integrado. En el momento que se encontraron fallas en los componentes desarrollados fueron corregidos para poder cumplir con los requerimientos solicitados

Prueba 1. Registro y ubicación de red inalámbrica.

Esta prueba verificará el buen funcionamiento del sistema para registrar y ubicar redes inalámbricas en la Facultad de Ingeniería. Primero se ingresará al sistema con cuenta de administrador y se procederá a registrar en el formulario los datos de una red de prueba que se usará en todas las pruebas posteriores. Según el diseño del módulo no se permitirá datos erróneos al momento de ingresar la información, es decir se validarán los campos donde el usuario ingrese información. Así mismo otro aspecto importante a probar, es el hecho de no poder registrar una red inalámbrica si ya existe un registro con el mismo nombre del AP y el SSID, cabe señalar que pueden existir 2 o más redes inalámbricas con el mismo SSID pero con diferente nombre del punto de acceso (por ejemplo la RIU) y viceversa.

Cuando se comienza a introducir los datos y se dejan campos vacios o que no corresponden al tipo de dato indicado, el sistema marca el mensaje de en donde se encontró información que no es la correcta o la esperada por el sistema, de esta manera se le indica al usuario en donde deberá corregir su información tomando en cuenta las 5 áreas en que está dividido el formulario.

FIGURA 4.20 Validación de campos del formulario 1

El otro aspecto que se está probando es el de poner el mismo nombre de AP y de SSID con un registro ya existente, aun cuando el tipo de datos es correcto en todos los campos, si la información del nombre de AP y SSID ya existen en el sistema, aparece el mensaje de que es necesario cambiarlos para poder completar el registro.

FIGURA 4.21 Validación de campos del formulario 2

En el momento en que se hayan llenado todos los campos con información correcta y no existe una red inalámbrica registrada con ese nombre de AP y SSID iguales el proceso de registro continua y pasa al siguiente nivel en donde se elige la ubicación de esta red inalámbrica, como ya se mencionó esta podrá ser en el conjunto norte o sur de Facultad de Ingeniería. Este caso de prueba se ubicará en el conjunto norte lo que nos dirige al mapa de la zona. Aquí se puede observar que la información de la red inalámbrica que se está registrando se presenta en la parte inferior de la aplicación.

FIGURA 4.22 Ubicación del punto de acceso

Una vez colocado el punto de acceso se envían estos datos y queda registrada esta red inalámbrica con una ubicación en la zona donde se instaló. De esta forma se puede observar que esta prueba cumple con los requerimientos iniciales de registro de redes inalámbricas.

Prueba 2. Visualizar la red inalámbrica registrada.

Esta prueba de visualizar las redes registradas se seguirá desarrollando con el mismo caso de la red que se acaba de registrar. Para probar si esta red registrada está visible en la zona en la que se dio de alta se procede a abrir la parte donde se visualizan las redes inalámbricas en el conjunto norte, al momento de abrir esta aplicación se pude observar que existen algunas otras redes inalámbricas en esta zona, así mismo podemos observar la existencia de la red que registramos y si le damos clic sobre el punto de acceso nos muestra la información de la red inalámbrica que acabamos de registrar.

FIGURA 4.23 Visualización de redes inalámbricas

De esta forma se verifica que este módulo cumple con el requerimiento de visualización de las redes inalámbricas de la zona según los registros en la base de datos.

Prueba 3. Editar datos y ubicación de red inalámbrica registrada.

La siguiente prueba de funcionamiento es la de edición de datos y ubicación de los registros. Este proceso se inicia con la elección de la red inalámbrica a la cual se le modificarán sus datos. En la página de administración de registros se presentan combos de selección con las redes inalámbricas existentes, una vez elegido el registro a modificar se procede a la siguiente fase en donde se editará la información de la red seleccionada.

FIGURA 4.24 Selección de registro para la edición de datos de red inalámbrica

Cuando se eligió el registro indicado el sistema nos envía al formulario en donde se ingresaron los datos inicialmente con los campos llenos de la información que se tiene de esa red inalámbrica, una vez en este formulario se puede modificar cualquier dato, sin embargo al igual que en el formulario inicial estos datos serán validados de nuevo así como verificar la existencia de redes inalámbricas con ese mismo SSID y nombre de APs. Cuando los datos estén correctos la información en la base de datos se actualizará.

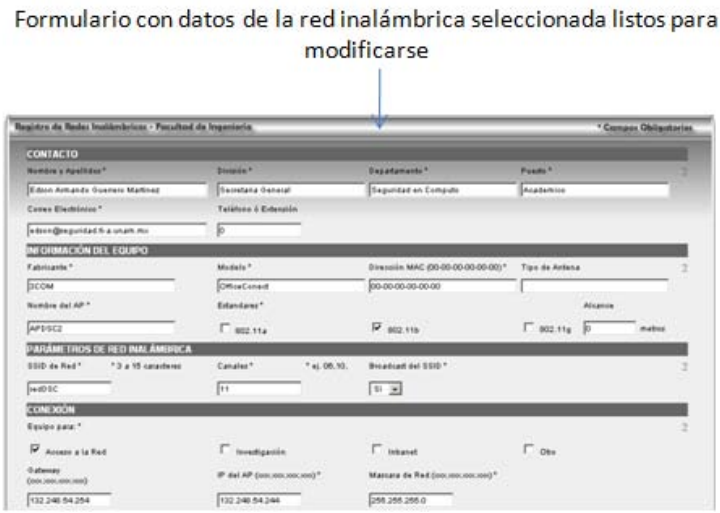


FIGURA 2.25 Formulario para edición de datos

Para modificar la ubicación de un registro de la red inalámbrica se procede de manera similar sólo que se elige el registro del combo de selección correspondiente a la edición de ubicación. Una vez seleccionado el sistema nos envía al mapa correspondiente de la zona en donde podremos volver a ubicar el punto de acceso de la red inalámbrica seleccionada. En el momento de enviar la nueva ubicación se actualizará en la base de datos y se podrá visualizar la nueva localización en la aplicación que permite localizar las redes inalámbricas en el mapa.

FIGURA 2.26 Ubicación modificada

Prueba 4. Eliminar la red inalámbrica registrada.

Para probar esta funcionalidad se procederá de la misma manera que la edición de datos, se seleccionará la red inalámbrica que se desea eliminar del combo de selección de eliminar una red inalámbrica del sistema y se enviarán los datos. Este procedimiento es directo, es decir no hay una confirmación ni advertencia de la eliminación del registro así que una vez enviado el registro que se desea eliminar, éste no existirá más en la base de datos.

FIGURA 4.27 Eliminar registro de red inalámbrica

Prueba 5. Ingresar con los dos perfiles de usuario existentes en el sistema y verificar las tareas que se pueden realizar.

El sistema fue desarrollado para funcionar en base a perfiles de usuarios, por lo que habrá que probar que al momento de ingresar con determinado tipo de cuenta de usuario se permitan o denieguen tareas en el sistema, según los requerimientos existen dos tipos de cuentas de usuarios la de administrador y la de consulta. Para probar esta funcionalidad es necesario ingresar al sistema con una cuenta de administrador, una de consulta y una cuenta que no exista, de esta forma se observará el comportamiento del sistema ante los posibles usuarios del sistema.

FIGURA 4.28 Perfil de usuarios

Esta funcionalidad de los perfiles de usuarios funciona según lo establecido y diseñado por las etapas previas al desarrollo por lo que se procede a la siguiente prueba del sistema.

Prueba 6. Verificar la zona de publicación de la información.

Esta prueba tiene que ver con la funcionalidad de publicación de información en el sistema Web, como se estableció en los requerimientos se podrá publicar información en el sistema y que esté disponible a cualquier usuario de Internet, por lo que el sistema deberá contar con páginas destinadas a esta actividad. La estructura de diseño del sitio permite al usuario navegar dentro del sitio Web de manera que pueda acceder a las diferentes páginas donde se presente información sin perderse en el sitio, es decir debe de tener la capacidad de ser lo más accesible al usuario de manera fácil y agradable.

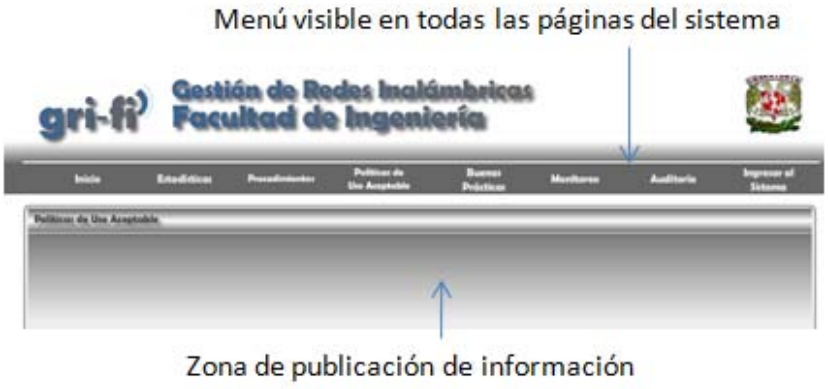


FIGURA 4.29 Barra de menú del sitio Web

Conclusiones de las Pruebas

La demostración de estas pruebas trato de involucrar los requisitos establecidos para verificar las que las funciones del producto se desarrollaron según lo diseñado por lo que se observó que el sistema está listo para iniciar un periodo de pruebas con información e interacción directa con los usuarios.

CAPÍTULO

5

IMPLANTACIÓN DE MEDIDAS DE GESTIÓN

En el capítulo anterior se implementó el sistema de gestión de redes inalámbricas el cual hasta este momento no cuenta con la información real requerida, es por ello que en los siguientes capítulos se desarrollará la información necesaria para cumplir con el objetivo principal de este trabajo de tesis que es gestionar de una manera adecuada el aspecto normativo, administrativo y de seguridad de las redes inalámbricas dentro de la Facultad de Ingeniería.

5.1 SISTEMA DE GESTIÓN DE REDES INALÁMBRICAS

El sistema de gestión de redes inalámbricas que se desarrolló fue diseñado conforme a las necesidades de información y control que existen, al momento, en relación al manejo y administración de este tipo de tecnologías dentro de la institución. Su función principal es la de tener una plataforma que permita el controlar el registro y ubicación de las redes inalámbricas, así como la publicación de información relacionada como las Políticas de Redes Inalámbricas de la Facultad de Ingeniería, buenas prácticas, recomendaciones de monitoreo y auditoría sobre dispositivos inalámbricos.

La administración de este sistema estará a cargo del Departamento de Seguridad en Cómputo de la Unidad de Servicios de Cómputo Académico de la Facultad, trabajando en coordinación con el Departamento de Redes y Operación de Servidores perteneciente a esta misma unidad, de esta manera se logrará la conjunción en operación y seguridad en redes inalámbricas.

La utilización de este sistema representará una herramienta de apoyo para administrar las comunicaciones inalámbricas de mejor forma al permitir la consulta de información de redes existentes en áreas comunes y poder gestionar los canales de comunicación y evitar al máximo el solapamiento de las redes. Además servirá como medio de comunicación para la difusión de las Políticas de Seguridad de Redes Inalámbricas también como información relacionada con buenas prácticas, monitoreo, auditoría.

La información que se llegue a almacenar en este sistema servirá de consulta para administradores de redes inalámbricas, usuarios y a la comunidad estudiantil en general. El mismo Departamento de Seguridad en Cómputo se encargará de tener actualizada la información ahí presentada y añadiendo en caso de ser necesario, la publicación de actualizaciones a las Políticas de Seguridad de Redes Inalámbricas en la Facultad de Ingeniería.

En este sistema, se centraliza la estrategia propuesta como solución a la situación actual que vive la Facultad de Ingeniería, la aplicación y seguimiento de lo aquí expresado dependerá de la previa autorización de las autoridades competentes.

5.1.1 HERRAMIENTA PUBLICADA EN WEB

La herramienta Web que se desarrolló deberá ser puesta en funcionamiento para cumplir con unas de sus principales funciones que se plantearon: la publicación de las políticas y procedimiento de registro de las redes inalámbricas. La razón de que sea un sitio Web es que permitirá la gestión de este sistema desde cualquier sitio donde se cuente con Internet y así los usuarios tendrán disponibilidad de la información en todo momento.

La solicitud de ser un usuario de este sistema será procesada directamente con el Departamento de Seguridad en Cómputo, ya que será el encargado de la administración del sitio Web. Es importante señalar que los usuarios que puedan llegar a tener cuenta de **consulta** de información de los mapas de las redes inalámbricas serán responsables con la información ahí presentada, ya que se podrán obtener datos de red y configuración de equipos que forman parte de la infraestructura de red y en manos equivocadas esto pudiera ser peligroso.

El sitio Web que se desarrolló tiene la capacidad de ser portable, lo que significa que con un mínimo de arreglos podrá instalarse en plataformas *Linux* y *Microsoft Windows*, esto ha sido probado en los sistemas operativos *Debian* y *Microsoft Windows XP*.

El nombre que se le dio a este sistema Web es propuesto por el mismo Departamento de Seguridad en Cómputo. El significado de GRIFI viene directamente de lo que pretende ser este sistema Web, **G**estión de **R**edes **I**nalámbricas en la **F**acultad de **I**ngeniería. Así mismo el diseño y contenido es responsabilidad del Departamento de Seguridad en Cómputo.

5.1.2 ESTADÍSTICAS AUTOMATIZADAS

El conocimiento del panorama que vive la Facultad de Ingeniería con relación a la existencia de redes inalámbricas se verá reflejado en la funcionalidad de sistema Web que de manera automatizada genere gráficas con estadísticas que permitan conocer aspectos relevantes del uso y configuraciones que se utilizan. El tener la información de cuáles son los canales de comunicación más utilizados, así como a quienes están dirigidas las redes inalámbricas es decir quiénes son los usuarios finales de este tipo de redes, servirá para orientar la toma de decisiones en cuanto a esta tecnología de información se refiere.

Las estadísticas serán un complemento del sistema Web que estarán visibles a cualquier usuario de Internet, en estas gráficas se podrá vislumbrar la actual proliferación y popularidad de las redes inalámbricas dentro de la Facultad de Ingeniería. Estos datos representan un aspecto innovador ya que no existen registros previos de instituciones que generen este tipo de información.

La información que se publicará ha sido seleccionada de forma cuidadosa y que represente la actualidad de esta tecnología en la institución. La obtención de estos datos será directamente de la base de datos en

dónde se almacenan los registros del sistema Web desarrollado, por lo que se deberán actualizar en cada modificación que se genere en el sistema.

Para esta tarea de la publicación de estadísticas se eligió la misma tecnología bajo la cual se ha desarrollado el sitio Web. La combinación de *Flash* con *XML* es en conjunto una tecnología actual muy utilizada para el desarrollo de gráficas dinámicas para Web. Después de hacer un análisis del software existente para la implementación de gráficas dinámicas Web que funcionan bajo el esquema de licencia de uso libre se eligió *FusionCharts Free.*

FusionCharts Free son componentes de flash que generan gráficos de manera dinámica, están desarrollados en *Macromedia Flash MX* y tienen soporte para lenguajes de programación como *PHP, ASP, .NET, JSP,* etcétera. Mediante el uso de archivos *XML* como origen de datos, estas animaciones generan gráficos interactivos y visualmente muy atractivos. La versión que se utilizó es de uso libre y es reducida de la que se distribuye de manera comercial, sin embargo las funcionalidades que ofrece son suficientes para el desarrollo de este sistema Web.

La selección de la información que se presentará en el sistema Web fue dividida en cuatro áreas, las cuales estarán accesibles a partir de un menú de gráficas donde se pueda ver la información referente a cada área.

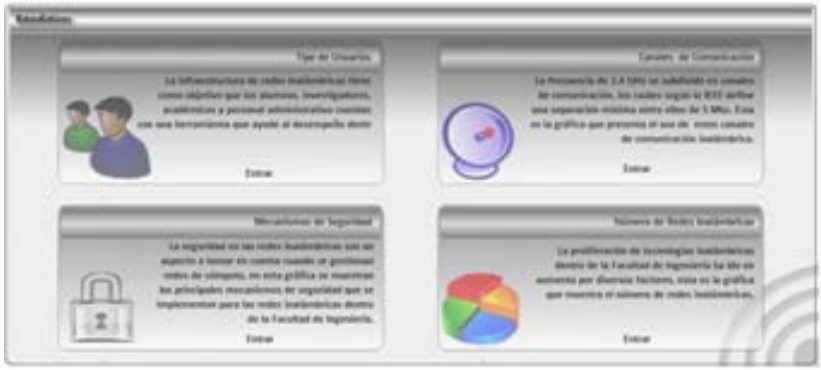


FIGURA 5.1 Menú de estadísticas de redes inalámbricas

1. Tipo de usuarios de las redes inalámbricas.

En esta gráfica se mostrará a quienes están dirigidas las redes inalámbricas dentro de la Facultad de Ingeniería. En el momento que se registraron en la base de datos las redes inalámbricas se diseño un campo para obtener esta información y poder generar información de quienes son los usuarios de estas redes. Los cuatro grupos de usuarios que se tiene dentro de la institución son alumnos, académicos, investigadores y personal administrativo.

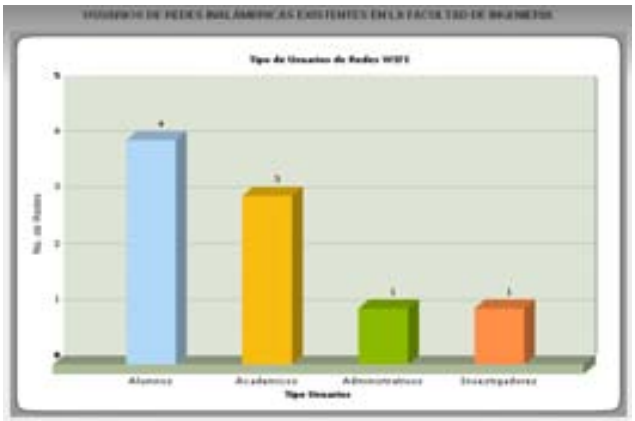


FIGURA 5.2 Gráfica de tipos de usuarios de las redes inalámbricas

2. Canales de comunicación inalámbrica utilizados.

En esta gráfica se muestra el uso de los canales de comunicación inalámbrica. Como se mencionó en los problemas que pueden llegar a presentar las redes inalámbricas cuando coexisten en una misma zona geográfica en el uso del mismo canal de comunicación por varias redes y por esta razón el funcionamiento no es el óptimo, esta gráfica podrá visualizar cuáles son los canales más utilizados.

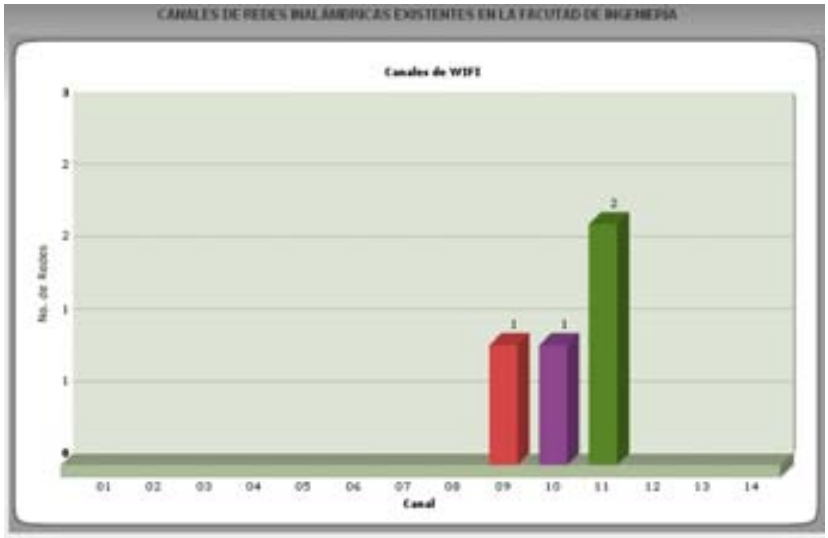


FIGURA 5.3 Gráfica de utilización de los canales de comunicaciones inalámbricas 802.11

3. Mecanismos de seguridad implementados.

Esta información deberá reflejar lo establecido por las políticas de redes inalámbricas de la Facultad de Ingeniería, ya que si se aplican estas normas los mecanismos de seguridad y cifrado de información serán los establecidos como recomendables para su uso. Así mismo deberá reflejar que no existan redes inalámbricas abiertas, ya que esto significaría una posible amenaza por carecer de seguridad de autenticación. También se podrá observar cuántas redes inalámbricas aplican mecanismos de seguridad como un servidor de autenticación.

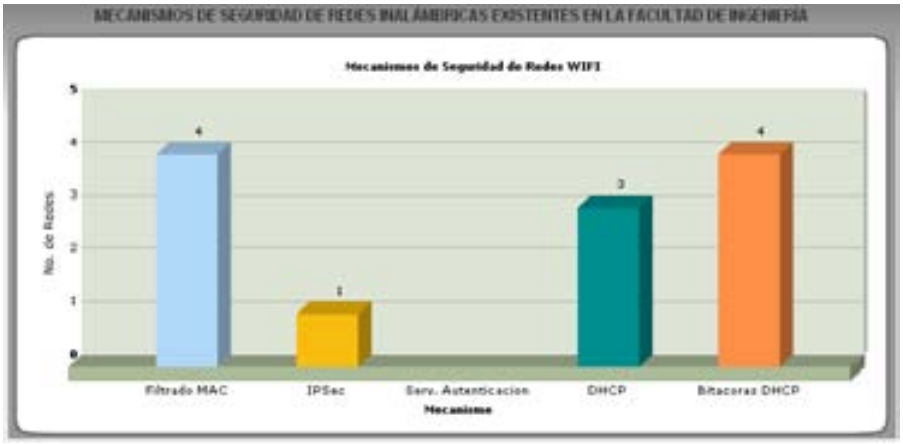


FIGURA 5.4 Gráficas de mecanismos de seguridad en redes inalámbricas

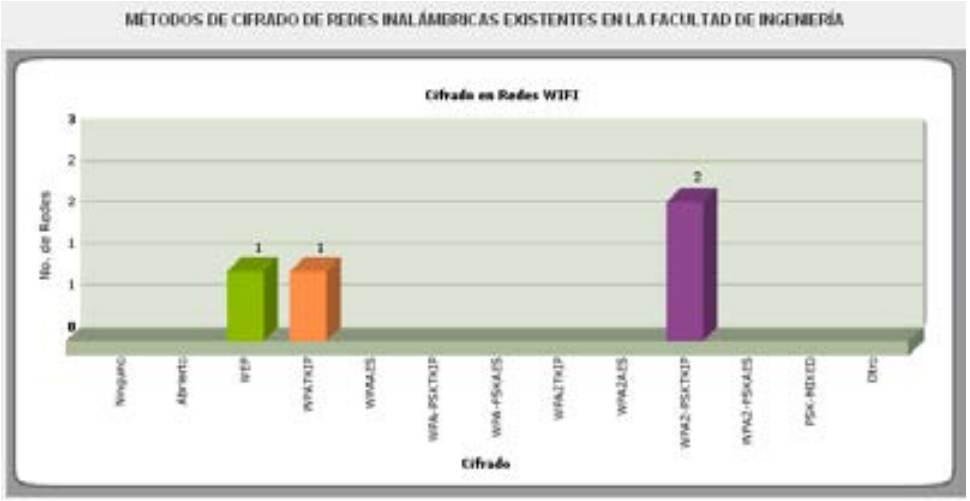


FIGURA 5.4 Gráficas de mecanismos de seguridad en redes inalámbricas

4. Número de redes inalámbricas dentro de la Facultad de Ingeniería.

Esta información representará cuántas redes inalámbricas existen actualmente en la Facultad de Ingeniería dividida en las zonas que se establecieron: conjunto norte y sur de la Facultad de Ingeniería. Además se publicará una gráfica de línea de tiempo que muestre como han ido apareciendo las redes inalámbricas conforme pasa el tiempo de donde se podrá deducir si van aumentando o disminuyendo. Estos datos de la fecha serán obtenidos del campo del formulario donde se introdujo la fecha de inicio de funcionamiento.

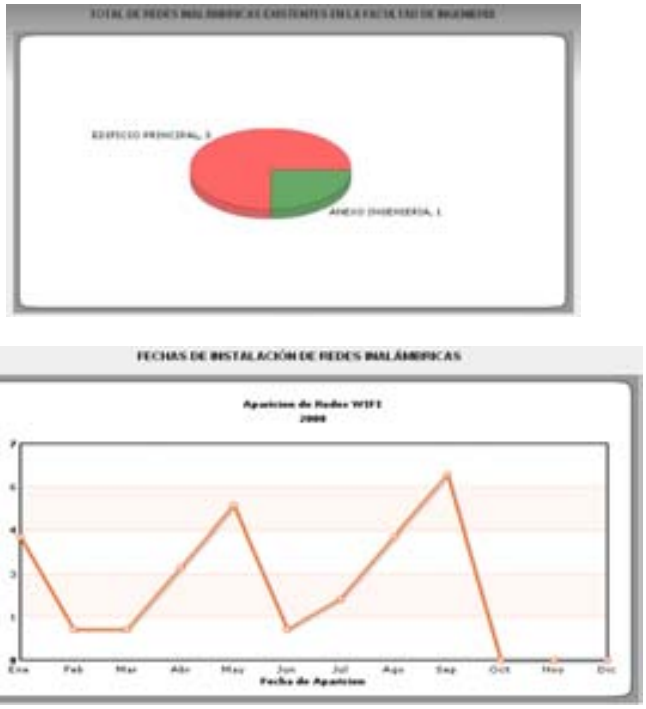


FIGURA 5.5 Gráficas de número de redes inalámbricas y gráfica de tiempos de aparición

Todas estas gráficas son muestras de datos prueba, por lo que la información mostrada no es real, sólo fue para ejemplificar la forma de las gráficas. Esta información será visible a los usuarios de Internet por lo que no se requiere de una cuenta del sistema.

5.2 POLÍTICAS

Como se mencionó en el capítulo III, las políticas de seguridad tienen un ciclo de vida que comprende varias etapas, la primera de ellas es la creación de las políticas y fue desarrollada en el ese mismo capítulo, posteriormente el siguiente paso a la creación es la Revisión y Aprobación de las mismas por lo que estas fases deberán ser implementadas por el área competente.

La siguiente etapa dentro del ciclo de desarrollo de las políticas es la de Implementación, esta fase comprende 3 aspectos que son: la Comunicación, el Cumplimiento y las Excepciones. Dentro de los objetivos de este trabajo de tesis se incluye la etapa de Comunicación.

5.2. 1 PUBLICACIÓN

Difundir las políticas es una fase elemental dentro de su ciclo de vida, ya que si la comunidad a la que están dirigidas desconocen su existencia, no podrán aplicarse para lograr el objetivo que persiguen. Es por ello que su publicación deberá realizarse por medios que aseguren que los involucrados tengan acceso a ellas en el momento en que sean requeridas.

Las políticas deben de ser difundías a la comunidad universitaria o a quienes sean afectados directamente por la política (alumnos, académicos, personal administrativo, personal encargado de áreas de cómputo, etcétera). La responsabilidad de difundirlas recae en primer lugar en el Departamento de Seguridad en Cómputo, quien deberá asegurar que estas estén disponibles, después está la responsabilidad de los jefes de área y responsables de sistemas quienes deberán de esparcir el conocimiento de la existencia de políticas que rigen las comunicaciones inalámbricas.

Esta etapa implica determinar el alcance y el método inicial de distribución de la política, por lo que se refiere al método de distribución inicialmente se contempla únicamente la publicación de esta normatividad en el sitio Web, lo que permite determinar el alcance al estar disponibles en una sitio Web la información puede ser atendida por la comunidad de la Facultad, sin embargo la complejidad de este método de distribución será la difusión que se le pueda dar al sitio Web por otros medios, ya sea por medios escritos como la Gaceta de Ingeniería, revistas internas de las áreas de la Facultad o hasta medios electrónicos como el correo electrónico.

Las políticas deben estar en un documento que sea fácil de acceder a él y descárgalo para imprimirlo y guardarlo. Es por ello que se deberá tener la opción de descargar este documento desde el sitio Web en formato PDF.

5.2.2 MECANISMOS DE DIFUSIÓN

Debe planificarse esta etapa con el fin de determinar los recursos necesarios y el enfoque que debe ser seguido para mejorar la visibilidad de la política. Aun cuando las políticas desarrolladas se encuentran disponibles en todo momento para los miembros de la institución, se debe de hacer conciencia de que estas políticas pueden cambiar en cualquier momento. El Departamento de Seguridad en Cómputo debe de trabajar en este aspecto para asegurar que todos los jefes de áreas y departamentos estén informados al respecto y permitir que ellos puedan filtrar la información en sus respectivas áreas.

No se debe de subestimar la parte de la comunicación de las políticas a los involucrados por ellas, ya que si estas políticas no se leen no se podrán poner en práctica. Dependiendo del tamaño en las organizaciones y de la madurez del proceso de desarrollo de las políticas esto va a ser más o menos complejo, las instituciones pequeñas tienen un menor trabajo en esta parte ya que la logística de difusión es menos compleja para alcanzar a todos los miembros y hacerles ver que deben de leerla y cumplirla. De cualquier forma, hacer que los usuarios lean la política es un desafío, especialmente cuando se realiza algún cambio dichas políticas.

Una forma de hacer frente a este problema sería el incluir el documento de las políticas de uso y seguridad en documentos oficiales, como por ejemplo cuando se hacen los contratos de trabajo, se deberán incluir y hacerle énfasis al nuevo miembro de la institución en la existencia de estas políticas, así como de sus respectivas sanciones en caso de no cumplirlas; otras formas de difusión podrían ser el poner documentos impresos en las áreas de registro y firma por parte del personal académico o dónde se realiza el pago al personal.

Cuando se den cursos de capacitación al personal sobre cómputo ya sea al inicio o al final de las actividades se debiera hacer conciencia de la normatividad existente en la institución, de esta forma se estarían difundiendo por un mayor número de medios las políticas.

El correo electrónico también es una posibilidad de medio de difusión de las políticas y sus probables actualizaciones. Este medio funciona de una manera rápida y efectiva, en donde se podrá incluir información del sitio en donde además se encuentran publicadas.

Una estrategia efectiva de sensibilidad de la seguridad permitirá que la comunidad esté pendiente de las políticas de seguridad, saber dónde las pueden encontrar y cómo aplicarlas, así como las consecuencias en caso de no cumplirlas.

5.2.3 MONITOREO DE REDES INALÁMBRICAS

Se utiliza el término de *Monitoreo* para designar el tipo de acciones consistentes en obtener información de las redes inalámbricas con el fin de detectar anomalías. Estas acciones son pasivas y su único objetivo es conocer el comportamiento respecto al tráfico del sistema de comunicación. Una vez que se conoce el sistema se puede proceder al control, implicaría acciones activas para solucionar las anomalías detectadas en esta actividad.

En el proceso de monitoreo de una red inalámbrica se consideran una serie de pasos como son: en primer lugar, una definición de la información que se monitoriza, una forma de acceso a la información de monitorización, un diseño de los mecanismos de monitorización y, finalmente, un procesado de la información de monitorización obtenida.

Por otra parte, la información de monitorización puede clasificarse según su naturaleza temporal en: información estática que se almacena en los elementos monitorizados; información dinámica que se almacena en los propios elementos o equipos especializados e información estadística que se genera a partir de la información dinámica y que puede residir en cualquier lugar que tenga acceso a la información dinámica.

5.2.3.1 SISTEMAS DETECTORES DE INTRUSOS

Como se observó en el capítulo II en el tema de Inseguridad, existen una gran cantidad de formas de vulnerar las redes inalámbricas, así que para asegurarla se necesita saber cuáles son los puntos de acceso existentes, que acciones tomar para deshabilitar puntos de acceso no autorizados que no cumplan con las

políticas de seguridad, saber que usuarios están conectados a la red inalámbrica, y saber qué tipo de información está viajando por ese medio sin ser cifrada. Para saber esto se debe monitorear el espacio aéreo con Sistemas Detectores de Intrusos de redes inalámbricas.

Una intrusión es cuando alguien intenta romper un sistema de información, un Sistema Detector de Intrusos (*IDS, Intrusion Detection System*) sirve para detectar dichas irrupciones. Un IDS de red esta monitoreando continuamente los paquetes de información buscando descubrir cualquier intento de filtraciones a los sistemas, además puede determinar otro tipo de ataques como lo son intentos de Denegación del Servicio (*DoS*) y en algunos casos puede también responder a tráfico de red malicioso y re-direccionarlo para ser bloqueado por el Firewall.

Un IDS puede correr sobre una máquina que este monitoreado su propio tráfico y sólo son procesados los paquetes que lleguen al equipo y se alerta cuando se detecte actividades anómalas. Alternativamente un IDS puede funcionar en una máquina independiente la cual este observando en *modo promiscuo* todo el tráfico de la red, este tipo de IDS's son colocados en puntos estratégicos como medida de monitoreo máximo de la red.

La necesidad de un detector de intrusos para las redes inalámbricas se ha convertido en una parte fundamental para la infraestructura de seguridad para este tipo de redes. La manera en que trabaja un IDS en las redes inalámbricas es muy diferente a como funcionan en las redes cableadas ya que en las redes cableada se tiene control total de qué tipo de tráfico circula por ella, sin embargo en las inalámbricas se utiliza el aire como medio de trasmisión lo que significa que el tráfico de red se envía a todos los dispositivos cercanos.

Existen Detectores de Intrusos de Redes Inalámbricas (*Wireless Intrusion Detection System, WIDS*) que pueden ser obtenidos de manera comercial como *Airdefense RogueWatch, Airdefense Guard* y otro es el *Internet Security System RealSecure Server*, pero también existe software con licencias libres como *Snort-Wireless* y *WIDZ*, para el sistema operativo Linux.

Típicamente las redes inalámbricas cubren una gran extensión de área para dar acceso a un número mayor de clientes, para estos casos se debe de instalar un IDS por cada punto de acceso para que puedan ser detectados la mayoría de los intentos de ataques e identificar más fácilmente a los intrusos en una gran infraestructura de red inalámbrica.

La detección de la localización física de un atacante es un aspecto crítico de los detectores de intrusos para las redes inalámbricas, los ataques son normalmente en una zona muy cercana al punto de acceso y más probable aun es que estos ataques se realicen en un periodo corto de tiempo para evitar la detección. Cuando se aplica una respuesta al incidente, es imperativo que no sólo la respuesta sea de tipo lógica (bloquear o cortar la conexión de la IP sospechosa y alertar a los Firewalls), además necesita incorporar una exploración física de los individuos para identificar al atacante, esta información de la ubicación también puede ser obtenida a partir de los IDS inalámbricos. La utilización de antenas direccionales puede ayudar al IDS a identificar el área de ubicación, u otras opciones que nos puede ofrecer *Kismet* para identificar el vecindario de la red inalámbrica.

Los IDS de redes inalámbricas también pueden ayudar a robustecer las políticas de seguridad, si se tiene una política de seguridad se debe de desarrollar y reforzar apropiadamente, permitiendo mitigar las vulnerabilidades de este tipo de redes. La mayoría de las políticas de seguridad aplicadas a redes inalámbricas sugieren que las comunicaciones deben ser cifradas, por lo tanto de se debe monitorear el tráfico 802.11 y las comunicaciones del AP con otros dispositivos, con un IDS de redes inalámbricas se puede alertar cualquier tráfico sin cifrar que haya sido detectado.

Otro atributo que puede ser implementado sobre los IDS de redes inalámbricas es crear una lista o pre-configurarla en el software con todos los puntos de acceso conocidos y autorizados, de esta manera cualquier AP desconocido y no autorizado será detectado con rapidez por el IDS y podrá alertar al respecto. Adicionalmente esta tarea automatizada ayuda a reforzar las políticas de seguridad ya que el personal que se destinaría para realizar la tarea, ahora se podría implementar de manera automatizada.

Existen un número considerable de IDS para redes inalámbricas disponibles en Internet que pueden ser adquiridos con licencia y algunos otros que son de uso libre. A continuación de describen algunos de estos programas:

- *Airdefense Guard* es un IDS para redes inalámbricas distribuido de manera comerciar creado por *AirDefense Inc.* Es un detector de intrusos para redes inalámbricas 802.11 a/b/g además de ser una solución de seguridad que identifica riesgos de seguridad y ataques, provee auditoría y monitoreo de la red en tiempo real para un mejor control de la red inalámbrica. Es capaz de detectar APs no autorizados y asegura la red inalámbrica reconociendo y respondiendo ante intrusos y ataques que estén siendo detectados. Permite la auditoría en tiempo real de la red para inventariar todo el hardware, los parámetros de la red así como administración y refuerzo de las políticas de seguridad; el monitor vigila la salud de la red identificando y respondiendo ante fallas de hardware, interfaces de red y degradación del funcionamiento.

- *Neutrino Wireless Sensor* está equipado con su propio agente de vigilancia inteligente, este IDS mira los paquetes, dispositivos y clientes para automáticamente detectar una multitud de condiciones que podrían influenciar en la seguridad y rendimiento de la red inalámbrica. *Neutrino Sensors* son unos pequeños dispositivos de hardware que incluyen dos adaptadores de red, uno para el protocolo 802.11 y otro para Ethernet.

- *WIDZ* es un IDS para redes inalámbricas, resguarda los AP y monitorea las frecuencias locales en busca de actividad maliciosa. Detecta escaneos, asociaciones de inundación y falsos AP o no autorizados.

- *Snort-Wireless* es un detector de intrusos de software libre y fácilmente escalable que puede ser integrado al IDS de la infraestructura cableada, es completamente compatible con *Snort 2.0.x* y añade diferentes funcionalidades, detecta dispositivos AP no autorizados, redes *Ad-Hoc* y detecta el uso de software como *Netstumbler*.

5.2.3.2 HERRAMIENTAS DE MONITOREO

Existe una gran variedad de herramientas que pueden ayudar a mantener la integridad de la red inalámbrica en estado saludable, esta gran variedad de herramientas muestran lo que está sucediendo en la red, algunas de estas con un propósito especifico como la saturación del ambiente en cuanto a comunicaciones inalámbricas hasta monitoreo de servicios de red específicos como servidores HTTP, SMTP (*Send Mail Transfer Protocol*), etcétera. Cuando monitoreamos la red podemos tener el conocimiento de cómo se está comportando ante situaciones de congestiones en la red, cuando se sufre de la propagación de *malware* y otras actividades que se necesitan tener controladas. Como se mencionó con anterioridad existen herramientas de uso de licencia comerciar y uso de licencia libre, a continuación se describen algunas herramientas que son de las más populares en este tipo de *software*.

5.2.3.3 *WIRESHARK (ETHEREAL)*

Es una herramienta analizadora de protocolos (anteriormente conocida como *Ethereal*) para solución de problemas, análisis, desarrollo de software y protocolos de red. Su funcionamiento está basado en la

captura de paquetes de información que estén pasando por la red, estableciendo la tarjeta de red en modo promiscuo; tiene una gran variedad de filtros de información que son presentados en una interfaz gráfica.

La capacidad de filtrar información puede ser explotada de dos maneras, una desde la red de datos directamente y estar filtrando esa información o desde archivos guardados con tráfico de red para análisis más minuciosos, se puede analizar cada paquete de información para ver cabeceras, *payload*, etcétera. La capacidad que tiene este software para hacer filtros lo ha colocado dentro del software más utilizado por administradores de redes. *Wireshark* además, es un software que funciona bajo GNU *General Public License*.

Puede ser obtenido desde *www.wireshark.org*. Este analizador de protocolos incluye el IEEE 802.11 por lo que puede ser utilizado como una herramienta de monitoreo de redes inalámbricas.

5.2.3.4 AIRODUMP

Este software se utiliza para capturar tráfico del protocolo 802.11, su uso se ha ligado a la captura de paquetes para ir acumulando vectores de inicialización con el fin de intentar utilizarlos con software que pueda intentar obtener la clave WEP de redes inalámbricas. Tiene la funcionalidad de mostrar coordenadas de los puntos de acceso que se vayan encontrando si se cuenta con un dispositivo GPS conectado al equipo.

Con el uso de *airodump* se podrá encontrar los puntos de acceso detectados en el área de cobertura en donde se encuentre, además permitirá encontrar los clientes conectados a estos puntos de acceso. Permite captura de información de los canales de comunicación y se puede especificar alguno es especial, así mismo detecta los métodos de cifrado que se están empleando en los puntos de acceso.

Este software está disponible para sistemas operativos Linux y Microsoft Windows, sin embargo un punto muy importante para el uso de *airodump* es el tipo de tarjeta de red inalámbrica que se emplea, no es compatible con todos los fabricantes de tarjetas de red inalámbrica y no todas las versiones de los controladores tienen soporte para este software. Por ejemplo para sistemas operativos con Microsoft Windows es necesario utilizar las librerías peek.dll y peek5.sys en el mismo directorio en donde se encuentre el ejecutable de *airodump*.

Cuando se vaya a utilizar *airodump* es necesario utilizar el script *airmon-ng* para listar las interfaces de red inalámbrica detectadas y así saber si es posible la ejecución del software, este script se puede descargar así como *airodump* desde el sitio *www.aircrack-ng.org*.

5.2.3.5 AIRCRACK

Es una herramienta muy poderosa para las redes inalámbricas, puede funcionar como un detector de redes, como un analizador de paquetes y además puede ser utilizado con fines de ruptura de llave WEP y WPA/WPA2-PSK. Este software puede recuperar las claves WEP cuando se cuenta con tráfico capturado de la red, como por ejemplo con el software de *airodump*, por medio de ataques de fuerza bruta y ataques estadísticos. Hace uso de un diccionario.

Aircrack puede trabajar con tarjetas de que puedan ser utilizadas como modo monitor, puede capturar tráfico de los protocolo 802.11a, 802.11b y 802.11g. Tiene la posibilidad de ser ejecutado en ambientes Linux y Microsoft Windows.

Utiliza técnicas estadísticas de ataques FMS, Ataques Korek y el de Fuerza Bruta como metodología para obtener las claves WEP. Este software puede ser adquirido desde el sitio oficial *www.aircrack-ng.org*.

5.2.3.6 AIRSNORT

AirSnort es una herramienta que puede obtener llaves de cifrado en las redes inalámbricas, operará de modo que monitorea de forma pasiva para capturar paquetes de información y cuando ha capturado la suficiente información puede realizar la obtención de las llaves de cifrado de datos. Al igual que *Aircrack*, este software hace uso del ataque FMS para obtener las claves WEP.

Este software puede ser utilizado en plataformas *Microsoft Windows, Unix, Linux*. Se requiere que la tarjeta de red sea capaz de funcionar en modo monitor para que pueda estar capturando los paquetes cifrados. Se distribuye bajo la licencia *GNU General Public License (GPL)* y se puede descargar desde el sitio *http://sourceforge.net/projects/airsnort*. Los requisitos para que funcione este software son los drivers que sean compatibles, instalar la librería libcap, y el software de *airsnort*.

5.2.3.7 KISMET

Kismet es un software descubridor de redes inalámbricas, además es un *sniffer* y un sistema detector de intrusos, pudiendo monitorear tráfico 802.11b, 802.11a y 802.11g. Puede ser instalado en equipos que cuenten con tarjeta que pueda funcionar en modo promiscuo. Identifica redes inalámbricas de manera pasiva capturando paquetes de información para detectar el protocolo en el cual están funcionando así como el identificador de estas redes, es capaz de ver las redes que aparecen ocultas.

Entre las funcionalidades que ofrece están:

- Compatibilidad con archivos de datos de *Ethereal/tcpdump*.
- Compatible con archivos de vectores de inicialización capturados con *Airsnort*.
- Detección de rangos de IP.
- Descubre las redes inalámbricas con el SSID oculto.
- Mapeo gráfico de las redes.
- Identificación de modelo y fabricante de los puntos de acceso y clientes.
- Detección de configuraciones de fábrica de los puntos de acceso.
- Decodificación de paquetes WEP en tiempo real de redes conocidas.
- Salidas de datos en archivos XML.
- Arriba de 20 tipos de tarjetas de red soportadas.

Kismet se distribuye bajo el esquema de *GNU General Public License* y se puede descargar del sitio oficial *www.kismetwireless.net*. Funciona bajo las plataformas de *Linux/ Unix /Microsoft Windows*.

5.2.3.8 NETSTUMBLER

Netstumbler es un descubridor de redes inalámbricas que funciona para los protocolos 802.11a, 802.11b y 802.11g. Está diseñado para funcionar en la plataforma de *Microsoft Windows*, aun sin soporte para *Windows Vista*. Entre las funcionalidades que ofrece están:

- Verifica la configuración de las redes detectadas.
- Estudiar la cobertura o nivel de señal que tenemos en diferentes puntos de una distancia.
- Detecta puntos de acceso no autorizados
- Tiene soporte para obtener las coordenadas de los puntos de acceso.
- Existe una versión *MiniStumbler* que se puede instalar en *Windows CE*.

Existe una lista de tarjetas de red que pueden correr la aplicación en el sitio oficial y en donde además se puede descargar una versión de prueba del software, ya que esta herramienta se distribuye en base a contribuciones de donativos, el sitio oficial es *http://stumbler.net/*.

TABLA 5.1 Software de monitoreo para redes inalámbricas

SOFTWARE	CATEGORÍA	PLATAFORMA	DISTRIBUCIÓN	ÚLTIMA VERSION	SITIO OFICIAL O DE DESCARGA
Wireshark	Analizador de paquetes	Microsoft Windows/Linux /Unix / Mac OS X/SUN/ FreeBSD, etc.	*GNU General Public License.*	1.0.3.	http://www.wireshark.org/download.html
Airopeek	Analizador de paquetes	Microsoft Windows	Comercial	1.1.1	http://www.wildpackets.com/products/legacy_products/airopeek
Airodump	Analizador de paquetes Descubridor de redes	Microsoft Windows/Linux	*GNU General Public License.*	1.0	http://www.aircrack-ng.org/doku.php#download
Aircrak	Descubridor de redes Analizador de paquetes WEP/WPA/WPA2 Cracking y herramientas de diccionario	Microsoft Windows/Linux	*GNU General Public License.*	1.0	http://www.aircrack-ng.org/doku.php#download
Airsnort	WEP/WPA/WPA2 Cracking y herramientas de diccionario	Microsoft Windows/Linux	*GNU General Public License.*	0.2.7c	http://sourceforge.net/projects/airsnort
WEPCrack	WEP Cracking	Linux /Unix	*GNU General Public License.*	0.1.0	http://sourceforge.net/projects/wepcrack/
Kismet	Descubridor de redes inalámbricas Analizador de paquetes	Microsoft Windows/Linux	*GNU General Public License.*	Kismet-2008-05-R1	http://www.kismetwireless.net/download.shtml
Netstumbler	Descubridor de redes inalámbricas	Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.	Donativos/ Uso	0.4.0	http://www.netstumbler.com/downloads/
Wifi Hopper	Descubridor de redes inalámbricas Analizador de paquetes	Microsoft Windows	Comercial	1.2	http://www.wifihopper.com/
Wellenreiter	Descubridor de redes inalámbricas	Linux /Unix	*GNU General Public License.*	1.9	http://wellenreiter.sourceforge.net/download.html

En el capítulo VII en los temas de Auditoría y Monitoreo se mostrará la forma de uso y configuraciones de algunas de estas herramientas como parte de las buenas prácticas que se deben de tomar en cuenta dentro de las redes inalámbricas.

CAPÍTULO

6

AUDITORÍA A REDES INALÁMBRICAS

En este capítulo se desarrolla el tema de auditoría a las redes inalámbricas como parte de la estrategia integral de gestión de esta tecnología de información, se explican algunos aspectos a tomar en cuenta para realizar auditorías a la configuración, al servicio, a la seguridad y al cumplimiento a las políticas.

6.1 AUDITORÍA A REDES INALÁMBRICAS

El manejo efectivo de la información y en general de los aspectos relacionados a las Tecnologías de Información se ha convertido en un aspecto de crítica importancia para el éxito de cualquier organización, esto debido al aumento de la dependencia de la información y de los sistemas asociados que operan con ella.

Una auditoría provee una historia de acciones que pueden ser usadas para determinar en qué puede estar mal, o cuando ira mal y cuáles son las causas de que vaya mal. Para determinar el nivel de seguridad en la red inalámbrica dentro de las organizaciones es imperativo auditarla para determinar que vulnerabilidades existen dentro del sistema, como podrían ser estas explotadas, y que se necesita hacer para protegerlas.

Un auditor debe de evaluar los procedimientos, las estrategias de acceso a la información por parte de los usuarios, la protección de los servicios, si el personal está capacitado, si los usuarios conocen las políticas de seguridad de la red, etcétera. En cuanto a los elementos que son visibles a terceros y teniendo en cuenta los tipos de datos y los recursos que podría conducir a ser comprometida, el auditor determinará los métodos que el atacante podría utilizar parta hacerse del control de los recursos de la red inalámbrica.

Los servidores, puntos de acceso, *routers*, equipos clientes entre otros elementos valiosos de una organización en manos equivocadas son una puerta abierta a la red inalámbrica y a los recursos críticos de información.

El auditor localiza y documenta las fallas en la configuración actual de seguridad, así como también recomienda la mejor manera de direccionar las soluciones para resolver estas fallas por orden de gravedad. Una vez que haya un plan se podrá comenzar de manera proactiva a proteger los intereses de la organización.

La institución debe continuamente realizar auditorías a la infraestructura para asegurar que las políticas que existan estén siendo aplicadas en todo momento, por el contrario si esto no se realiza, la organización deberá de asumir que las redes inalámbricas no son seguras.

Un plan de auditoría está compuesto por seis fases: Planeación, Campo de trabajo y Documentación, Numeración de los descubrimientos y Validación, Desarrollo de Solución, Informe de publicación y por último Seguimiento al Problema.

En la **Planeación de la Auditoría** se debe determinar que se planea auditar, se debe de considerar si los aspectos elegidos llevarán a obtener un reporte que situé la actualidad del funcionamiento de los sistemas. En esta fase de deben de determinar objetivos y parámetros que se deberán obtener para cumplir con la meta de la auditoría.

En la fase de **Campo de Trabajo y Documentación** es donde se lleva a cabo la mayor parte de la auditoría, ya que aquí se ejecutan los planes establecidos en la fase previa, los auditores recaban los datos de diversas fuentes y formas para identificar los riesgos y determinar cuáles no están siendo mitigados de manera apropiada. Esta información recabada directamente en las áreas de trabajo deberá documentarse de manera detallada para que posteriormente se puedan obtener conclusiones de la auditoría.

La siguiente fase de **Numeración de los descubrimientos y validación**. Los problemas potenciales descubiertos son listados y validados como situaciones de riesgo, es muy importante validar que estos problemas descubiertos sean lo suficientemente significativos para ser reportados.

Una vez listados y validados los problemas potenciales es tiempo de trabajar para desarrollar un plan de acción direccionado a la resolución de cada uno de los problemas listados, esta fase de **Desarrollo de Solución** se hacen recomendaciones por parte del grupo de auditores de cómo mitigar los riesgos encontrados durante la auditoría.

En la **Publicación del Informe** se plasman los resultados obtenidos durante la obtención de datos así como las soluciones desarrolladas, en este informe está documentada toda la auditoría, sirve como un registro de esta actividad, sus resultados y los planes de acción. Este reporte final debe de ser entregado al personal directivo de la organización.

Por último, el **Seguimiento del problema** representa una continuidad a que los problemas descubiertos sean solventados con las soluciones desarrollas y planteadas en el documento del informe de la auditoría. El proceso de auditar las redes inalámbricas deberá ser continuo, debido a que estas tecnologías representan una gran parte de la infraestructura de la red institucional. Una vez que se dispone de la información, se puede obtener un panorama del costo del daño que podría causar el ataque o la intrusión a la red inalámbrica.

6.1 DE LA CONFIGURACIÓN

Para una red inalámbrica segura, no es suficiente el configurar los puntos de acceso y la infraestructura de comunicación inalámbrica de manera correcta cuando se instalaron por primera vez, especialmente en organizaciones de gran tamaño con múltiples personas pertenecientes al área de administración de las Tecnologías de Información. Es muy común para un punto de acceso perder las configuraciones por alguna razón del hardware o por algún error humano, o en el peor de los casos si un intruso malicioso se

conecta a alguna interfaz del punto de acceso, podría habilitar o alterar la configuración de una manera que violara las políticas de seguridad de la organización.

Para combatir las omisiones de configuración en los puntos de acceso, se debe de proporcionar una detallada auditoría y registro del sistema para realizar un seguimiento a cada configuración cambiada por el usuario como tarea fundamental dentro de la estrategia de mitigación de riesgos en las Tecnologías de Información de las organizaciones. Mediante el rastreo de la fuente de todos los cambios de configuración y errores, la gestión de la seguridad de las redes inalámbricas garantiza asegurar la rendición de cuentas en caso de posibles incidentes de seguridad, así como a identificar que usuarios incurrieron en la falta, de esta manera se podrán tomar algunas medidas de prevención como capacitación del personal por ejemplo.

Además de proporcionar información de la infraestructura de las redes inalámbricas y la rendición de cuentas en caso de posibles incidentes, las organizaciones deben realizar auditorías frecuentes de la configuración de cada AP para garantizar que sus configuraciones reales siempre se ajusten a las políticas de seguridad. La actividad inicial de la auditoría de la configuración ha de ser la realización de un minucioso inventario de los dispositivos presentes en la infraestructura TI, estas auditorías pueden llevarse a cabo no sólo de manera manual, ya que puede haber cientos de configuraciones diferentes que deben de ser auditados en cada punto de acceso inalámbrico, se pueden utilizar herramientas de software que existen en la actualidad.

Sólo una red inalámbrica centralizada puede ser manejada de manera que se comparen las configuraciones de todos los puntos de acceso existentes con las políticas de configuración predefinidas, para automáticamente detectar discrepancias. Un manejo centralizado de la seguridad de la red inalámbrica usa un proceso altamente efectivo para detectar dispositivos y evaluar sus configuraciones actuales, lo que permite llevar auditorías básicas continuas.

La función más crítica de la auditoría de la configuración será la verificación de los datos de configuración actuales. La detección a tiempo de dispositivos erróneamente configurados reducirá significativamente las situaciones de inestabilidad de la infraestructura TI, lo que podría llegar a dar lugar a fallos catastróficos. Además, la auditoría de la configuración es una de las mejores maneras de eliminar las brechas de seguridad internas y externas.

Una auditoría de seguridad sobre los dispositivos las redes inalámbricas también provee un control de los registros de los cambios de configuración que los usuarios puedan realizar (quién hace qué y cuándo, y en qué dispositivo), estos informes deben ser capaces de ofrecer una visión automatizada de los cambios, y, en algunos casos, alertar de las desviaciones que dichos cambios experimenten respecto de las políticas esperadas.

Como resultado de la auditoría de la configuración de los dispositivos resulta un informe que ayudará a minimizar las alertas a causa de errores de configuración, también puede incluir un factor de escalado que estime el número de usuarios afectados. Esto puede ayudar a determinar el costo de un fallo.

6.2 DEL SERVICIO

La infraestructura de Tecnologías de Información de cualquier organización está diseñada e implementada bajo un objetivo de funcionamiento, es decir que tienen el objetivo de dar un servicio tecnológico al personal. Cuando se pierde este objetivo y se comienza a utilizar con fines diferentes o no apropiados se estará incurriendo en faltas a las políticas de seguridad. Es por ello que auditar el servicio es una cuestión de suma importancia para mantener la integridad, confidencialidad y disponibilidad de las redes inalámbricas.

El propósito bajo el cual fue concebida la red inalámbrica dictará la directriz para la realizar la auditoría, podrán existir redes que den sólo acceso a Internet o redes que estén diseñadas con esquemas de seguridad avanzados y por ello variarán las metodologías y procedimientos para auditarlas. Sin embargo se deberán poner a prueba los procedimientos bajo los cuales están funcionando.

Para auditar el servicio que puedan estar ofreciendo las redes inalámbricas de manera general se auditan parámetros como los son pruebas de congestión para auditar como se comportaría la red inalámbrica en caso de tener un sobre uso del ancho de banda, se audita el manejo de la información que se trasmite por este medio, si existen prioridades de acuerdo al tipo de tráfico de red, entre otros. Además de aspectos administración de las cuentas de acceso, si son para uso exclusivo del personal, si estas cuentas y contraseñas disponen de mecanismos de confidencialidad, etcétera.

Otro aspecto importante a auditar es la continuidad del servicio, esto involucra hacer pruebas control cuando por ejemplo se realizan cambios en la infraestructura de la red inalámbrica, caso de ello podría ser el cómo se ve afectada la red inalámbrica cuando de actualiza el *firmware* de algún dispositivo. La continuidad del servicio debe planearse y diseñarse para asegurar la disponibilidad de la información y del servicio en casos de incidentes, así mismo el procesamiento de la información se ha convertido en parte fundamental de las organizaciones por lo que la falta de disponibilidad en los servicios pone en peligro la viabilidad permanente del alcance de los objetivos establecidos para esos servicios.

6. 3 DE LA SEGURIDAD

La auditoría de seguridad se divide en dos, seguridad técnica y seguridad operacional, dependiendo de las metas y necesidades, se auditan más o menos aspectos.

Inicialmente uno de los aspectos para auditar es asegurarse que los puntos de acceso estén funcionando en su última versión de software, ya que si estos dispositivos están con una versión vieja de *firmware* existen algunos AP's que dejan abiertos huecos de seguridad a posibles ataques o no utilizan las configuraciones mas robustas en cuanto a seguridad. Para auditarlos es necesario verificar cada uno de ellos y obtener el dato de que versión se está utilizando, además de saber que el software de actualización haya sido descargado del distribuidor oficial del equipo.

El siguiente paso a auditar es que el software de administración del punto de acceso este siendo usado con las opciones de seguridad que tiene disponibles, se deberá auditar aspectos como las configuraciones que trae por default. Así como la forma de administración de los AP's sea desde una red cableada y estén deshabilitadas las demás formas de administración.

Cuando se hace una auditoría en la seguridad de la red inalámbrica no se debe de omitir la auditoría de los clientes, ya que si los clientes no tienen las medidas necesarias de seguridad, este sería el punto donde los atacantes podrían vulnerar, los dispositivos clientes deberán de tener los mecanismos de protección mínimos como Firewall y antivirus actualizado.

Otro aspecto muy importante a evaluar en la auditoría es el método de autenticación que utiliza la red inalámbrica, ya que si no se cuenta con algún método de autenticación la red inalámbrica está abierta a conexiones de usuarios que estén dentro del perímetro de cobertura de la red y que cuenten con una tarjeta de red inalámbrica, este problema viola la integridad de la red y pone en riesgo los sistemas de la organización. El método de autenticación implementado en la red inalámbrica deberá ser justificado por los responsables de la implementación, si la red inalámbrica no utiliza algún método de autenticación, esto deberá ser tomado como un punto crítico a considerar en el reporte final de la auditoría.

Una vez que el cliente se ha autenticado con el punto de acceso la información comienza a fluir por el medio inalámbrico, evaluar la seguridad del método de cifrado de la comunicación implementado también

es de gran importancia ya que la información puede ser interceptada por atacantes y más aun si la información se envía en texto claro, esto es grave problema. Se deberá auditar que método de cifrado se implemento, sí está correctamente utilizado, sí los clientes cumple con él, etcétera.

Las redes inalámbricas deben ser monitoreadas continuamente por los administradores, se deberá auditar si se utiliza algún software para realizar monitoreo de seguridad y si se revisan las bitácoras de los dispositivos con regularidad, ya que esta actividad reduce los riesgos de posibles ataques a la red. Para auditar estos parámetros se deberá tener una comunicación con el administrador de la red para saber sí estas actividades son realizadas con frecuencia, sí la información que se recaba en las bitácoras es la suficiente o es excesiva, y sí los hacen personal capacitado.

Auditar que no existen puntos de acceso no autorizados es una tarea de este proceso que puede arrojar más información de la que se cree, para verificar la existencia de este problema se utilizan diversas herramientas de monitoreo y *wardriving*, estas herramientas permitirán identificar si existen puntos de acceso que se estén conectando a la red sin la autorización debida.

Una de las tareas del auditor es evaluar cómo se respondería en caso de alguna interrupción al servicio de la red inalámbrica, si se tiene un plan de recuperación para minimizar el tiempo de restauración del acceso inalámbrico. Se debe de tener algún proceso que facilite la restauración del servicio, un punto de acceso listo con las mismas configuraciones por ejemplo, en una organización donde se requiera tener el servicio de red inalámbrica en todo momento, es muy importante contar con planes contra desastres.

6.4 DEL CUMPLIMIENTO A POLÍTICAS

Las políticas ayudan a asegurar que los usuarios cumplan con estándares y procedimientos que permitan la mejor utilización de los recursos de Tecnologías de Información de las organizaciones, y sus posibles consecuencias en caso de violarlas, es por ello de vital importancia auditar su cumplimento.

La auditoría de cumplimiento a políticas determina la distancia entre la situación actual y la deseada frente a la normatividad vigente o la estructura documental y procedimental de una organización. Para auditar este aspecto se debe de establecer un marco de referencia deseado que será conforme a las políticas establecidas y se realiza un análisis para identificar los porcentajes de cumplimiento de las políticas. De esta manera se conocerá el estado actual de la situación y así emitir recomendaciones en caso de ser necesarias.

Determinar el nivel de cumplimiento de la Política de Seguridad y de determinados procedimientos será una tarea que el auditor deberá ir realizando conforme elabora las demás actividades de auditoría debido a que las políticas deberán estar establecidas para cubrir aspectos como instalación y configuración de dispositivos, de estándares de cifrado de datos, etcétera; por lo que el cumplimiento de estas políticas se irá evaluando durante toda la auditoría.

En las organizaciones debe de existir una normatividad que regule las comunicaciones inalámbricas, en caso de no ser así, este punto es un gran problema a resolver y que deberá ser documentado en el reporte de la auditoría, se deberá emitir la recomendación de que exista la reglamentación de uso de las redes inalámbricas para poder considerar un mayor grado de seguridad en la red. Así mismo en el caso de que exista la reglamentación se deberá de evaluar que el alcance de la normatividad esté acorde a la institución.

Cuando se audite las políticas de las redes inalámbricas deberán cubrir algunos aspectos como lo son:

- Que todas las transmisiones inalámbricas deben de ser cifradas para prevenir la perdida de confidencialidad en los datos.
- Que los puntos de acceso estén actualizados en su *firmware*.

- Que sólo los usuarios autorizados tengan el acceso a la administración de los puntos de acceso.
- Que sólo el personal autorizado pueda instalar puntos de acceso.
- Que las contraseñas de administración de los puntos de acceso cumplan con la política de la institución.
- Que los parámetros de SSID y nombre del punto de acceso hayan sido cambiados por los personalizados.
- Que el SSID de la red este deshabilitado para el *broadcast*.
- Que la potencia de trasmisión de la señal del punto de acceso se reduzca lo más que se pueda a sólo tener cobertura en el área del servicio.
- Que los equipos clientes tengan las medidas básicas de seguridad como Firewall y antivirus.
- Que de preferencia se utilicen métodos tunelizados como *IPSec* o *VPNs*.
- Que se tenga el personal adecuado para realizar la actividad de monitoreo en busca de puntos de acceso no autorizados.

Estos puntos básicos a evaluar deberán ser cubiertos por las políticas institucionales, de no ser así se deberá de emitir la recomendación en el reporte de la auditoría que se deberán tomar en cuenta para la actualización de esas políticas.

La aplicación de esta reglamentación en los usuarios es clave en la seguridad de la red inalámbrica, si no se cumplen se estarán corriendo riesgos y dejando abierta la posibilidad de sufrir posibles ataques a la infraestructura de la red.

TABLA 6.1 Auditoría de redes inalámbricas

AUDITORÍA EN LAS REDES INALÁMBRICAS	
De la Configuración	Del Servicio
• Revisión de bitácoras de cambios en la configuración. • Revisión de bitácora de acceso a los dispositivos. • Revisión de las configuraciones actuales de los dispositivos no sean las de fábrica. • Revisar que la señal de la antena sea reducida para cubrir sólo el área de trabajo. • Revisar que las configuraciones las hagan personal capacitado para esta tarea. • Revisar que la ubicación de los APs sea sólo accesible por los administradores.	• Revisar el funcionamiento con pruebas de congestión de tráfico. • Revisar la continuidad del servicio de la red inalámbrica. • Revisar si la cobertura de la señal llega a áreas en donde se requiere. • Revisar las prioridades del tráfico de la red inalámbrica. • Revisión de retardo y pérdida de paquetes de información. • Revisión de comportamiento de la red en caso de una actualización de *firmware* de los APs. • Revisión de configuraciones de calidad en el servicio si se tiene habilitado. • Revisar el procedimiento de recuperación a fallos.
De la Seguridad	Del Cumplimiento a las Políticas
• Revisar que la versión del *firmware* del AP sea la última. • Revisar que la administración de los AP se haga desde una red cableada. • Revisar que las formas de administración de los AP se que no se utilicen, sean deshabilitadas. • Revisar que los clientes cuenten con antivirus y Firewall. • Revisar que las comunicaciones utilicen un método de autenticación y cifrado. • Revisar que la actividad de monitoreo se realice de manera periódica.	• Revisar que el personal de administración y usuarios implemente las políticas existentes. • Revisar que todos los involucrados en la red inalámbrica conozcan las políticas. • Revisar que todos los involucrados conozcan donde se encuentran publicadas.

CAPÍTULO 7

CONFIGURACIONES ADECUADAS Y BUENAS PRÁCTICAS

En este último capítulo se presentan algunas recomendaciones y buenas prácticas que permiten ayudar al mejor funcionamiento de las redes inalámbricas dentro de la Facultad de Ingeniería, se muestra el uso de ciertas herramientas obtienen información relevante para la gestión de redes inalámbricas.

7. 1 GUIAS Y RECOMENDACIONES

El siguiente cuadro presenta guías y recomendaciones para implementar y mantener una red inalámbrica 802.11 segura. Para cada una de ellas se colocaron dos columnas, la primera de ellas "Mejor Práctica" si está seleccionada significa que esto es recomendado para todo tipo de redes inalámbricas en las organizaciones. La segunda columna "Se debería considerar" si está seleccionada significa que esta medida debería ser tomada muy en cuenta por las organizaciones por tres razones; la primera porque implementar esta recomendación puede proveer de un ambiente de red inalámbrica más seguro ofreciendo medidas de protección. La segunda, porque representa una medida de estrategia de seguridad avanzada. Y la tercera, porque implementarla significaría un impacto en el rendimiento, operación y costo, por lo que esta columna debe ser considerada en una relación de costo/beneficio.

TABLA 7.1 Guías y recomendaciones para las redes inalámbricas

	Recomendación de Seguridad	Lista de Verificación	
		Mejor práctica	Se debe considerar
	Recomendaciones de Administración		
1.	Desarrollar una política de seguridad relacionada con el uso de las redes inalámbricas 802.11.	✓	
2.	Asegurarse que los usuarios de la red están completamente capacitados en la seguridad en cómputo, que tengan conciencia de los riesgos	✓	

	asociados con las tecnologías inalámbricas.		
3.	Realizar una evaluación de riesgos para entender el valor de los activos críticos en la organización y las necesidades de protección.	✓	
4.	Asegurarse que los puntos de acceso y las tarjetas de red de los clientes (NIC's) tengan la capacidad de actualizar su *firmware* y parches de seguridad que hayan sido liberados.	✓	
5.	Realizar evaluaciones de seguridad global de forma periódica y en tiempos no planeados (incluyendo validación de puntos de acceso no autorizados) para entender de mejor manera la postura de seguridad en donde se encuentra.	✓	
6.	Asegurarse que los límites externos de protección en el perímetro de las instalaciones de la organización.	✓	
7.	Desarrollar controles de acceso en las áreas restringidas de la organización (Credenciales, Huellas Dactilares, etcétera).	✓	
8.	Completar una evaluación para medir y establecer la cobertura del AP para la organización.	✓	
9.	Hacer un inventario lógico de todos los puntos de acceso y dispositivos inalámbricos 802.11.	✓	
10.	Asegurarse que las redes inalámbricas no son utilizadas hasta que se cumplen las políticas de seguridad de la organización.	✓	
11.	Localizar los puntos de acceso dentro de la organización lo más ajeados de los límites exteriores, paredes y ventanas como sea posible.	✓	
12.	Localizar los puntos de acceso en áreas seguras para prevenir accesos físicos no autorizados y manipulación por parte de los usuarios.	✓	
	Recomendaciones Técnicas		
13.	Probar empíricamente los límites del rango de cobertura de los puntos de acceso para conocer con exactitud el alcance de la señal.	✓	
14.	Asegurarse que los puntos de acceso sean apagados cuando no estén siendo utilizados (fines de semana, días festivos, etcétera).	✓	
15.	Asegurarse que la función de *Reset* de los puntos de acceso sea utilizada sólo cuando se requiere y que esta operación sea sólo realizada por un grupo autorizado de personas.	✓	
16.	Restaurar en los puntos de acceso las últimas configuraciones de seguridad cuando sea utilizada la función de *Reset*.	✓	
17.	Cambiar el SSID que traen los puntos de acceso de fábrica.	✓	
18.	Deshabilitar la función de *broadcast* del SSID para que sólo los clientes que conozcan el SSID se puedan asociar.		✓
19.	Validar que el SSID no refleje el nombre o la actividad destinada para la red inalámbrica.	✓	
20.	Asegurarse que los canales en los puntos de acceso estén al menos 5 canales de diferencia de otra red inalámbrica que haya en el área para prevenir interferencias.	✓	
21.	Entender y asegurase que los parámetros por *default* de los puntos de acceso hayan sido cambiados.	✓	
22.	Deshabilitar todos los protocolos inseguros y aquellos que no se vayan a ocupar en los puntos de acceso.	✓	
23.	Habilitar todas las configuraciones de seguridad de los dispositivos inalámbricos, incluyendo la autenticación criptográfica.	✓	
24.	Asegurarse que el tamaño de la llave de cifrado sea de al menos 128-bits o tan grande como sea posible.	✓	
25.	Asegurarse que las llaves compartidas sean cambiadas de manera periódica y guardando un historial de claves para evitar la repetición.	✓	
26.	Instalar y configurar de manera adecuada un Firewall entre la red cableada y la red inalámbrica.	✓	
27.	Instalar software antivirus en los clientes de la red inalámbrica.	✓	
28.	Instalar software de Firewall personal en cada cliente de la red	✓	

	inalámbrica.		
29.	Deshabilitar las capetas compartidas en los clientes de la red inalámbrica (especialmente en ambientes muy concurridos).	✓	
30.	Desarrollar un control de acceso por dirección física en los puntos de acceso.		✓
31.	Considerar la instalación de *switches* de capa 2 en lugar de *Hubs* para la conectividad de los puntos de acceso.	✓	
32.	Implementar *IPsec* o *Virtual Personal Networks* en las redes inalámbricas.		✓
33.	Asegurarse que el método de cifrado sea el adecuado para el tipo de información que viaja por la red inalámbrica así como para la velocidad de procesamiento de los equipos clientes.	✓	
34.	Hacer pruebas de comportamiento cuando se instalen parches de seguridad o actualizaciones de los equipos.	✓	
35.	Asegurarse que todos los puntos de acceso tengan contraseñas de administración robustas.	✓	
36.	Asegurarse que todas las contraseñas sean cambiadas de manera regular.	✓	
37.	Desarrollar autenticación de usuarios cómo Infraestructura de Llave Publica PKI (*Public Key Infraestructure*).		✓
38.	Asegurarse que la topología Ad-Hoc de 802.11 esté deshabilitada a menos que sea muy necesario utilizarla.	✓	
39.	Usar IP estáticas en el segmento de la red inalámbrica.		✓
40.	Deshabilitar el DHCP (si el servicio lo permite).		✓
41.	Activar mecanismos de autenticación la administración de las interfaces de los puntos de acceso.	✓	
42.	Usar SNMPv3 y/ó SSL/TTL para Web seguro para la administración de los puntos de acceso.	✓	
	Recomendaciones Opcionales		
43.	Configurar los parámetros de SNMP en los puntos de acceso con los menores privilegios (sólo lectura).	✓	
44.	Usar el puerto serial del punto de acceso para administrarlo, de esta manera se reduce el riesgo de exponer la información a la red.		✓
45.	Considerar otras formas de autenticación para la red inalámbrica cómo un servidor *Radius* o *Kerberos*.		✓
46.	Implementar agentes de detección de intrusos en la parte de la red inalámbrica para descubrir conductas sospechosas, accesos y actividad no autorizada.		✓
47.	Implementar tecnologías de auditoría para analizar las bitácoras del servidor *Radius* para detectar accesos no autorizados.		✓
48.	Habilitar la utilización de protocolos que permiten una comunicación inalámbrica más segura cómo 802.1X		✓
49.	Cuando ya no se utilicen más algunos puntos de acceso borrar las configuraciones para prevenir perdida de llaves, contraseñas, etcétera.	✓	
50.	Si los puntos de acceso permiten la creación de bitácoras, habilitarlas y revisarlas de manera regular.	✓	

7.2 AUDITORÍAS

Como ya se mencionó con anterioridad, las redes inalámbricas al igual que las redes cableadas están expuestas a riesgos como intrusiones a la red, códigos maliciosos y virus, accesos no autorizados, pérdidas de datos, pérdida de integridad y disponibilidad de la información, y demás problemas inherentes al medio de trasmisión por lo que prácticas como las auditorías deben ser actividades que se realicen de manera frecuente cuando se cuenta con este tipo de tecnologías implementadas.

Las prácticas de auditoría deben de perseguir dos objetivos esenciales, el primero de ellos es asegurar que sólo los usuarios autorizados pueden tener conexión a la red. El segundo objetivo es asegurar que ningún

usuario no permitido pueda tener acceso a la información que viaja por la red, si los datos que viajan por la red están cifrados, estos serán difíciles de ver por los intrusos.

En busca de que la red inalámbrica sea segura, el auditor debe de explorar otras posibilidades. El estudio de la topología y área de cobertura de la red inalámbrica, la revisión de la configuración de los equipos participantes en la red y la comprobación de que su software se encuentre actualizado, son temas a considerarse durante la auditoría de redes inalámbricas.

Existen herramientas que facilitan esta actividad de manera considerable, ejemplo de ello son los *Live CDs* que son distribuciones de *Linux* que ya traen muchas utilidades que se pueden emplear para diagnosticar el estado de la red inalámbrica. Entre los *Live CDs* más populares están y que se pueden obtener de manera gratuita están *BackTrack 3, OSWA, WIFISLAX, WIFIWAY*, entre algunas otras herramientas existentes en el mercado que se distribuyen de manera comercial.

En la actividad de la auditoría de redes inalámbricas se debe de utilizar software que permita una mejor visión de la situación actual de funcionamiento de la red, por ejemplo se deben de utilizar:

- Monitores de radiofrecuencia.
- Analizadores de paquetes.
- Software de mapeo de puntos de acceso.
- Kits de software para explotar las vulnerabilidades conocidas.

EJEMPLO DE CONFIGURACIÓN DE UN EQUIPO PARA REALIZAR UNA AUDITORÍA.

Las aplicaciones que se utilizarán requieren que la tarjeta de red inalámbrica pueda tener la funcionalidad de modo monitor. Entonces primero que nada debemos configurarla en modo monitor, de esta manera se puede detectar todo el tráfico que circula por su alrededor. Para esta práctica utilizaremos una tarjeta de red inalámbrica PCMCIA con chipset *Atheros* que permite esta funcionalidad. Para determinar el estado de las tarjetas de red inalámbricas en nuestro sistema se utiliza el comando: *iwconfig ath0*

```
ath0      IEEE 802.11g  ESSID:""  Nickname:""
          Mode:Managed  Channel:0  Access Point: Not-Associated
          Bit Rate:0 kb/s   Tx-Power:18 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-92 dBm  Noise level=-92 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Una vez identificado el modo de funcionamiento de la tarjeta de red inalámbrica es necesario ponerla en modo monitor con el comando: *iwconfig ath0 mode monitor*. Después de poner la tarjeta en modo monitor podemos observar si los cambios se realizaron con éxito: *iwconfig ath0*

```
ath0      IEEE 802.11g  ESSID:""  Nickname:""
          Mode:Monitor  Frequency:2.432 GHz  Access Point: 00:1D:6A:3E:90:16
          Bit Rate:0 kb/s   Tx-Power:18 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality=0/94  Signal level=-93 dBm  Noise level=-93 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

Iniciaremos a auditar redes inalámbricas con *Kismet* para obtener los parámetros de auditoría:

- Detección de los puntos de acceso.
- Detección de los clientes.

- SSID, canal de comunicación, cifrado, fabricante y configuración de los puntos de acceso vecinos.
- Coordenadas de localización de los puntos de acceso si se cuenta con un GPS.

KISMET

Para instalar *kismet* y la herramienta que servirá para comunicarlo con el gps se hace mediante el comando:

apt-get install kismet gpsd

Una vez instalado *kismet* hay que configurar algunos parámetros en el archivo */etc/kismet/kismet.conf* como son la línea de *source* que es en donde se coloca la fuente de datos de *kismet,* en este caso *source=madwifi_ag,ath0,madwifi* además de la línea de *gps=YES* en ese mismo archivo.

Cuando se ha conectado el GPS en el puerto serial y ya ha adquirido señal es necesario iniciar el demonio antes que *kismet* mediante el comando *gpsd –p /dev/ttyS0;* una vez iniciado el *gpsd* es tiempo de ejecutar *kismet* mediante el comando: *kismet***.**

FIGURA 7.1 Interfaz gráfica de *Kismet*

Esta pantalla está dividida en las siguientes secciones

1. Información (*Info*)

La sección de información es una lista resumida de todo lo que ha recolectado *kismet:* número de redes detectadas, número de paquetes de red, cuántos de estos paquetes han sido cifrados, cuántos de ellos son débiles o fáciles de descifrar para ser vulnerados, número de paquetes que presentan ruido, paquetes inservibles y tasa de captura de paquetes por segundo. Además muestra el tipo de *driver* que está utilizando así como el canal en el cual está capturando la información.

2. Estado (*Status*)

La sección de Estado lista los eventos recientes (en este caso como nuevas redes detectadas), puede mostrar advertencias de equipos clientes que se encuentran monitoreando las redes inalámbricas sin estar asociado a alguna de ellas. Esta información es muy importante para cuando se está utilizando como detector de intrusos. Muestra el estado de la pila del equipo en el cual se está utilizando.

3. Redes (*Networks List*)

La primer columna es donde se identifica el SSID de las redes detectadas, en esta columna se puede identificar las redes Ad-Hoc así como los dispositivos que están conectados a ella. La columna T se refiere al tipo de dispositivo (Access Point (A), grupo de dispositivos inalámbricos (G), red Ad-Hoc (H), etcétera). La siguiente columna W representa el tipo de cifrado, si la columna indica *Y* entonces significa que la red implementa el protocolo WEP, cuando indica O es que implementa algún otro método diferente a WEP y cuando indica N es cuando no implementa método de cifrado.

También se encuentra la columna de canal de comunicación en el cual está funcionando la red. La columna de *Packts* indica cuántos paquetes han sido capturados. La columna de *Flags* puede indicar parámetros críticos como la bandera F que significa que la red está funcionando con los parámetros de fábrica. La comuna IP *Range* mostrará el rango de *IPs* utilizadas si pudo obtenerse el dato.

Esta sección también puede ser ordenada según parámetros como: SSID, canal, conteo de paquetes, nivel de la intensidad de la señal, por cifrado, entre otros. Una vez que se ha seleccionado una red de este listado es posible ver los clientes conectados a esta red y de estos se puede también obtener información como fabricante, dirección MAC, dirección IP, etcétera.

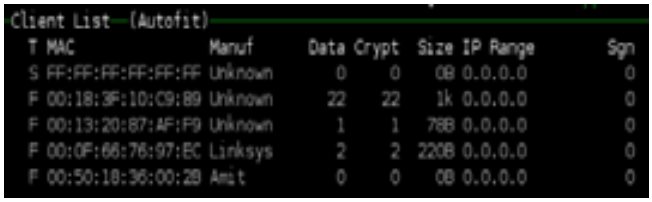


FIGURA 7.2 Listado de clientes detectados por *Kismet*

AIRODUMP

Esta herramienta puede servir dentro de la auditoría de redes inalámbricas para determinar que tan bien implementadas están las claves WEP cuando se utiliza este protocolo, esta herramienta captura paquetes de información y puede ir acumulándolos para después intentar obtener las claves. También si se cuenta con GPS puede mostrar las coordenadas de los puntos de acceso detectados. *Airodump* también requiere de tener la tarjeta de red que funcione en modo monitor.

Para ejecutarlo se tiene la siguiente sintaxis: **airodump [interface] [archivo de salida] [no. canal] [Banderas IVs].** Un ejemplo de ejecución de este software es: *airodump ath0 11* y la pantalla de salida es la siguiente.

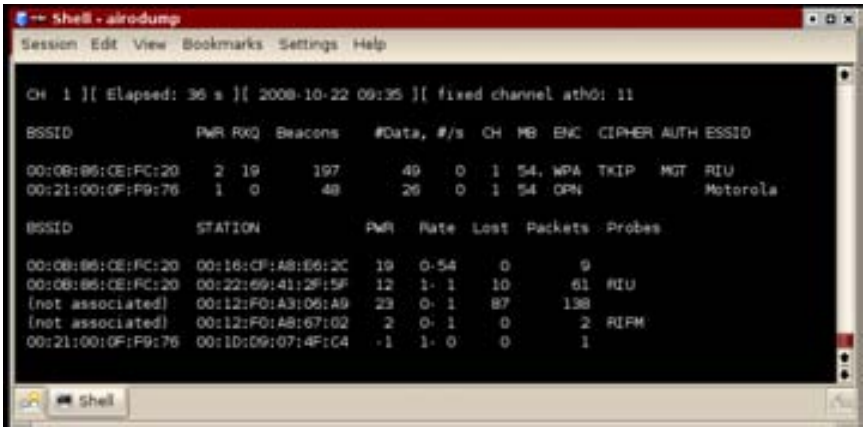


FIGURA 7.3 Datos capturados por *airdump*

En esta pantalla podemos obtener los siguientes datos útiles para la auditoría: la dirección física MAC, el SSID de red inalámbrica, número de paquetes capturados, en qué canal están funcionado, el tipo de

cifrado implementado, los clientes detectados. Una vez terminada la captura el archivo que se generó puede ser utilizado para intentar obtener las claves WEP con *airocrack*.

AIROSNORT

Esta aplicación nos permitirá obtener mayor información para la auditoría, datos como la dirección física del punto de acceso, el canal de comunicación, el SSID de las redes inalámbricas encontradas, además detecta si utiliza el protocolo WEP esta parte es muy importante ya que esta herramienta hace un ataque directo a los paquetes capturados con protocolo de cifrado WEP, por lo que si se deja capturando información el tiempo suficiente *Airsnort* puede obtener las claves WEP de las redes inalámbricas detectadas. Esta herramienta también necesita del funcionamiento en modo monitor de la tarjeta de red inalámbrica, por lo que para empezar a utilizarlo es necesario poner la tarjeta en modo monitor:

iwconfig ath0 mode monitor
iwconfig ath0 channel 6
airsnort

Una vez iniciado se muestra la siguiente interfaz de usuario en donde el menú de *File* permite cargar y guardar archivos de captura de datos para romper llaves de red en múltiples sesiones. Otra característica importante incluye que se puede seleccionar directamente en la interfaz gráfica, con qué tarjeta de red inalámbrica (*Network device*) podemos trabajar, así como el tipo de *driver* que se utilizará (*Driver type*). La opción de *scan* permite descubrir las redes inalámbricas que se encuentren a su alrededor. Por último podemos escoger mediante la opción de *channel* en qué canal de comunicación queremos capturar información.

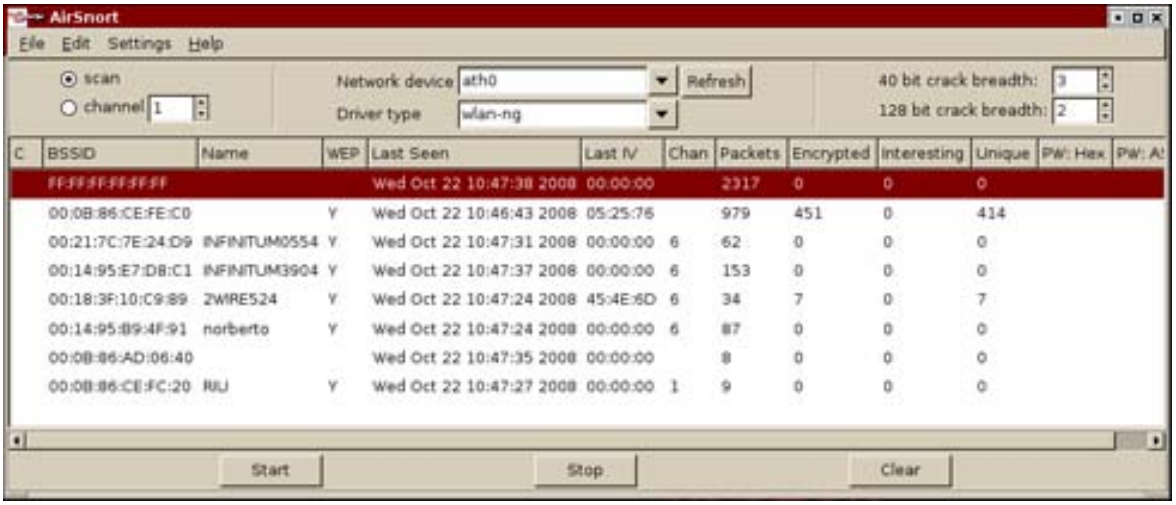


FIGURA 7.4 Interfaz gráfica de *AirSnort*

Trabajando en el modo original que trabaja *Airsnort* requiere de aproximadamente de 5 a 10 millones de paquetes cifrados capturados, una vez que han sido obtenidos puede determinar la llave WEP hasta en un minuto. Esto nos servirá para determinar que tan robustas están implementadas las claves WEP y completar la información de la auditoría a las redes inalámbricas.

7.3 MONITOREO

El monitoreo de la red inalámbrica permitirá la identificación de problemas relacionados con el protocolo 802.11, existen diferentes visualizadores de tráfico de red los cuales serán una herramienta para obtener estadísticas de tráfico, permitirán la depuración de problemas en la red, capturas de información para

análisis de protocolos y también como detector de intrusos. Se utilizará *Wireshark* para mostrar el funcionamiento de un monitor de tráfico de red que se puede utilizar para las redes inalámbricas.

EJEMPLO DE MONITOREO DE REDES INALÁMBRICAS CON WIRESHARK

Como se mencionó en el capítulo V, esta herramienta se puede descargar libremente y hacer uso de ella. Para instalarlo se puede mediante el comando:

apt-get install wireshark

Una vez instalado se puede ejecutar *wireshark* con el comando: *wireshark* y obtendremos la interfaz de inicio de esta aplicación. Para empezar a capturar paquetes nos dirigimos a *Capture/Interfaces*. Aparecerá entonces una lista de las interfaces de red. Pulsando el botón *"Start"* de una de las interfaces, empezaremos a capturar paquetes con esa tarjeta de red. Para detener la captura haremos clic sobre *Capture/Stop*. En la ventana principal de la aplicación aparecerán entonces los paquetes capturados. *Wireshark* muestra la información capturada en tres secciones principales.

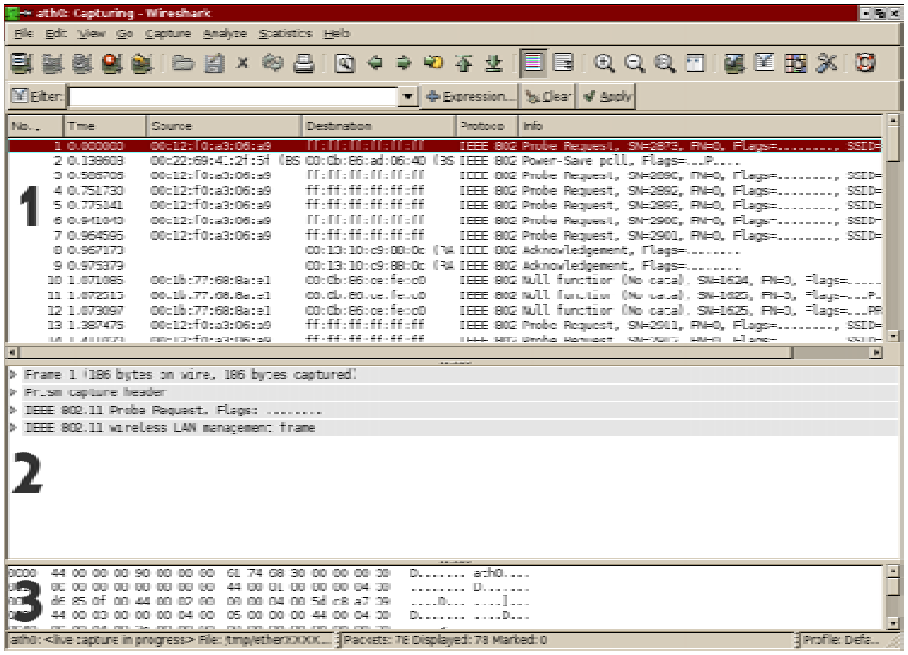


FIGURA 7.5 Interfaz gráfica de *Wireshark*

En la primera sección aparece un listado de los paquetes capturados con su información más relevante. En la segunda sección podemos observar los detalles del protocolo seleccionado en la sección 1. En la última sección se muestran los paquetes en bruto, es decir, tal y como fueron capturados por la tarjeta de red.

Filtrando paquetes: Como la información obtenida puede ser muy grande, podemos filtrar los paquetes para mostrar sólo aquellos que cumplen los requisitos indicados. Para filtrar paquetes debemos dirigirnos a *Capture/Options* y escribir el filtro que queramos en "*Capture Filter*".

Filtros de *display:* Otro tipo de filtros que podemos utilizar son los filtros de *display*, que son mucho más completos y flexibles ya que estos filtros funcionan sobre la información capturada y podemos hacer un análisis más minucioso de estos datos sin perder información que pueda llegar a ser relevante y que no estemos capturando. Una vez escrito el filtro, tan sólo hay que pulsar sobre el botón "*Apply*". Para eliminar el filtro hay que pulsar sobre el botón "*Clear*".

Wireshark cuenta con un asistente para crear filtros de *display*. Si hacemos clic sobre el botón "*Filter*", aparecerá la siguiente ventana en la que aparecen algunos filtros ya predefinidos. Si queremos capturar, por ejemplo, todo el tráfico HTTP, tendríamos que seleccionar HTTP en la lista de filtros. Para utilizar filtros de *display* también podemos hacer clic sobre el botón "*Expression*".

FIGURA 7.6 Filtros en *Wireshark*

7.4 ATENCIÓN A INCIDENTES

Se define un evento como toda ocurrencia observable en un entorno informático, por otra parte, un evento adverso es un evento con consecuencias negativas. A partir de estas declaraciones podemos definir un incidente de seguridad como un evento adverso en un entorno informático, que puede comprometer la confidencialidad, integridad o disponibilidad de la información. Así como una violación o inminente amenaza de violación de una política de seguridad de la información, política de uso aceptable o mejores prácticas de seguridad.

Determinar la preparación que se tiene en cuanto incidentes de seguridad en redes inalámbricas dentro de la Facultad de Ingeniería es una parte fundamental de la estrategia de gestión de redes inalámbricas. La mayoría de las organizaciones aprenden a responder a los incidentes de seguridad sólo cuando ya han sufrido de las consecuencias de ataques de diversas índoles a sus sistemas de información.

El concepto de equipo de respuesta a incidentes seguridad en cómputo se ha convertido en una práctica aceptada e implementada en muchas organizaciones. Las respuestas a incidentes exitosas son normalmente multidisciplinarias, en donde se involucra a participantes con diversidad de habilidades, en este equipo normalmente se debería incluir personal de recursos humanos, administradores, personal legal, auditores, personal de seguridad en cómputo, administrador de riesgos, etcétera.

Existe una metodología utilizada para el manejo de atención de incidentes, está compuesta por las fases de: preparación, identificación, erradicación, recuperación y de aprendizaje. Estas fases proveen de un plan de acción para manejar y mitigar el incidente en el periodo de tiempo más corto posible, este plan de acción es independiente al tamaño del equipo de respuesta a incidentes.

FASE DE PREPARACIÓN

Esta fase permite verificar y asegurar que las herramientas así como el personal adecuado estén en el lugar donde haya ocurrido un incidente de seguridad. Algunas actividades que se desarrollan durante esta fase son:

- Seleccionar los miembros del equipo de respuesta a incidentes y organizar al equipo.
- Desarrollar soporte de manejo del incidente y preparar al personal del equipo de respuesta.
- Desarrollar un plan de comunicación de emergencias.
- Proveer de facilidades de reportes de incidentes.
- Establecer guías para la cooperación entre departamentos y áreas.
- Prestar especial atención a las relaciones con los administradores de sistemas.
- Tener un conocimiento del correcto funcionamiento de los sistemas.
- Definir e implementar esquemas de resguardos.

FASE DE IDENTIFICACIÓN

Esta fase es importante porque es donde se decide si existe o no un incidente de cómputo, que el evento observado es lo suficientemente crítico para clasificarlo como un incidente. Entendiendo la diferencia entre un evento y un incidente se permitirá manejar al incidente de manera que se concentre la energía en la dirección correcta.

FASE DE CONTENCIÓN

Como el nombre lo indica, en esta fase se limita el daño del incidente de seguridad en el ambiente de cómputo. El equipo de respuesta a incidentes tiene un trabajo duro en esta fase, ya que se requiere que realicen una variedad de tareas como actualizar los sistemas, cambio de contraseñas, cambio de las reglas de los Firewalls, administración de las cuentas, detener los servicios y hacer escaneos con los sistemas antivirus.

Otra tarea clave en esta fase es reunir y preservar la evidencia del incidente de seguridad que puede ser admisible en procedimientos legales. Para hacer esto se debería de hacer una imagen completa del sistema o parte del sistema, capturar datos volátiles como procesos corriendo, RAM, conexiones de red entre otros. Independientemente del método que se utilice para preservar la evidencia, asegurar que se están utilizando archivos binarios limpios y que se está documentando todo lo que se está realizando.

FASE DE ERRADICACIÓN

Esta fase involucra la remoción de cualquier actividad maliciosa o de artefactos dejados por los intrusos. Típicamente la erradicación participa en la remoción de infección de virus, software *backdoor*, datos dejados por los intrusos y la desinstalación de herramientas de ataque. En algunos casos se debe de estar dispuesto a anular el ataque sin tener que reconstruir el sistema. En el caso que el sistema haya sido comprometido por un *rootkit*, la única manera de recuperar es reconstruir por completo los sistemas.

Otras actividades de esta fase son: incrementar las defensas, conducir un análisis de vulnerabilidades, encontrar el último respaldo limpio del sistema. Estas actividades son importantes ya que corregirán la manera que utilizó el atacante para entrar al sistema y disminuir al máximo la posibilidad que suceda de nuevo en un futuro. Usando la información obtenida del análisis de vulnerabilidades, el equipo de respuesta a incidentes podrá desarrollar una relación de trabajo con los administradores de los sistemas para verificar las últimas actualizaciones de los dispositivos estén vigentes.

FASE DE RECUPERACIÓN

El principal objetivo de esta fase es regresar los sistemas al modo de operación normal. Examinar de manera exhaustiva que el sistema funcione como antes es una tarea que los operadores deben de efectuar, así como verificar que la fuente del incidente haya sido controlada. Debido a la desconfianza que existirá

de que vuelvan a ocurrir incidentes de cómputo en esos sistemas, será necesario implementar algunas medidas de monitoreo para asegurar que no se presenten incidentes de cómputo nuevamente.

FASE DE APRENDIZAJE

Una de las partes más importante de la atención a incidentes y más frecuentemente omitida es la del aprendizaje y las mejoras al funcionamiento de los sistemas. Mediante la creación de bases de conocimiento se permitirán las mejoras a los sistemas dando lugar a una disminución a los posibles incidentes que pudieran llegar a aprovecharse de las mismas vulnerabilidades. Es muy importante ir documentando el estado actual de los sistemas, así como un resumen del incidente como se detectó, que acciones se tomaron, etcétera.

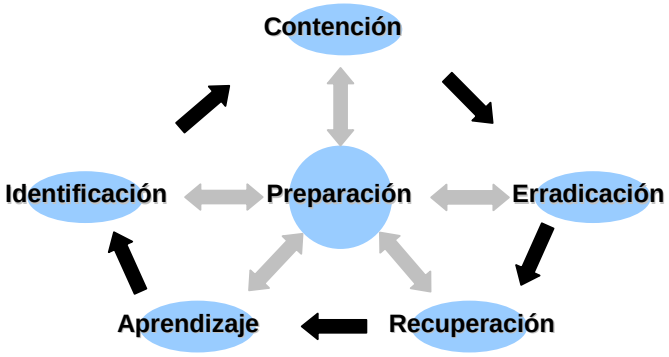


FIGURA 7.7 Atención a incidentes

Es necesario empezar a tomar medidas de gestión de riesgos de seguridad en las redes inalámbricas dentro de la institución:

- Medidas preventivas: que involucran contraseñas de administración de puntos de acceso, claves de acceso seguras (WEP, WPA-PSK, WPA2-PSK, etcétera), definición de políticas de seguridad, Firewalls en los perímetros, procedimientos de respaldos de información, implementación de métodos de cifrado, configuraciones adecuadas, entre otras.
- Medidas de detección: registros de auditoría en puntos de acceso, dispositivos clientes y servidores de control de acceso (*RADIUS, KERBEROS*), además sistemas detectores de intrusos, revisiones de seguridad a la infraestructura de red, monitoreo de las redes inalámbricas, etcétera.
- Medidas correctivas: esquema de tolerancia a fallos, procedimientos de *restore* para los puntos de acceso, planes de recuperación de desastres, procedimientos de restablecimiento de los servicios inalámbricos, entre otras.

La gestión de los incidentes de cómputo tiene grandes beneficios como:

- La respuesta a incidentes de seguridad de forma sistemática.
- Facilitar una recuperación rápida y eficiente minimizando la pérdida de información e interrupciones de servicios.
- Prevenir la ocurrencia reiterada de incidentes mediante el aprendizaje.
- Apoya en el mejoramiento continuo del marco de seguridad y el proceso de tratamiento de incidentes, ayuda a dirigir correctamente los aspectos legales que pudieran surgir en el tratamiento de incidentes.

CONCLUSIONES

El trabajo de tesis se ha concluido de manera satisfactoria, sobrepasando incluso, las expectativas iniciales, y es ahora un documento de referencia para el fortalecimiento lógico de las redes inalámbricas.

Se concluye que se ha alcanzado el objetivo inicial, el cual era: "Crear los elementos que permitan la gestión de manera ordenada y adecuada en los aspectos normativos, técnicos y de seguridad de las Redes Inalámbricas de la Facultad de Ingeniería de la UNAM; proporcionando para ello un fundamento teórico y práctico, a través del análisis, de políticas y de la creación de una herramienta en línea que consolide las actividades de regulación; generando con todo ello buenas prácticas en la operación de las redes inalámbricas".

Es importante destacar puntualmente los productos relevantes de este trabajo, por la importancia que representa haberlos generado en y para la Facultad de Ingeniería:

Se realizó el análisis de riesgos de las redes inalámbricas existentes en la Facultad de Ingeniería, utilizando la metodología OCTAVE lo que permitió la creación de una estrategia para mitigar los riesgos detectados, la aplicación de esta metodología arrojó los siguientes productos:

La creación de Políticas de Seguridad en Redes Inalámbricas permitirán regular el uso e implementación de este tipo de redes, como se mencionó durante el desarrollo de este trabajo, las políticas aquí descritas son una propuesta que deberán ser aprobadas por las autoridades correspondientes.

El procedimiento de registro de redes inalámbricas permitirá tener un control administrativo de las redes 802.11 existentes en la institución, que a su vez reflejará la aplicación de las Políticas de Seguridad en Redes Inalámbricas. Así mismo se podrán obtener datos estadísticos relacionados con estas tecnologías lo que dará lugar a obtener un panorama de la situación actual en cuanto a comunicaciones inalámbricas.

El desarrollo del sitio Web de "Gestión de Redes Inalámbricas de la Facultad de Ingeniería" permitirá centralizar la administración del sistema que se encargará de almacenar los registros de las redes inalámbricas que se tienen identificadas. Además este sistema Web permitirá la publicación de aspectos relacionados con buenas prácticas, auditoría y monitoreo en redes inalámbricas lo que harán de este proyecto un conjunto de fundamentos teóricos y prácticos en busca de una mejor gestión de estas tecnologías.

Las buenas prácticas para las redes inalámbricas permitirán ser una guía de implementación de estas tecnologías que ayudarán a dar solución a posibles vulnerabilidades en configuraciones de los dispositivos, siendo estas publicadas en el sitio Web.

Otra actividad que vale la pena resaltar fue el levantamiento del inventario lógico de redes inalámbricas el cual arrojó mucha información útil para establecer la actualidad del vecindario de comunicaciones 802.11, además la utilización de las herramientas empleadas dieron como resultado mapas de aproximación de parámetros de red que permiten concluir que es necesaria la aplicación de medidas normativas en este ámbito. Esta actividad fue parte del análisis de riesgos realizado que a su vez permitió la creación de una estrategia de mitigación de riesgos en base a las vulnerabilidades encontradas.

La aplicación de esta estrategia será un trabajo en donde se involucren las autoridades de la Facultad de Ingeniería, el Comité Asesor de Cómputo, los administradores de las redes, los responsables de cómputo del área, coordinación, secretaría o división, así como de los Departamentos de Seguridad en Cómputo y el Departamento de Redes y Operación de Servidores además de los usuarios finales.

La realización de este trabajo representó para mí una gran oportunidad para conocer de estas tecnologías inalámbricas que cada vez son más populares, me dio un panorama de que tan importante es la gestión de los recursos de cómputo en las organizaciones. El proyecto me permitió aplicar conocimientos adquiridos durante mi carrera profesional, desde programación de sistemas hasta seguridad en cómputo.

Se recomienda fortalecer el proyecto mediante la difusión de esta estrategia, ya que por sí mismo en estos momentos representa un eje fundamental en la administración de la infraestructura de cómputo en la Facultad de Ingeniería, además de que este sistema podría tener una mayor proyección mediante la automatización de ciertos procesos que en estos momentos se realizan de manera manual como son la obtención de datos para auditar las redes inalámbricas existentes.

GLOSARIO

A

AAA *(Authentication, Authorization, and Accounting).* Protocolo o sistema que permite a los usuarios proveer su identidad, obtener acceso a recursos y recolectar estadísticas de uso.
ACK (*acknowledgment).* Mensaje de confirmación de la estación receptora si la trasmisión fue correcta.
ACL *(Access Control List)* es un concepto usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.
ActionScript es un lenguaje de programación orientado a objetos (OOP), utilizado en especial en aplicaciones web animadas realizadas en el entorno Adobe Flash, la tecnología de Adobe para añadir dinamismo al panorama web.
Ad-hoc. Red inalámbrica que se caracteriza por ser temporal, conexión directa entre nodos.
AES *(Advanced Encryption Standard).* Esquema de cifrado por bloque de tamaño fijo de 128-bits, con llaves de 128, 192 o 256 bits respectivamente.
AP *(Access Point).* Dispositivo que une las estaciones 802.11 inalámbricas una red de estructura principal con cables.
API *(Application Programming Interface)* es el conjunto de funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.
ARP *(Address Resolution Protocol).* Es un protocolo de nivel de red responsable de encontrar la dirección hardware que corresponde a una determinada dirección IP.
ATM *(Asynchronous Transfer Mode)* es una tecnología de telecomunicación desarrollada para hacer frente a la gran demanda de capacidad de transmisión para servicios y aplicaciones

B

BSS *(Basic Service Set).* Conjunto de servicios básicos, es la base de las redes 802.11, conjunto de estaciones que están asociadas lógicamente entre sí.
BSSID *(Basic Service Set Identifier).* Identificador de 48 bits utilizado por todas las estaciones en un BSS de encabezados de trama.
Backbone también se refiere al cableado troncal o subsistema vertical en una instalación de red de área local que sigue la normativa de cableado estructurado.
Bluetooth es una especificación industrial para redes inalámbricas de área personal que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre.
Bridge es un dispositivo de interconexión de redes que opera en la capa 2 del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete.
Broadcast es un área lógica en una red en la que cualquier computadora conectada a la red puede transmitir directamente a cualquier otro en el dominio sin precisar ningún dispositivo de encaminamiento, dado que comparten la misma subred, dirección de puerta de enlace y están en la misma red de área local.

C

CCK *(Complementary Code Keying*). Cifrado de código complementario. Un esquema de modulación que trasforma los bloques de datos en códigos complejos y que puede codificar diversos bits por bloque.
CCM *(Counter Mode with CBC-MAC).* Un modo de código de bloque definido, se puede utilizar con cualquier código de bloque de 128 bits pero normalmente se utiliza con AES.

CCMP *(Counter Mode with CBC-MAC Protocol)*. 802.11i define el uso de AES con el método de operación CCM como CCMP. Es el protocolo de cifrado más fuerte para su uso en las redes inalámbricas de área local.
CRC es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión o almacenamiento
CSMA *(Carrier Sense Multiple Access)*. Acceso múltiple con escucha de portadora. Un esquema de escuchar antes de hablar utilizado para medir el acceso a un recurso de transmisión.
CSMA/CA *(Carrier Sense Multiple Access with Collision Avoidance)*. Acceso múltiple con escucha de portadora y evitación de colisión. Es un método que intenta evitar un acceso simultaneo aplazando el acceso al medio 802.11.
COBIT *(Control Objectives for Information and related Technology)* es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información.

D

DHCP *(Dynamic Host Configuration Protocol)*. Protocolo de configuración de host dinámico. Es un estándar IETF utilizado por los administradores de red para configurar hosts automáticamente.
DNS es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet.
DSSS *(Direct-Sequence Spread-Spectrum)*. Espectro disperse de secuencia directa. Una técnica de trasmisión que propaga una señal sobre una banda de frecuencia ancha para la trasmisión.

E

EAP *(Extensible Authentication Protocol)*. Protocolo de autenticación extensible. Protocolo de autenticación de estructura utilizado por 802.1x para proporcionar autenticación de la red.
ECB *(Electronic Code Book)*. Modo de cifrado de datos en el cual los mensajes se dividen en bloques y cada uno de ellos es cifrado por separado. La desventaja de este método es que a bloques de texto en claro idénticos les corresponde bloques idénticos de texto cifrado, de manera que se pueden reconocer estos patrones como guía para descubrir el texto en claro a partir del texto cifrado.
ESS *(Extended Service Sets)*. Conjunto de servicios extendidos. Colección lógica de puntos de acceso unidos.
Ethernet es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD.

F

FHSS *(Frequency Hopping Spread Spectrum*) es una técnica de modulación en espectro ensanchado en el que la señal se emite sobre una serie de radiofrecuencias aparentemente aleatorias, saltando de frecuencia en frecuencia sincrónicamente con el transmisor.
Firewall es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red.
Firmware es un bloque de instrucciones de programa para propósitos específicos, grabado en una memoria de tipo no volátil (ROM, EEPROM, flash,...), que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo.

G

GNU GPL es una licencia creada por la Free Software Foundation a mediados de los 80, y está orientada principalmente a proteger la libre distribución, modificación y uso de software.

GPS **(***Global Positioning System***)** es un Sistema Global de Navegación por Satélite (GNSS) que permite determinar en todo el mundo la posición de un objeto, una persona, un vehículo o una nave, con una precisión hasta de centímetros.
Gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

H

HTML **(***HyperText Markup Language***)** es el lenguaje de marcado predominante para la construcción de páginas web. Es usado para describir la estructura y el contenido en forma de texto, así como para complementar el texto con objetos tales como imágenes. HTML se escribe en forma de "etiquetas",
HTTP *(HyperText Transfer Protocol)* es el protocolo usado en cada transacción de la Web define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor.
HR/DSSS *(High-Rate Direct Sequence)* Espectro disperso de secuencia directa de alta velocidad. Abreviatura para las señales trasmitidas por equipamiento 802.11b.
Host una máquina conectada a una red de computadoras y que tiene un nombre de equipo.

I

IP *(Internet Protocol)* es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.
IBSS *(Independent Basic Service Set)*. Conjunto de servicios basicos independiente. Una red 802.11 sin un punto de acceso.
ICV *(Integrity Check Value)*. Valor de comprobacion de integridad. Suma de comprobación calculada sobre una trama antes de su cifrado WEP. Está diseñado para proteger la trama frente a sabotajes permitiendo a un receptor detectar alteraciones en la misma.
IEEE *(Institute of Electrical and Electronics Engineers)*. Organización profesional que ha estandarizado las redes IEEE 802.
IrDA *(InfraRed Data Association)* define un estándar físico en la forma de transmisión y recepción de datos por rayos infrarrojo.
IPsec *(Internet Protocol Security)* es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.
ISM *(Industrial, Scientific, and Medical)*. La parte 15 de las reglas FCC establecen aparte bandas de frecuencia en los Estados Unidos para su uso por equipamiento industrial, científico y medico sin licencia. La banda ISM de los 2.4 GHz inicialmente se estableció aparte para los hornos de microondas con el fin de que los usuarios de este electrodoméstico no necesitaran pedir una licencia FCC simplemente para calentar comida.
ITU *(International Telecommunications Union)*. Tecnicamente ITU emite recomendaciones, no reglas ni estadares. Sin embargo muchos países proporcionan recomendaciones ITU por ley.
IV *(Initialization Vector)*. Vector de inicialización. Generalmente utilizado como término para el material de cifrado expuesto en encabezados criptográficos. WEP expone 24 bits de clave secreta al mundo en el encabezado de la trama, incluso anque WEP se base en un código de flujo.
IEC *(International Electrotechnical Commission)* es una organización de normalización en los campos eléctrico, electrónico y tecnologías relacionadas.
ITIL *(Information Technology Infrastructure Library)*, es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

J

JSP (*Java Server Pages*) es una tecnología Java que permite generar contenido dinámico para web, en forma de documentos HTML, XML o de otro tipo.

K

Kerberos es un protocolo de autenticación de redes de ordenador que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Se basa en criptografía de clave simétrica y requiere un tercero de confianza.
Kbps Un kilobits por segundo es una unidad de medida que se usa en telecomunicaciones e informática para calcular la velocidad de transferencia de información a través de una red.
Keystream es un flujo de caracteres aleatorios o pseudoaleatorios que son combinados con un mensaje en texto plano para producir un mensaje cifrado.

L

LLC *(Logical Link Control)*. Control de enlace lógico. Una especificación de IEEE que permite más multiplexado sobre Ethernet. Las tramas 802.11 trasportan unidades de datos encapsulados en LLC.
L2TP *(Layer 2 Tunneling Protocol*) fue diseñado por un grupo de trabajo de IETF como el heredero aparente de los protocolos PPTP y L2F, creado para corregir las deficiencias de estos protocolos y establecerse como un estándar aprobado por el IETF.
Live CD es un sistema operativo (normalmente acompañado de un conjunto de aplicaciones) almacenado en un medio extraíble, tradicionalmente un CD o un DVD (de ahí sus nombres), que puede ejecutarse desde éste sin necesidad de instalarlo en el disco duro de una computadora, para lo cual usa la memoria RAM como disco duro virtual y el propio medio como sistema de ficheros.

M

MAC *(Medium Access Control*). Control de acceso al medio. Función en las redes IEEE que arbitran el uso de la capacidad de la red y determina las estaciones a las que les permite utilizar el medio para la trasmisión.
MIC *(Message Integrity Code)*. Código de integridad del mensaje. Un valor has calculado sobre un conjunto de datos protegidos para protegerlos frente al sabotaje. En la mayoría de los sistemas criptográficos, este valor se denomina código de autenticación de mensaje. 802.11 utiliza el algoritmo MIC para evitar la confusión con la capa de control de acceso al medio.
Mbps es una unidad que se usa para cuantificar un caudal de datos equivalente a 1000 kilobits por segundo o 1000000 bits por segundo.
Mhz Un Megahercio (MHz) equivale a 10^6 hercios (1 millón). Se utiliza muy frecuentemente como unidad de medida de la frecuencia de trabajo de un dispositivo de hardware.
MySQL es un sistema de gestión de base de datos relacional, multihilo y multiusuario.

N

NIC *(Network Interface Card)* Una tarjeta de red permite la comunicación entre diferentes aparatos conectados entre si y también permite compartir recursos entre dos o más equipos.
NIST *(National Institute of Standards and Technology)*. Agencia gubernamental de los Estados Unidos responsable de establecer los estándares de tecnología para el gobierno federal.

O

OFDM *(Orthogonal Frecuency Division Multiplexing)*. Multiplexado de división de frecuencia ortogonal. Una técnica que divide una banda de frecuencia estrecha e invierte los datos multiplexados a través de los subcanales. 802.11a y 802.11g se basan en OFDM .
OSI *(Open Systems Interconnection*). Interconexión de sistemas abiertos. Es un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones.

P

PAE *(Physical Address Extensión)* se refiere a una característica de los procesadores x86 que permite a los sistemas de 32-bit utilizar hasta 64 gigabytes (64 GiB) de memoria física, suponiendo que el sistema operativo proporcione el adecuado soporte
Payload material trasmitido sobre la red incluyendo datos e información que identifica la fuente y destino del material.
PCMCIA *(Personal Computer Memory Card International Association*). Un grupo del sector ha estandarizado el factor de forma de "tarjeta PCMCIA" y ha hecho posible conectar una amplia variedad de periféricos a equipos portátiles.
PDA *(Personal Digital Assistant)* es un computador de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, bloc de notas y recordatorios) con un sistema de reconocimiento de escritura.
PKI *(Public Key Infrastructure)* una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.
PLCP *(Physical Layer Convergence Procedure)*. Procedimiento de convergencia. El componente superior de la capa física en redes 802.11. Cada capa física tiene su propio PLCP, que proporciona tramas auxiliares para MAC.
PPP *(Point-to-point Protocol)* es un protocolo de nivel de enlace estandarizado en el documento RFC 1661. Por tanto, se trata de un protocolo asociado a la pila TCP/IP de uso en Internet permite establecer una comunicación a nivel de enlace entre dos computadoras.
PPTP *(Point to Point Tunneling Protocol)* es un protocolo desarrollado por Microsoft, U.S. Robotics, Ascend Communications, 3Com/Primary Access, ECI Telematics conocidas colectivamente como PPTP Forum, para implementar redes privadas virtuales o VPN.
PSK *(Pre-shared Key)*. En 802.11i, se refiere al método de autenticación que depende de la clave de autenticación cifrada estáticamente que tiene que distribuirse manualmente.

Q

QoS *(Quality of service)* son las tecnologías que garantizan la transmisión de cierta cantidad de datos en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio.

R

RADIUS *(Remote Authenticated Dial-In User Service)*. Servicio de autenticación de conexión telefónica remota autenticada. Un protocolo utilizado para autenticar usuarios de conexión telefónica que se ha utilizado más ampliamente debido a la autenticación 802.1X Es el tipo más común de servidor de autenticación utilizado en sistemas 802.1X.
A protocol used to authenticate dial-in users that has become more widely used because of 802.1X authentication. The most common type of authentication server used in 802.1X systems
RC4 . Algoritmo de código propietario desarrollado por RSA Data Security y cuya licencia es muy cara. Tambien se utiliza como base para WEP y evitar la existencia de implantaciones WEP de código libre debido a la amenaza de litigios por parte de RSA.

RF *(Radio Frequency)*. Radio frecuencia. Utilizado como objetivo para señalar que algo pertenece a la interfaz de radio ("modulador RF", "energía RF", etc.).
RSN *(Robust Security Network)*. Red de seguridad robusta. Una red que utiliza los métodos de seguridad de 802.11i y que no proporciona ninguna compatibilidad con WEP.
Rootkit es una herramienta, o un grupo de ellas que tiene como finalidad esconderse a sí misma y esconder a otros programas, procesos, archivos, directorios, llaves de registro, y puertos que permiten al intruso mantener el acceso a un sistema para remotamente comandar acciones o extraer información sensible, a menudo con fines maliciosos o destructivos.

S

SSID *(Service Set Identity)*. Identificador del conjunto de servicio. Una cadena utilizada para identificar conjunto de servicios extendido. Normalmente el SSID es una cadena de caracteres reconocibles.
Sniffer es un programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente, aunque también puede ser utilizado con fines maliciosos.
SSL **Secure Sockets Layer** Protocolo de Capa de Conexión Segura- protocolo criptográfico que proporciona comunicaciones seguras por una red.
Spam **correo basura** o **sms basura** a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor
Switch es un dispositivo analogico de logica de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (*Open Systems Interconnection*). Un conmutador interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.
Smart Cards. Tarjeta Inteligente es cualquier tarjeta del tamaño de un bolsillo con circuitos integrados que permiten la ejecución de cierta lógica programada.
SNMP *(Simple Network Management Protocol)*. Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento.
SMTP (*Send Mail Transfer Protocol*) protocolo simple de transferencia de correo. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.).
script un **script** es un guión o conjunto de instrucciones. Permiten la automatización de tareas creando pequeñas utilidades.

R

RTP *(Real-time Transport Protocol)* Es un protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo audio y vídeo en una video-conferencia.
Roaming es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra.

T

TKIP *(Temporal Key Integrity Protocol)*. Protocolo de integridad de clave temporal. Uno de los protocolos de cifrado mejorados en 802.11i que utiliza las operaciones fundamentales de WEP con los nuevos mecanismos de comprobación de integridad y cifrado WEP para ofrecer una seguridad adicional.
TCP *(Transmission-Control-Protocol)*. Protocolo de Control de Transmisión es uno de los protocolos fundamentales en Internet. Garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina.

TLS *(Transport Layer Security)*. Seguridad de la Capa de Transporte son protocolos criptográficos que proporcionan comunicaciones seguras por una red, comúnmente Internet.
TTL *(Time To Live)*. Tiempo de Vida es un concepto usado en redes de computadores para indicar por cuántos nodos puede pasar un paquete antes de ser descartado por la red o devuelto a su origen.
TDMA*(Time Division Multiple Access)*. Acceso múltiple por división de tiempo es una técnica de multiplexación que distribuye las unidades de información en ranuras ("slots") alternas de tiempo, proveyendo acceso múltiple a un reducido número de frecuencias.
TOKEN CARD es un dispositivo electrónico que proporciona autenticación a los usuarios vía telefónica y de internet.

U

UDP *(User Datagram Protocol)* es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera.
UMTS *(Universal Mobile Telecommunications System)* es una de las tecnologías usadas por los móviles de tercera generación (3G, también llamado W-CDMA), sucesora de GSM.

V

VPN (*Virtual Private Network)*. Red Privada Virtual es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

W

WLAN *(Wireless Local Area Network)*. Es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.
Wardriving. Se llama *wardriving* a la búsqueda de redes inalámbricas Wi-Fi desde un vehículo en movimiento. Implica usar un coche o camioneta y un ordenador equipado con Wi-Fi, como un portátil o una PDA, para detectar las redes.
Warchalking es un lenguaje de símbolos normalmente escritos con tiza en las paredes que informa a los posibles interesados de la existencia de una red inalámbrica en ese punto.
WEB. Red Global Mundial es un sistema de documentos de hipertexto y/o hipermedios enlazados y accesibles a través de Internet.
WEP *(Wired Equivalent Privacy)*. Privacidad equivalente al cableado. Estandar para codificación individual de las tramas de datos. Sediseño para proporcionar una privacidad mínima.
Wi-Fi La Wi-Fi- Allienace inicio el programa de certificación de certificación Wi-Fi (Fidelidad Inalámbrica) para aprobar la interoperatividad de la implantación 802.11. Originalmente el término se aplicaba a dispositivos que cumplían con 802.11b, ahora incluye la interoperatividad 802.11g y 802.11a así como la seguridad WPA.
WPA y WPA2 .Acceso Wi-Fi protegido. Estandar de seguridad basado en el borrador 3 de 802.11i.Wi-Fi Alliance tomo el borrador 3 de 802.11i y empezó a certificar la conformidad con las primeras implantaciones TKIP para acelerar la adopción de los protocolos de seguridad de 802.11.WPA2 se basa en la versión totalmente ratificada de 802.11i.

X

XOR Una **puerta lógica**, o **compuerta lógica**, es un dispositivo electrónico que es la expresión física de un operador booleano en la lógica de conmutación. Cada puerta lógica consiste en una red de dispositivos

interruptores que cumple las condiciones booleanas para el operador particular. Son esencialmente circuitos de conmutación integrados en un chip.

XML*(Extensible Markup Language)*. Es un metalenguaje extensible de etiquetas desarrollado por el World Wide Web Consortium (W3C).

BIBLIOGRAFÍA

Capítulo 1

1. **Barceló Ordinas José María, Íñigo Griera Jordi, Martí Escalé Ramón, Olivé Peig Enric**, *Redes de Computadores*, Fundació per a la Universitat Oberta de Catalunya, Marzo 2004, Barcelona.

2. **Beaver Kevin, T. Davis, Petter** *Hacking Wireless Networks For Dummies*, Wiley Publishing, Inc., 2005, Indianapolis, Inidana, USA.

3. **Convery, Sean,** *Network Security Architectures*, Cisco Systems, Inc, 2004, Indianapolis, USA.

4. **F. Mir, Nader**, *Computer and Communication Networks*, Prentice Hall, November 02, 2006, USA.

5. **Gast, Matthew**, *802.11 Wireless Networks: The Definitive Guide,O'Reilly*, April 2002. USA.

6. **Geier, Jim**, *Wireless LAN´s Second Edition*, Sams Publishing, 2002, Indianapolis, Indiana, USA.

7. **Harte, Lawrence,** *Introduction to 802.11 Wireless LAN (WLAN): Technology, Market, Operation, Profiles, & Services*, ALTHOS Publishing Inc.,2004, USA.

8. **Ilyas Mohammad, Ahson Syed**, *HANBOOK OF WIRELESS LOCAL AREA NETWORKS Applications, Technology, Security, and Standards*, Taylor & Francis Group, 2005,USA.

9. **J. Velte Toby, T. Velte Anthony***, Cisco 802.11 Wireless Networking Quick Reference*, Cisco Press, October 20, 2005,USA.

10. **K. Sarkar Tapan, J. Mailloux Robert, A. Oliner Arthur, L. Sengupta Diapk**, *History Of Wireless*, John Wiley & Sons. Inc.,2006, Canada.

11. **Maufer, Thomas**, *A Field Guide to Wireless LANs for Administrators and Power Users*, Prentice Hall PTR, October 17, 2003, USA.

12. **Minoli, Daniel,** *Hotspot Networks: Wi-Fi for Public Access Locations*, McGraw-Hill, 2003, USA.

13. **Ohrtman Frank, Roeder Konrad**, *Wi-Fi Handbook: Building 802.11b Wireless Networks,* McGraw-Hill,2003,USA.

14. **Prasad R.,Anand, Prasad R.,Neeli**, *802.11 WLANs and IP Networking security, QoS, and mobility*, Artech House mobile communicatos library, 2000,USA.

15. **Pejman Rpshan, Jonathan Leary**, *802.11 Wireless LAN Fundamenteals*, Cisco Press, December 23,2003, Indianapolis , USA.

16. **R. Vacca John***, Guide to Wireless Network Security*, Springer Science+Business Media, 2006, USA.

17. **Sankar Krishna, Sundaralingam Sri, Balinsky Andrew, Miller Darrin**, *Cisco Wireless LAN Security,* Cisco Press, November 15, 2004, Indianapolis, USA.

18. **Sarkar Kumar, T.G. Basavaraju, C, Puttamadappa**, *Ad Hoc Mobile Wireless Networks. Principles, Prorocols, and Applications*, Auerbach Publications Taylor & Francis Group, 2008,FL.,USA.

19. **Sweeney, Daniel**, *WiMax Op3rqtor´s Manual. Building 802.16 WirelessNetworks (Second Edittion)*, Apress, 2006, USA.

20. **Teare Diane, Paquet Catherine**, *Campus Network Design Fundamentals*, Cisco Press, December 08, 2005,Indianapolis, USA.

21. **Wheat Jeffery, Hiser Randy,Trucker Jackie, Neely Alicia, McCullough Andy**, *Design a Wireless Network*, Syngress Publishing Inc., 2001, USA.

Capítulo 2

1. **Barba Martí Antoni**, *Gestión de Red*, Edicions UPC, 1999, Barcelona.

2. **K. Shim Joe, G. Siegel Joel,** *THE VEST POCKET GUIDE TO INFORMATION TECHNOLOGY*, John Wiley & Sons, Inc.,2005, USA.

3. **Kamel, Sherif**, *Managing Globally with Information Technology*, Idea Group Publishing, 2003, USA.

4. **Kangas, Kalle,** *Business Strategies for Information Technology Management*, Idea Group Publishing, 2003,USA.

5. **L. Brennan Linda, E. Victoria**, *Social, Ethical and Policy Implications of Information Technology*, Idea Group Publishing, 2004, PA, USA.

6. **Reis, Ricardo***, Information Technology Selected Tutorials*, Kluwer Academic Publishers,2004, Boston,USA.

7. **T. Marchewka, Jack**, *INFORMATION TECHNOLOGY PROJECT MANAGEMENT.*

8. *Tecnología e innovación en la empresa. Dirección y gestión*, Edicions UPC,1998, Barcelona.

Capítulo 3

1. **Alberts Christopher, Dorofee Audrey,** *Managing Information Security Risks: The OCTAVE^{SM} Approach*, Addison Wesley, July 09, 2002, USA.

2. **David Cheye Hock Queay**, *FORMULATING A WIRELESS LAN SECURITY POLICY: RELEVANT ISSUES, CONSIDERATIONS AND IMPLICATIONS*, SANS Institute, 21 Feb 2002, FL,USA.

3. **Hurley Chris, Thornton Frank**, *War Driving & Wireless Penetration Testing, Syngress Publishing,* Inc., 2007, Canadá.

4. **J. Alberts Christopher, J. Dorofee Audrey**, *OCTAVE Technical Report*, Carnegie Mellon, December 2001, Pittsburg, USA.

5. **Vicente Altamirano Carlos Alberto, Espina García Eduardo**, *Mecanismos básicos de seguridad para redes de cómputo*, Dirección General de Servicios de Cómputo Académico, Diciembre 2005, México.

Capítulo 4

1. **Alarcón, Raúl,** *UML , DISEÑO ORIENTADO A OBJETOS CON UML*, Grupo EIDOS Consultaría y Documentación Informática, S.L., 2000, 2000, Madrid.

2. **Anderson Eve, Greenspun Philip, Grumet Andrew,** *Software Engineering for Internet Applications*. Massachusetts Institute of Technology, 2006, USA.

3. **Jacobson Dov, Jacobson Jessee,** *Flash and XML: A Developer's Guide*, Addison Wesley, November 20, 2001, Indianapolis USA.

4. **Rosenzweig, Gary,** *Sams Teach Yourself Flash™ MX Action Script in 24 Hours*, Sams Publishing, May 02, 2002, USA.

5. **S. Pressman, Roger,** *Software Engineering. A Practioner's Approach*, McGraw-Hill, 2001, New York, NY, USA.

6. **Schnier, Joachim,** *Flash XML Applications, Use AS2 and AS3 to Create Photo Galleries, Menus, and Databases*, Elsevier, Inc., 2008, Oxford, UK.

7. **Turner, James,** *MySQL™ and JSP™ Web Applications: Data-Driven Programming Using Tomcat and MySQL*, Sams Publishing, March 27, 2002, USA.

8. **W. Ambler Scott, Nalbone John, J. Vizdos Michael**, *The Enterprise Unified Process: Extending the Rational Unified Process*, Prentice Hall PTR, February 11, 2005, USA.

9. **Wutka Mark, Mittal Kunal,** *Sams Teach Yourself JavaServer Pages™ 2.0 with Apache Tomcat in 24 Hours,* Sams Publishing, December 04, 2003, USA.

Capítulo 6

1. **Chirillo, John,** *Hack Attacks Testing, How to conduct your own security audit*, Wiley Publishing, Inc., 2003, Indianapolis, Indiana, USA.

2. **Davis Chris, Wheeler Schillerandkevin Mike**, *IT Auditing: Using Controls to Protect Information Assets*, McGraw-Hill, 2007, NY, USA.

3. **E. Cascarino, Richard,** *Audito's Guide to Information Systems Auditing*, John Wiley & Sons, Inc., 2007, New Jersey, USA.

4. **Parker Tom, Shaw Eric, Stroz Ed, G. Devost Matthew, H. Sachs Marcus,** *Cyber Adversary Characterization: Auditing the Hacker Mind*, Syngress Publishing, Inc., 2004, USA.

5. **S. Wright Craig**, *A Taxonomy of Information Systems Audits, Assessments and Reviews*, SANS Institute, 2007, FL, USA.

6. **T. Hoesing Michael, Raval Vasant**, *Using Wireless Network Audit Techniques, Information Systems Audit and Control Association,* 2004, USA.

Capítulo 7

1. **B. Ferreyro, Lorena**, *Gestión y tratamiento de incidentes de seguridad de la información*, ArCERT, Julio 2008, Argentina.

2. **Lafarge, Eduard,** *Wireless Network Audits using Open Source tools*, SANS Institute, 2003, FL, USA.

3. **Merola, Antonio**, *WiFi with BackTrack*, SANS Institute, 2007, FL,USA.

4. **Milus, Stu**, *The Institutional Need for Comprehensive Auditing Strategies*, SANS Institute,2003, FL, USA.

5. **Turner, Raymond**, *Wireless Security and Monitoring for the Home Network*, August 21, 2003, FL, USA.

MESOGRAFÍA

1. "***A Wireless LAN (WLAN) security site provided for 802.11*** ", disponible en: http://wirelessdefence.org/ , enero 2009.

2. **"*Aircrack-ng*",** disponible en: http://www.aircrack-ng.org/doku.php , enero 2009.

3. ***"Como usar archivos XML en Flash",*** disponible en: http://www.leobaraldi.com.ar/index.php?paged=2&s=ect , enero 2009.

4. David Alayonon, ***"Tutorial: Hacking Wireless"***, disponible en: http://www.pisitoenmadrid.com/blog/2006/12/tutorial-hacking-wireless/, enero 2009.

5. David Maynor, "***Beginner's Guide to Wireless Auditing"***, disponible en: http://www.securityfocus.com/infocus/1877 , enero 2009.

6. ***"Ethereal",*** disponible en: http://thud.ethereal.com/, enero 2009

7. ***"FusionCharts Free",*** **disponible en: http://www.fusioncharts.com/free/, enero 2009.**
8. ***"Herramientas del software Wi-Fi para las plataformas múltiples",*** disponible en: http://www.mapawifi.cl/softwares-para-redes-wifi/, enero 2009.

9. **"*Hotplug vs. Garmin USB on Linux*"**, disponible en: http://www.gpsbabel.org/os/Linux_Hotplug.html, enero 2009.

10. ***"Identity Theft Tool – Kismet"***, disponible en: http://www.wifisecurityguy.com/learn/blog/identity-theft-tool-kismet , enero 2009.

11. ***"Insertar SWF de Flash en XHTML valido",*** disponible en: http://www.cristalab.com/tutoriales/insertar-swf-de-flash-en-xhtml-valido-c154l/, enero 2009.

12. ***"Installing Kismet with a handheld gps device"***, disponible en: http://www.yesyesnono.co.uk/ , enero 2009.

13. **"*Kismet + GPSDrive + MySQL + Python = Google Earth Wlan Map*"**, disponible en: http://www.larsen-b.com/Article/212.html#gpsdrive , enero 2009.

14. ***"Manual Básico (in)seguridad wireless ",*** disponible en: http://foro.elhacker.net/hacking_wireless/manual_basico_inseguridad_wireless_usando_y_configurando_linux_troppix-t105952.0.html , enero 2009.

15. Manuel González Valiñas, ***"Seguridad en Redes 802.11x"***, disponible en: http://www.atc.uniovi.es/inf_med_gijon/3iccp/2006/trabajos/wifi/, enero 2009.

16. Osvaldo Callegari, *"**El malvado Evil Twin"***, disponible en: http://www.ventasdeseguridad.com/index.php/De-Portada-Tecnologias-de-la-informacion/El-malvado-Evil-Twin , enero 2009.

17. ***"SANS InfoSec Reading Room - Wireless Access",*** disponible en: http://www.sans.org/reading_room/whitepapers/wireless/, enero 2009

18. Tabacman Eduardo, "***Las 20 mejores prácticas para gestionar redes inalambricas Wi-Fi",*** disponible en**:** http://www.virusprot.com/Redes-Inalambricas-Wifi/articulos-wireless-wifi/wifi-redes-best-practices.htm#Red_WIFI_Best_Practices_Políticas, enero 2009.

19. *"**Tomcat, Apache y JSP"**,* disponible en: http://huevon.blogspot.com/2007/08/tomcat-apache-y-jsp.html, enero 2009.

20. *"**Tutorial de XML en Flash"**,* disponible en: http://www.cristalab.com/tutoriales/tutorial-de-xml-en-flash-c12l/, enero 2009.

21. Universidad de Alicante ***"Normativa para las redes inalámbricas locales departamentales",*** disponible en**:** http://www.ua.es/es/internet/wirelessua/otros/index.html, enero 2009.

22. University of California, *"**IT Security-related policies and guidelines**",* disponible en: https://security.berkeley.edu/policies.html, enero 2009.

23. ***"Wardriving tools and wireless utilities download resource."***, disponible en: http://www.pointblanksecurity.com/wardriving-tools.php , enero 2009.

24. ***"Wardriving with Ubuntu Linux and Google Earth"***, disponible en: http://www.perrygeo.net/wordpress/?p=55, enero 2009.

25. "***Wardriving Kismet / GPSD***", disponible en: http://scratchdrive.com/wordpress/?p=8, enero 2009.

26. "***Wardriving Using An Ubuntu Notebook With Garmin Etrex, Kismet, And GPSDrive***", disponible en: http://www.howtoforge.com/wardriving_garmin_kismet_gpsdrive_ubuntu, enero 2009.

27. ***"Wireless Vulnerabilities & Exploits",*** disponible en: http://www.wirelessve.org/entries/vulnerabilities?page=2 , enero 2009.