UNIVERSIDAD TÉCNICA DE COTOPAXI

CARRERA DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

TEMA:

"IMPLEMENTACIÓN DE LA CONECTIVIDAD Y SEGURIDAD INALÁMBRICA PARA EL MINISTERIO PÚBLICO SEDE LATACUNGA"

POSTULANTE:

Villamar Parra Jorge Luis

DIRECTOR:

Ing. Patricio Chávez

Latacunga – Ecuador

Febrero - 2009

AUTORÍA

Yo, Villamar Parra Jorge Luis declaro que el trabajo aquí presentado es de mi autoría, que no ha sido previamente presentado, y que he consultado todo lo que en este tomo está incluido.

Villamar Parra Jorge Luis

C.I. 050218467-4

CERTIFICACIÓN

HONORABLE CONSEJO ACADÉMICO DE LA UNIVERSIDAD TÉCNICA DE COTOPAXI.

De mi consideración.

Cumpliendo con lo estipulado en el capítulo IV, (art. 9 literal f), del reglamento del curso profesional de la Universidad Técnica de Cotopaxi, informo que el postulante: Villamar Parra Jorge Luis, ha desarrollado su tesis de grado de acuerdo al planteamiento formulado en el plan de tesis con el tema: "Implementación de la Conectividad y Seguridad Inalámbrica para el Ministerio Público sede Latacunga", cumpliendo con los objetivos planteados.

En virtud de lo antes expuesto, considero que la presente tesis se encuentra habilitada para presentarse al acto de la defensa de tesis.

Latacunga, 13 de Noviembre del 2008

Atentamente,

Ing. Patricio Chávez.

DIRECTOR DE TESIS

AGRADECIMENTO

Quiera agradecer sinceramente aquellas personas que compartieron sus conocimientos conmigo para hacer posible la conclusión de estas tesis. Especialmente agradezco a mi Director y Asesor de Tesis. Gracias a todos mis compañeros por su gran ayuda cuando me enfrentaba con ciertos problemas.

Gracias a todos ellos.

Jorge Luis

DEDICATORIA

A mi madre y a mi Hermano, por su gran ejemplo de superación y valioso apoyo en todos los momentos desde el inicio de mis estudios.

A mi esposa por ese optimismo que siempre me impulsó a seguir adelante y por los días y horas que hizo el papel de madre y padre.

A mis hijos por todas las veces que no pudieron tener a un Papá de tiempo completo.

A mis familiares y amigos que tuvieron una palabra de apoyo para mí durante mis estudios.

Jorge Luis

ÍNDICE GENERAL

RESUMEN

Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante ondas de radio o luz infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos.

La tecnología de redes inalámbricas ofrece movilidad y una instalación sencilla, además permite la fácil ampliación una red. Es decir, que podemos estar moviéndonos por nuestra empresa / calle / parque / cafetería / aeropuerto (imaginación al poder) sin perder la conectividad con la red. Esto es algo que actualmente está tomando gran importancia, no ya tanto para el típico ejecutivo de chaqueta y portátil, sino para todo el mundo.

El Ministerio Público de Latacunga al no contar con un edificio propio no puede darse el lujo de invertir en cableado estructurado para poder levantar su infraestructura de comunicaciones, por lo que la implementación de una WLAN se hace imperiosa por su versatilidad y movilidad que estás nos puede proporcionar.

Las redes inalámbricas tienen un costo un tanto más elevado que las redes convencionales con cables, pero una vez implementada esto ayudaría a que se ahorre en costos y rendimiento ya que un usuario ya no tendría que estar realizando su trabajo de forma rígida como se acostumbra, sino más bien la tendencia es trabajar con computadores portátiles que cada día revolucionan el mercado por sus prestaciones y valor.

Las redes inalámbricas han abierto una gran cantidad de oportunidades de negocio a nivel mundial. Sin embargo, existe un aspecto que aún despierta muchas inquietudes y genera duda entre los usuarios. Este aspecto está relacionado con la criticidad de la información en lo concerniente a la seguridad de la misma. En esta documento se identifican los riesgos más importantes a los que se expone la información administrada empleando tecnología de redes inalámbricas, y se presentan diversas estrategias y mecanismos, que implementados en soluciones móviles o inalámbricas, pueden garantizar la protección de dicha información.

INTRODUCCIÓN

En los últimos tiempos la informática es la herramienta más poderosa que el hombre ha tenido en sus manos y que en este momento interviene de forma directa ó indirecta en, prácticamente, todas las actividades humanas. Dejar que esta herramienta sea controlada y restringida por agentes solo interesados en su propio lucro supone un perjuicio para las sociedades. La interconectividad inalámbrica constituye una oportunidad histórica de tomar el control de nuestro propio destino. Por esta razón es hora ya que empresas, instituciones, universidad y hogares hagamos conciencia, y busquemos la manera de explotar de mejor manera este recurso.

Desde siempre el anhelo de todos los usuarios de computadores personales o de portátiles, ha sido el poder contar con el Internet en todo su hogar u oficina sin necesidad de estar relegado a un solo sitio, pudiendo movilizarse a través de toda la casa o de todas las oficinas que pueden constituir una institución o empresa. Como consecuencia de esto todos buscamos alternativas para lograr alcanzar y cumplir con está meta.

La mejor manera de alcanzar este objetivo es equipar las computadoras de la oficina y las portátiles con trasmisores y receptores de radio de onda corta que permita comunicarse. Todo esto hizo que más empresas busquen comercializar las

redes inalámbricas, para satisfacer las necesidades de comunicación tanto a clientes como instituciones.

En el Ministerio Público se decide adoptar está tecnología luego de un minucioso estudio de factibilidad en la cual se investiga marcas y desempeño de cada una de ellas, se reviso, las prestaciones alcance, versatilidad y por supuesto la escalabilidad, luego de lo cual el que más se ajustó a las necesidades de la institución fue DLINK, así también una vez escogido los equipos se investigó el estándar que más se enmarque en la realidad del Ministerio.

El objetivo del presente tema de estudio fue demostrar que mediante una red inalámbrica podremos brindar un buen servicio de intercomunicación entre computadoras, adicionalmente flexibilidad para el traslado de los computadores de un lado a otro, adicionando un valor agregado que es la seguridad de la información, precautelando las actividades de los usuarios de red.

De las fortalezas de la presente investigación es el poder contar con suficiente información bibliografíca, además de que se baso íntegramente en los estándares internacionales para las configuraciones, no podemos dejar de mencionar la importante colaboración de parte del Departamento de Sistemas del Ministerio Público del Ecuador con su sede principal en la ciudad de Quito de los

departamentos de sistemas de algunas empresas las cuales nos sirvieron como modelo para poder llegar alcanzar los objetivos.

Este trabajo de investigación para una mejor interpretación se lo ha estructurado en tres capítulos:

El primer capítulo corresponde a la descripción de algunos aspectos importantes de las redes Inalámbricas, de las WLAN (Wireless Local ÁREA Network), así como información de las Seguridades, servidores, etc.

El segundo corresponde a la investigación de campo, la misma que se realizó mediante una entrevista al Director del Departamento de Ingeniería en Sistemas del Ministerio Publico del Ecuador, las encuestas realizadas en el Ministerio Público sede Latacunga sobre el servicio que presta el departamento en la actualidad y sobre su opinión ante la implementación de una red inalámbrica.

El tercer capitulo consta de la implementación y configuraciones de las seguridades de las redes inalámbricas, previo el estudio de la factibilidad técnica-tecnológica y económica de la institución.

Finalmente las conclusiones con sus respectivas recomendaciones producto del presente trabajo de investigación.

CAPITULO I

1. ESTUDIO DE LA CONECTIVIDAD Y SEGURIDAD INALÁMBRICA

1.1.REDES INALÁMBRICAS

1.1.1. Conceptos

Partamos de la definición de inalámbrico, este término se refiere al uso |de la tecnología sin cables la cual permite la conexión de varios computadores entre sí. "Las redes de área local inalámbricas (WLAN, Wireless Local Area Network) están ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas. Las WLAN permiten a sus usuarios acceder a información y recursos en tiempo real sin necesidad de estar físicamente conectados a un determinado lugar. Con las WLANs la red, por si misma, es móvil y elimina la necesidad de usar cables y establece nuevas aplicaciones añadiendo flexibilidad a la red. Un usuario dentro de una red WLAN puede transmitir y recibir voz, datos y vídeo dentro de edificios, entre edificios o campus universitarios e inclusive sobre áreas metropolitanas a velocidades de 11 Mbit/s, o superiores".[1]

[1] Carballar, José A. El libro de las Comunicaciones del PC, HP, España, 2006. Pág. 10-39

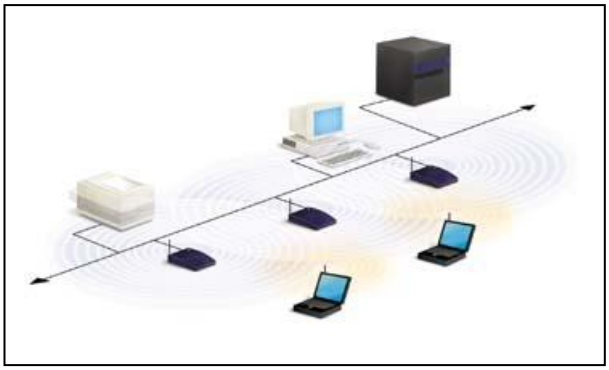


Gráfico 1.1: REDES INALAMBRICAS
Fuente: EL INVESTIGADOR

1.1.2. Orígenes

"Las redes de área local inalámbrica funcionan desde hace varios años en entornos industriales y de investigación.

Se implementaron por primera vez en 1979 como resultados de un experimento realizado por ingenieros de IBM en Suiza, consistente en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

En marzo de 1985 la Comisión Federal de Comunicaciones, FCC, organismo encargado de la regulación de las telecomunicaciones en Estados Unidos, asignó a los sistemas WLAN las bandas frecuenciales 902-928 MHz., 2.400-2.4835 GHz. y 5.725-5.850 GHz también conocidas como ISM (Industrial, Científica y Médica) y que pueden utilizarse bajo licencia administrativa.

Esta asignación de una localización frecuencial fija propició una mayor actividad industrial. En este punto las redes de área local inalámbrica dejaron de ser meramente experimentales para empezar a introducirse en el mercado.

Entre los anos 1985 y 1990 se trabajó en el desarrollo de productos WLAN y finalmente, en mayo de 1991, se publicaron algunos trabajos que hablaban sobre redes inalámbricas que superaban la velocidad de transferencia de 1 Mbps, velocidad mínima a partir de la cual el comité IEEE considera que una red es de área local.

Hasta ese momento las WLAN habían tenido una aceptación marginal en el mercado por dos razones fundamentales: falta de un estándar y precios elevados de la solución inalámbrica". [2]

En estos últimos años se ha producido un crecimiento en el mercado de hasta un 100 % anual. Este hecho es atribuible a dos razones principales:

- El desarrollo del mercado de los equipos portátiles y de las comunicaciones móviles que han producido que los usuarios puedan estar en continuo movimiento manteniendo comunicación constante con otros terminales y elementos de la red. En este sentido, las comunicaciones inalámbricas ofrecen una prestación no disponible en las redes cableadas: movilidad y acceso simultáneo a los recursos de la red.

- La conclusión de la definición de la norma IEEE 802.11 para redes de área local inalámbricas el pasado junio de 1997 que ha establecido un punto de referencia y ha mejorado muchos de los aspectos de estas redes.

A pesar del atractivo y funcionalidad de las WLAN, la falta de estándares que brinden confianza a los potenciales usuarios de esta tecnología, fue otra de las razones de la lenta acogida que tuvieron

[2] Tomado de: www.monografias.com/reporte/redesinal/redinal.htm

en el pasado. En la actualidad se han definido normas internacionales que regulan la operación y funcionamiento de los elementos y protocolos de WLAN. Entre las normas más importantes para este tipo de redes tenemos la realizada por e! subcomité 802.11 del Instituto de Ingenieros Eléctricos y Electrónicos de los Estados Unidos (IEEE).

1.1.3. Ámbito de aplicación

En nuestra era han surgido los adictos a la información, gente que necesita estar todo el tiempo en línea. Para estos usuarios móviles, cable de par trenzado, el cable coaxial y la fibra óptica nos son útiles.

Ellos necesitan obtener datos para sus computadores laptops, notebook, de bolsillo, de mano, celulares, de pulsera o reloj, sin estar limitados a la infraestructura de comunicaciones terrestres. Para estos usuarios la comunicación inalámbrica en general veremos que tiene otras aplicaciones importantes además de proporcionar conectividad a los usuarios que desean navegar por la WEB.

1.1.3.1. Espectro Electromagnético

"Se denomina **espectro electromagnético** al conjunto de ondas electromagnéticas o, más concretamente, a la radiación electromagnética que emite (espectro de emisión) o absorbe (espectro de absorción) una sustancia. Dicha radiación sirve para identificar la sustancia de manera análoga a una huella dactilar.

Van desde las de menor longitud de onda, pasando por la luz ultravioleta, la luz visible y los rayos infrarrojos, hasta las ondas electromagnéticas de mayor longitud de onda, como son las ondas de radio."[3]

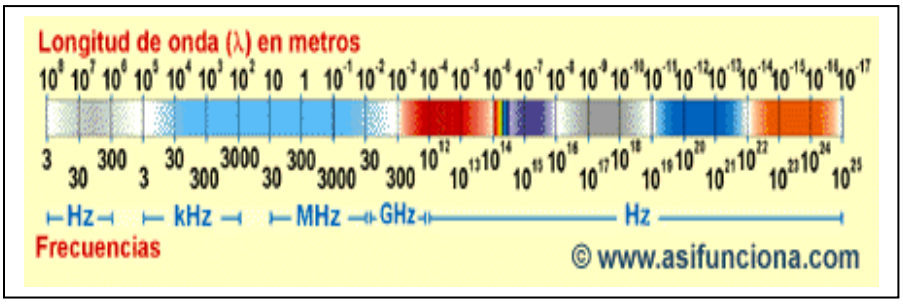


Gráfico 1.2: ESPECTRO ELECTROMAGNÉTICO.
Fuente: WIKIPEDIA, LA ENCICLOPEDIA LIBRE.

1.1.3.2. Ondas Electromagnéticas

"Son ondas producidas por la oscilación o la aceleración de una carga eléctrica. Las ondas electromagnéticas tienen componentes eléctricos y magnéticos. La radiación electromagnética se puede ordenar en un espectro que se extiende desde ondas de frecuencias muy elevadas (longitudes de onda pequeñas) hasta frecuencias muy bajas (longitudes de onda altas)"[4].

1.1.3.3. Ondas de radio.

"Las ondas de Radio son un tipo de ondas electromagnéticas, lo cual confiere tres ventajas importantes: No es necesario un medio

[3] Tomado de: www.wikipedia.org/ondas.html, Espectro Electromagnético, Pablo Sanchez, Mayo 2006.
[4] Tomado de: www.wikipedia.org/ondaselectro.html, Ondas Electromagnéticas, Pablo Sanchez, Mayo 2006.

físico para su propagación, las ondas electromagnéticas pueden propagarse incluso por el vacío. La velocidad es la misma que la de la luz, es decir 300.000 Km/seg. Objetos que a nuestra vista resultan opacos son transparentes a las ondas electromagnéticas"[5].

Gráfico 1.3: ONDAS DE RADIO
Fuente: REDES DE COMPUTADORAS. ANDREW TANENBAUM

1.3.3.1.2 Microondas Terrestres

Suelen utilizarse antenas parabólicas. Para conexiones a larga distancia, se utilizan conexiones intermedias punto a punto entre antenas parabólicas. Se suelen utilizar en sustitución del cable coaxial o las fibras ópticas ya que se necesitan menos repetidores y amplificadores, aunque se necesitan antenas alineadas. Se usan para transmisión de televisión y voz.

Gráfico 1.4: MICROONDAS TERRESTRES
Fuente: REDES DE COMPUTADORAS. ANDREW TANENBAUM

[5] Tomado de: Redes de Computadoras, Cuarta Edición, TANENBAUM Andrew, Editorial Prentice Hall, Año 2005, Pág 65

1.1.3.4. Ondas Infrarrojas.

Llamadas también térmicas, llegan hasta la luz visible (el rojo del espectro), se producen por la vibración de los electrones de las capas superiores de ciertos elementos, estas ondas son absorbidas fácilmente por la mayoría de los materiales. La energía infrarroja que absorbe una sustancia aparece como calor, ya que la energía agita los átomos del cuerpo, e incrementa su movimiento de vibración o translación.

1.1.3.5. Ondas Visibles.

Son la parte del espectro electro-magnético que puede percibir el ojo humano. La luz se produce por la disposición que guardan los electrones en los átomos y moléculas. Las diferentes longitudes de onda se clasifican en colores que varían desde el violeta el de menor longitud de onda hasta el rojo el de mayor longitud de onda (de 4 a $7x10^{-7}$).

1.1.3.6. Ondas Ultravioletas.

Los átomos y moléculas sometidos a descargas eléctricas producen este tipo de radiación. No debemos de olvidar que la radiación ultravioleta es la componente principal de la radiación solar. La energía de los fotones de la radiación ultravioleta es del orden de la energía de activación de muchas reacciones químicas.

1.1.3.7. Rayos X.

Si se aceleran electrones y luego, se hacen chocar con una placa metálica, la radiación de frenado produce rayos X. Los rayos X se han utilizado en medicina desde el mismo momento en que los descubrió Röntgen debido a que los huesos absorben mucho más radiación que los tejidos blandos.

1.1.4. Wireless LAN entre oficinas

La tecnología WLAN puede remplazar a las redes cableadas tradicionales o ampliar su alcance y sus capacidades. De igual modo que sus homologas con cables, el equipo de las WLAN interiores se compone de una tarjeta PC y adaptadores de clientes PCI e ISA, así como de Puntos de Acceso, que realizan funciones similares a las que realizan los hubs en las redes tradicionales.

1.2. PROTOCOLOS DE TRANSMISIÓN

Los diversos mecanismos de acceso que se han propuesto e implantado para WLAN se agrupan en dos categorías: protocolos con arbitraje (FDMA, TOMA) y protocolos por contención (CDMA/CD, CDMA/CA).

Tipo de configuración WLAN sencilla, entre varias computadoras sin necesidad de usar un Access Point también se han diseñado protocolos que son una combinación de estas dos categorías.

Aunque ya no es habitual su utilización dentro de los sistemas WLAN, el mecanismo de mulitplexación en frecuencia, FDMA, divide todo el ancho de banda asignado en distintos canales individuales. Este es un mecanismo simple que permite el acceso inmediato al canal, pero poco eficiente para

su utilización en sistemas que presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa algo más factible es asignar todo el ancho de banda disponible a cada nodo durante un breve intervalo de tiempo de manera cíclica, este sistema llamado multiplexación en el tiempo (TOMA), requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias.

Este último esquema ha sido utilizado con cierto éxito, sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

Por el contrario, el protocolo de acceso múltiple por división de código (COMA), es el mecanismo de acceso por excelencia para que puedan coexistir diferentes redes.

Varias de las primeras redes utilizaban el algoritmo de acceso al medio, CSMA/CD. El cual se caracteriza por comprobar previamente que el medio de comunicación esté libre, antes de iniciar la transmisión. Si se tiene esta condición, entonces se transmite la información y si no, se espera a que se libere el medio.

Como existía la posibilidad de que dos estaciones transmitieran información simultáneamente, este mecanismo exigía que a pesar de iniciar la transmisión se debiera continuar con la vigilancia del canal para detectar posibles colisiones. Cuando esto ocurría, la transmisión era suspendida y las estaciones involucradas en el conflicto debían esperar un tiempo aleatorio antes de repetir nuevamente el algoritmo.

El protocolo 802.11, utiliza un tipo de protocolo conocido como CSMA/CA (Carrier-Sense, Múltiple Access, Colusión Avoidance). Este

protocolo introduce una variante en el algoritmo anterior que evita las colisiones en la transmisión, en lugar de descubrir una colisión, fundamentado en el hecho de que la mayor probabilidad de que se produzca una colisión en CSMA/CD se da al terminar una transmisión.

Es decir, al haber más de una estación esperando que una transmisión en curso termine para que ellas puedan comenzar a transmitir, si no se adoptan las medidas oportunas estas estaciones comenzarán, todas a la vez, a enviar información provocando una colisión en el medio.

En el sistema CSMA/CA, cuando una estación identifica el fin de una transmisión, espera un tiempo aleatorio antes de transmitir, disminuyendo así la probabilidad de colisión.

A pesar del buen comportamiento general de este sistema, presenta una deficiencia debida al problema conocido como Terminal Oculto. Este problema se presenta cuando un dispositivo inalámbrico transmite con la potencia justa para que sea escuchado por un nodo receptor, pero no con la suficiente como para que otra estación, que se encuentra a la espera, sepa que hay otra unidad que está transmitiendo. Para resolver este conflicto, se ha añadido al protocolo de acceso CSMA/CA un mecanismo de intercambio de mensajes con reconocimiento positivo.

Este proceso hace que cuando una estación está lista para transmitir, primero envía una solicitud al punto de acceso (RTS - Request to Send)) quien, si no encuentra problemas, responde con una autorización (CTS - Clear to Send) que permite al solicitante enviar su datos. Cuando el punto de acceso ha recibido correctamente la información, envía una trama de reconocimiento (ACK - acknowledgment packet) notificando al transmisor el éxito de la transmisión.

Independientemente de los protocolos de acceso al medio y para dar soporte a las medidas de seguridad tan necesarias en este tipo de redes, ios sistemas inalámbricos, como complemento adicional y característica optativa para evitar las escuchas indiscretas, disponen de una herramienta de codificación de la información. La seguridad de los datos se realiza mediante una compleja técnica de codificación conocida como WEP (Wired Equivalent Privacy Algorithm).

El sistema WEP se basa en proteger los datos transmitidos en el medio RF, usando una clave generada por un número pseudo aleatorio y un algoritmo de encriptación. Cuando se habilita este sistema, sólo se protege la información del paquete de datos y no protege el encabezamiento de la capa física para que las demás estaciones puedan escuchar el control de datos necesario para la adecuada gestión de la red.[6]

1.3. ORÍGENES DE LAS REDES DE ÁREA LOCAL INALÁMBRICAS

El origen de las LAN inalámbricas (WLAN) se remonta a la publicación en 1979 de los resultados de un experimento realizado por ingenieros de IBM en Suiza, consistía en utilizar enlaces infrarrojos para crear una red local en una fábrica. Estos resultados, publicados en el volumen 67 de los Proceeding del IEEE, pueden considerarse como el punto de partida en la línea evolutiva de esta tecnología.

Las investigaciones siguieron adelante tanto con infrarrojos como con microondas, donde se utilizaba el esquema del "spread-spectrum"(frecuencias altas), siempre a nivel de laboratorio. En mayo de 1985, y tras cuatro años de estudios, el FCC (Federal Communications Comission), la agencia federal del Gobierno de Estados Unidos encargada de regular y administrar en materia de telecomunicaciones, asignó las

[6] Carballar, José A. El libro de las Comunicaciones del PC, HP, España, 2006. Pág. 120-139

bandas IMS (Industrial, Scientific and Medical) 902-928 MHz, 2,400-2,4835 GHz, 5,725-5,850 GHz a las redes inalámbricas basadas en "spread-spectrum". IMS es una banda para uso comercial sin licencia: es decir, el FCC simplemente asigna la banda y establece las directrices de utilización, pero no se involucra ni decide sobre quién debe transmitir en esa banda. La asignación de una banda de frecuencias propició una mayor actividad en el seno de la industria: ese respaldo hizo que las WLAN empezara a dejar ya el laboratorio para iniciar el camino hacia el mercado. Desde 1985 hasta 1990 se siguió trabajando ya más en la fase de desarrollo, hasta que en mayo de 1991 se publicaron varios trabajos referentes a WLAN operativos que superaban la velocidad de 1 Mbps, el mínimo establecido por el IEEE 802 para que la red sea considerada realmente una LAN.[7]

Fuente: WWW.AIRONET.COM

1.4. TIPOS DE REDES INALÁMBRICAS

1.4.1. Redes de área extensa (WAN)

La revolución más grande de la comunicación si cables se inició con los teléfonos móviles, los cuales han sido el producto electrónico con mayor éxito de todos lo tiempos. Inicialmente solo ofrecían comunicación por voz, ahora con baterías de mayor duración interfaces inteligentes,

[7] www.aironet.com/wireless.php, Origen de la tecnología inalámbrica, Juan Paúl Salvatierra, Octubre 2003.

reconocimiento de voz y mayor velocidad, su uso futuro estará relacionado más con sus nuevos servicios inalámbricos.

1.4.2. Métodos de Acceso celular

Los usuarios que ocupan un área geográfica deben disputarse un número limitado de canales y existen varios métodos de dividir el espectro para proporcionar acceso de forma organizada: El FDMA (Frequency División Múltiple Access), El TDMA (Time Division Multiple Access), El GSM (Global System for Mobile Communications), El CDAM (Code Division Multiple Access). Existen dos tipos principales de señales la analógica y la digital.

1.4.3. Redes de área local (LAN)

Una red de área local es un grupo de computadores y otros equipos relacionados que comparten una línea de comunicación y un servidor común dentro de un área geográfica determinada como un edificio de oficinas. Es normal que el servidor contenga las aplicaciones y controladores que cualquiera que se conecte a la LAN pueda utilizar.

1.4.4. Redes de área local sin cables (WLANs)

Ofrece acceso sin cables a todos los recursos y servicios de una red corporativa (LAN) en un edificio o todo un campus. Proporciona más libertad en el ambiente de trabajo. A través de una red sin cables los trabajadores pueden acceder a la información desde cualquier lugar de la compañía. Lo cual les ofrece numerosas ventajas:

- Acceso fácil y en tiempo real para realizar consultas desde cualquier lugar.
- Acceso mejorado a la base de datos.
- Configuración de red simplificada con mínima implicación MIS.
- Acceso independiente de la localización para administradores de redes.

1.4.5. Redes de área personal (PAN)

Existe dentro de un área relativamente pequeña, que conecta dispositivos electrónicos con ordenadores, impresoras, escáner, aparatos de fax, PDAs y ordenadores notebook, sin la necesidad de cables ni conectores para que sea efectivo el flujo de información. El estándar de comunicaciones sin cables WPAN se centra en temas como el bajo consumo (para alargar la vida de los dispositivos portátiles), tamaño pequeño (para que sean más fáciles de llevar) y costos bajos (para que los productos puedan llegar a ser de uso masivo).

1.5. REDES PÚBLICAS DE RADIO

Las redes públicas tienen dos protagonistas principales: "ARDIS" (una asociación de Motorola e IBM) y "Rarn Mobüe Data" (desarrollado por Ericcson AB, denominado MOBITEX). Este último es el más utilizado en Europa.

Estas Redes proporcionan canales de radio en áreas metropolitanas, las cuales permiten la transmisión a través del país y que mediante una tarifa pueden ser utilizadas como redes de larga distancia.

La compañía proporciona la infraestructura de la red, se incluya controladores de áreas y Estaciones Base, sistemas de cómputo tolerantes a fallas. Estas redes se encuentran de acuerdo al modelo de referencia OSI.

ARDIS especifica las tres primeras capas de la red y proporciona flexibilidad en las capas de aplicación, permitiendo al cliente desarrollar aplicaciones de software, por ejemplo una compañía llamada RF Data, desarrolló una rutina de compresión de datos para utilizarla en estas redes públicas).

Los fabricantes de equipos de cómputo venden periféricos para estas redes (IBM desarrolló su "PCRadio" para utilizarla con ARDIS y otras redes, públicas y privadas).

La PCRadio es un dispositivo manual con un microprocesador 80C186 que corre DOS, un radio/fax/módem incluido y una ranura para una tarjeta de memoria y 640 Kb de RAM.

Estas redes operan en un rango de 800 a 900 Mhz. ARDIS ofrece una velocidad de transmisión de 4.8 Kbps. Motorola Introdujo una versión de red pública en Estados Unidos que opera a 19.2 Kbps; y a 9.6 Kbps en Europa (debido a una banda de frecuencia más angosta).

1.6. VENTAJAS DE LAS REDES INALÁMBRICAS

La informática inalámbrica no sólo ofrece la libertad de permanecer conectado a medida que se moviliza por una oficina o el hogar. Sino que también brinda la libertad de conectar un equipo portátil móvil a la Internet desde cualquier habitación en casa o desde cualquier lugar donde lo lleve.

El deshacerse de los cables puede ser complicado. Implica el tener que enfrentarse a distintos estándares inalámbricos y todo el hardware y software resultante.

No obstante, la industria inalámbrica estableció el estándar 802.11 b (o WLAN) como el predominante en 1999, lo cual ha reducido los precios a medida que la demanda ha aumentado. En un futuro no lejano, el equipo para redes WiFi diseñado para las empresas y los hogares tendrán precios que equivalen a los de las redes cableadas, siendo fáciles de comprar y configurar.

Entre otras ventajas importantes de las redes inalámbricas tenemos:

- Implementación de redes de área loca! inalámbricas en edificios históricos, de difícil acceso y en general en entornos en donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.
- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

- Interconexión de redes que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos.

1.7. ESTÁNDARES INALÁMBRICOS

1.7.1. IEEE 802.11(A), IEEE 802.11(B), IEEE 802.11(G)

Bajo el título de "Redes WLAN", donde WLAN proviene de Wireless Fidelity, agrupamos a un conjunto de redes de área local donde el medio de acceso es inalámbrico. Actualmente, las redes WLAN están basadas en el conjunto de estándares IEEE 802.11 (IEEE: Institute of Electrical and Electronics Engineers).

Definición de los Estándares de la IEEE 802.11

El primer componente del estándar IEEE 802.11 fue ratificado en 1997 y luego en 1999, cuando también se realizaron las primeras extensiones. La estructura de los estándares de la IEEE es tal que las extensiones se elaboran como modificaciones del estándar original y se nombran agregándole una letra al nombre del estándar. En el caso de 802.11, tenemos extensiones 802.11a, 802.11b, etc. En realidad, el estándar 802.11 es sólo una parte de un conjunto más amplio de estándares de IEEE: el 802. La Figura muestra esquemáticamente la estructura del conjunto de estándares 802, dedicado a las capas más bajas de arquitectura de redes.

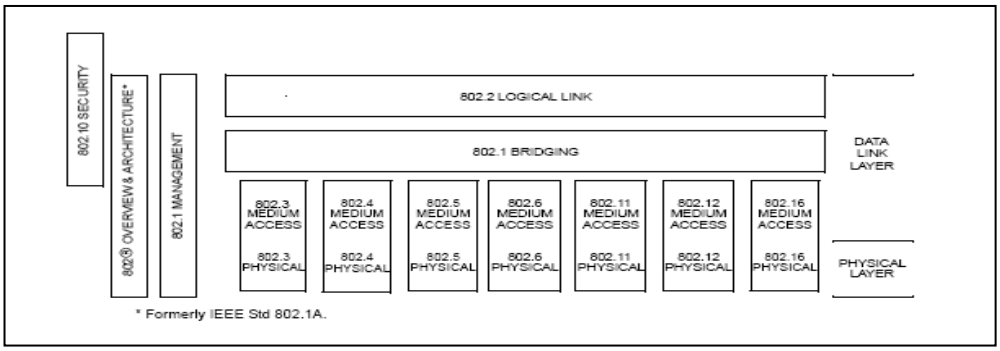


Gráfico 1.6: FAMILIA DE LOS ESTANDARES DE LA IEEE. 802.11

Fuente: http://www.ieee.org

Estándar de la IEEE 802.11 b

Este estándar es una parte de una familia de los estándares para las redes del área local y metropolitana. Esta familia de los estándares con las capas de transmisión de la comprobación y de datos es de acuerdo a lo definido por el modelo de la referencia básica del Sistema Abierto de Interconexión de la Organización Internacional por Estandarización (ISO) (ISO/IEC 7498- 1:1994).

Descripción

Esta cláusula especifica la extensión de la alta tarifa del PHY para el sistema directo del espectro de la extensión de la secuencia (DSSS) (cláusula 15 del IEEE 802.11, en el año 1999, más luego se aplica como la alta tarifa PHY para la banda de 2.4 gigahertz señalada para los usos de ISM. Dicha extensión de las estructuras del sistema de DSSS en las capacidades de la tarifa de datos, según lo descrito en la cláusula 15 de IEEE 802.11, en el año 1999, para proporcionar 5.5 Mbit/s y 11 tarifas de datos de la carga útil de Mbit/s además del 1 Mbps y de 2 tarifas de Mbps.

Para proporcionar las tarifas más altas, el código complementario 8-chip que afina (CCK) se emplea como el esquema de la modulación. La tarifa que salta es 11 megaciclos, que es igual que el sistema de DSSS descrito en la cláusula 15 de IEEE 802.11, del año 1999, así proporcionando la misma anchura de banda ocupada del canal. La nueva capacidad básica descrita en esta cláusula se llama el espectro directo de la extensión de la secuencia de la alta tarifa (hora DSSS). La alta tarifa básica PHY utiliza el mismo preámbulo y el jefe de PLCP que el DSSS PHY, así que PHYs puede coexistir en el mismo BSS y puede utilizar el mecanismo de la conmutación de la tarifa en la manera prevista.

Estándar de la IEEE 802.11 g

IEEE y 802.11g, son marcas de fábrica registradas en los EE.UU. Por el Instituto de Eléctricos y Ingenieros Electrónicos. Cada padrón de IEEE es sujeto a la evaluación por lo menos cada cinco años, para la revisión o la reafirmación. Los documentos de niveles de IEEE son desarrollados dentro de las sociedades de IEEE, y los padrones coordinadas por el comité de Estándar, sus padrones a través de un proceso de consenso, y aprobadas por el Instituto Estadounidense de Estándares Nacionales. La existencia de un padrón de IEEE no insinúa que no hay ninguna otra manera de producir, hacer pruebas, medir, comprar el mercado, o proveer otros bienes y servicios relacionados con el alcance del padrón. Esta enmienda es parte de una familia de padrones para junta local y redes de área metropolitana, en la cual se arregla con el reconocimiento físico, a las capas de enlace de datos. “La organización para interconexión (OSI) modelo de referencia básico de sistemas abiertos de normalización (ISO) (ISO/IEC 7498, los padrones se definen en

algunos tipos de tecnologías de acceso mediano, y son asociados a medios de comunicación físicos, apropiados para las aplicaciones especiales a los objetivos del sistema. Tiene un alcance de un Ancho de banda máximo de hasta 54 Mbps, Opera en el espectro de 2.4 Ghz sin necesidad de licencia, resulta ser compatible con el IEEE 802.11b, su Modulación es DSSS y OFDM".[8]

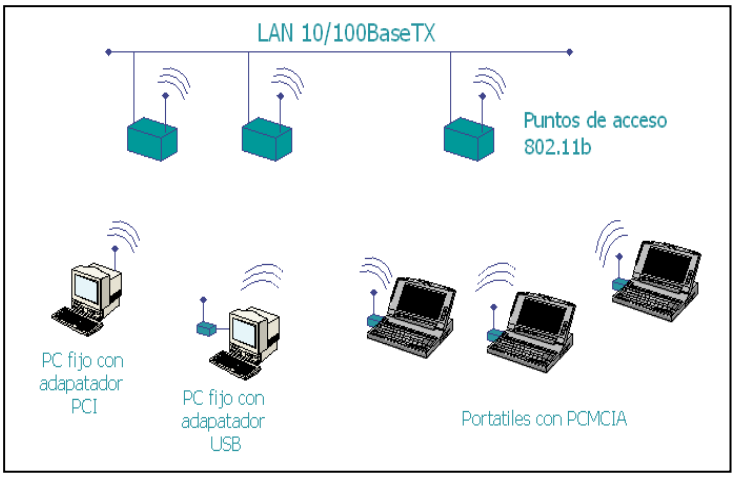


Gráfico 1.13: ESTANDARES DE CALIDAD PARA LAS REDES INALAMBRICAS
Fuente: EL INVESTIGADOR

Estándar de la IEEE 802.11 a

"El IEEE ratificó en julio de 1999 el estándar en 802.11a (los productos comerciales comienzan a aparecer a mediados del 2002), que con una modulación QAM-64 y la codificación OFDM (Orthogonal Frequency Division Multiplexing) alcanza una velocidad de hasta 54 Mbit/s en la banda de 5 GHz, menos congestionada y, por ahora, con menos interferencias, pero con un alcance limitado a 50 metros".[9]

[8] "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ANSI/IEEE Std 802.11, 1999 Edition.
[9] Hills. "Large-Scale Wireless LAN Design". IEEE Communications Magazine, vol. 39, nº 11, noviembre 2001.

Estándar de la IEEE 802.11 d

Constituye un complemento al nivel de control de Acceso al Medio (MAC) en 802.11 para proporcionar el uso, a escala mundial, de las redes WLAN del estándar 802.11. Permitirá a los puntos de acceso comunicar información sobre los canales de radio admisibles con niveles de potencia aceptables para los dispositivos de los usuarios.

Estándar de la IEEE 802.11 e

El objetivo de dicho estándar es la mejora del nivel MAC del 802.11 para el aumento y la gestión de la QoS (Quality of Service), proporcionar una serie de servicios y mejorar el mecanismo de seguridad y autentificación. El objeto es permitir una gestión más eficaz de la banda en presencia de aplicaciones multimedia (voz, imagen y sonido).

1.8. TOPOLOGÍAS Y PROTOCOLOS INALÁMBRICOS

1.8.1. Redes ad-Hoc

Una red "Ad Hoc" consiste en un grupo de ordenadores que se comunican cada uno directamente con los otros a través de las señales de radio sin usar un punto de acceso. Las configuraciones "Ad Hoc" son comunicaciones de tipo de-igual-a-igual. Los ordenadores de la red inalámbrica que quieren comunicarse entre ellos necesitan configurar el mismo canal y ESSID en modo "Ad Hoc". La ventaja de este modo es que se puede levantar una comunicación de forma inmediata entre

ordenadores, aunque su velocidad generalmente no supera los 11Mbps aunque su tarjeta soporte 125Mbps.

¿Qué es el ESSID?

Es un identificador de red inalámbrica. Es algo así como el nombre de la red, pero a nivel WIFI.

1.8.2. Redes de infraestructura

Esta es la forma de trabajar de los puntos de acceso. Si queremos conectar nuestra tarjeta a uno de ellos, debemos configurar nuestra tarjeta en este modo de trabajo. Solo decir que esta forma de funcionamiento es bastante más eficaz que AD-HOC, en las que los paquetes "se lanzan al aire, con la esperanza de que lleguen al destino.", mientras que la Infraestructura gestiona y se encarga de llevar cada paquete a su sitio. Se nota además el incremento de velocidad con respecto a AD HOC.

1.9. INSTALACIÓN Y CONFIGURACIÓN DE ACCESS POINT

1.9.1. Modelos de operación

Hay dos modos de operación, uno ad-hoc, en el que las estaciones se comunican entre sí directamente, y otro de Infraestructura, en el que las estaciones acceden a la red a través de uno o varios puntos de acceso.

El interés suscitado en este campo de las redes inalámbricas ha posibilitado una rápida evolución del estándar inicial y actualmente existen tres extensiones:

- **802.11b** "Higher-Speed Physical Layer Extension in the 2.4 GHz Band".-
  - Estándar predominante de red inalámbrica en redes locales para la empresa y el hogar, así como puntos de conexión públicos.
  - Se ejecuta en tres canales en el espectro de los 2,4 GHz
  - Transfiere datos a velocidades de hasta 11 Mbps en distancias que alcanzan unos 90 metros.

- **802.11a** "High-speed Physical Layer in the 5 GHZ Band".

  - Se ejecuta en 12 canales en el espectro de los 5 GHz
  - Transfiere datos a velocidades de hasta 54 Mbps en distancias que alcanzan unos 15 metros.
  - No es compatible con 802.11 b, por lo que necesitará un nuevo equipo inalámbrico si cambia de estándar
  - Pocos problemas de interferencias

- **802.11g** "Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band".-

  - Se ejecuta en tres canales del espectro de los 2,4GHz (al igual que 802.11 b)
  - Presenta la misma velocidad que 802.11a, pero cuenta con compatibilidad con el estándar 802.11 b
  - Más seguro

Dentro del mercado, el estándar que más aceptación ha tenido es el 802.11b, aunque la velocidad de transmisión máxima (11Mbps) es inferior a la del 802.11a(54Mbps).

La razón es que debido a que se trabaja a una banda de mayor frecuencia (5GHz) el alcance es justo la mitad que en el 802.11b que trabaja en la banda de 2,4GHz. El nuevo estándar 802.11g, que aun está en estudio, trata de llegar a velocidades de transmisión similares al 802.11a, pero en la frecuencia de 2,4GHz.

1.9.2. Punto de Acceso

Un **punto de acceso inalámbrico** (**WAP** o **AP** por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cableada y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". (Por otro lado, una red donde los dispositivos cliente se administran a sí mismos - sin la necesidad de un punto de acceso - se convierte en una red **ad-hoc**).”Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada”.[10]

[10] http://www.pucelawireless.net/index.php?pagename=AccessPoint

Gráfico 1.8: ACCES POINT.
Fuente: HTTP://ES.WIKIPEDIA.ORG/WIKI/PUNTO_DE_ACCESO

1.9.3. Switch inalámbrico

El Switch inalámbrico WS2000 es una poderosa solución integrada que simplifica y reduce los costos de la gestión de redes cableadas e inalámbricas (802.11a/b/g) en sucursales. El dispositivo integra router, puerta de enlace, servidor de seguridad, Power-over-Ethernet (PoE) y otras funciones, se elimina la necesidad de adquirir varios dispositivos y la complejidad de su gestión. La compatibilidad con extensiones Wi-Fi Multimedia (WMM) permite al WS2000 ofrecer el mejor rendimiento incluso en las aplicaciones más complejas con voz y vídeo.

Gráfico 1.15: SWITCH INALÁMBRICO SYMBOL WS2000.
Fuente: HTTP://WWW.ZETES.COM/ELINK/05Q1/SPAIN/WIRELESS-SWITCH.HTM.

1.9.4. Puente inalámbrico

Cuando se tiene varias LAN y se desean interconectar. Este tipo de redes se puede conectar mediante dispositivos llamados **Puentes,** que funcionan en la capa de enlace, que funcionan en la capa de enlace de datos.

Los puentes examinan las direcciones de la capa de enlace de datos para enlutar los datos. Como no tienen que examinar las direcciones de la capa útil de las tramas que enlutan, pueden transportar paquetes IPv4, IPv6 Apple Talk, ATM, OSI o de otros tipos. En contraste, los enrutadores examinan las direcciones de los paquetes y realizan su trabajo de enrutamiento con base en ellas. Aunque está parece una clara división entre puentes y los enrutadores, algunos desarrollos modernos como el surgimiento de la Ethernet conmutada, han enturbiado las aguas.[11]

1.9.5. Puente multi-punto

Un uso común de los puntos es conectar dos o más LAN distantes, Por ejemplo una empresa podría contar con plantas en varias ciudades, cada una con su propia LAN. En un plano ideal todas las LAN deberían estar interconectadas de tal forma que funcionan como una sola LAN grande.

1.9.6. Antenas direccionales

Estas antenas son capaces de enfocar toda la señal que le aplica la tarjeta o punto de acceso, a una dirección concreta en función del modelo y características.

[11] REDES DE COMPUTADORES, TANENBAUM, Andrew, Cuarta Edición. Tomado de la Página 318.

Normalmente estas antenas se usan para establecer enlaces punto a punto (direccional con direccional) o para enlazar con un nodo que tenga una antena Omni direccional.

Dentro de la gama de antenas direccionales, existen también varios modelos y formas, cada una con un uso concreto:

1.9.6.1. Antena Direccional de rejilla, o parabólica.

Esta antena está diseñada para establecer enlaces punto a punto o para conectar a un nodo. Se caracterizan por su alta ganancia, que va desde unos 15dBi hasta los 24dBi. Cuanta más alta es la ganancia de este tipo de antenas, más alta es su direccionalidad, ya que se reduce en gran medida el ángulo en el que irradian la señal, llegando a ser tan estrechos como 8° de apertura.

1.9.6.2. Antena Direccional tipo Patch Panel.

Con estas antenas se consigue crear pequeñas zonas de cobertura, tanto como recintos, estaciones de metro y similares, consiguiendo con varias de ellas establecer 'células' como en telefonía móvil.

Otra utilidad puede darse para sustituir una antena omnidireccional, tras la cual pudiera encontrarse un edificio u otra estructura que impidiera que la señal se propagase, poniendo varias de ellas para cubrir la zona deseada y no

desperdiciar señal. A esta unión de antenas se las llama 'Array'.

Normalmente la anchura del haz que irradian estas antenas es de 25° tanto en vertical como en horizontal.

1.9.6.3. Antenas Omni-Direccionales.

Como su nombre indica, estas antenas son capaces de emitir señal en todas las direcciones, pero esto tiene un pequeño matiz.

La radiación en todas las direcciones, pero esto no es lo que realmente sucede, pues las antenas no emiten señal en todas las direcciones, sino más bien sobre su propio plano pues es aquí en donde se conseguirá la máxima potencia.

Una cosa que pasa de forma bastante habitual, es que se pone la antena en un lugar muy alto, y luego a la altura de la calle no llega la señal pues la antena es omnidireccional sólo sobre su mismo plano.

Con la ganancia de las antenas omnidireccionales pasa algo muy similar a lo que ocurría con las direccionales: cuanto más alta es su ganancia, más estrecha es ia radiación horizontal que estas emiten.

1.10. INSTALACIÓN Y CONFIGURACIÓN DE LAS TARJETAS DE RED

Basándome en la experiencia y los informes presentados por muchos de las personas integrantes del foro gíreles presento esta

tabla que recoge algunas de las características que deben ser tenidas en cuenta a la hora de la elección de las mismas para la auditoria wireless. No se pondrá bajo ningún concepto ningún precio ni ninguna dirección donde poder adquirirlas ya que estos datos cambian constantemente y será estudio particular de cada persona en función de sus necesidades y de su economía.

Modelo	Chipset	Win	Lin	Inyección	Antena	Cobertura	Observaciones
AirisV257 mini-pci 11g	Ralink RT2500	No	Si	Lx (??)	No	Buena	Mini PCI
Belkin F5D7050	Ralink RT2570	No	Si	Lx (b/g)	No	Normal	Barata. USB, R. V3
CiscoAironet PCM352	Aironet	airo	Si	No+??	No	Buena	Necesario act. firmware
D-link DWL-510	RTL8180L	airo	Si	Lx (b/g)	Si	Normal	PCI. R A1. RTL = Realtek
Edimax EW-7128g	Ralink RT2500	No	Si	Lx (b/g)	Si	Normal	PCI
Gygabyte GN_WMAG	Atheros	airo	Si	Lx+??	No	**Muy sorda**	PCMCIA - 108M
Intellinet 54 Wireless	Ralink RT2500	No	Si	Lx (b/g)	Si	**Sorda**	PCI.
IPW 2100 (Portatiles)	Intel Centrino	com	Si	No	No	Muy buena	Mini PCI. Cobertura OK
Linksys WMP54G v2	Broadcom	Si	??	No	No	**Sorda**	Difícil linux-drivers V2
Netgear WG311T (FS)	Atheros A2	**??**	Si	Lx(b/g)	Si	**Sorda**	Sicodelica
Orinco Gold 8470WD	Atheros	airo/com	Si	Lx(b/g)+CV	Si	Normal	Pcmcia. Pigtail MC-Card
Senao2511cdplusext2	Prism 2.5	No	Si	Lx (b)	No	**Sorda**	Pcmcia. Pigtail MMCX
SMC SMCWPCIT-G	Atheros	airo/com	Si	Lx(b/g)+CV	Si	Buena	PCI. Barata

Zcom XI-32HP+300W	Prism 2.5	No	Si	Lx (b)	Si	Normal	Pcmcia. Pigtail MMCX

Tabla 1.1: TABLA DE TARJETAS INALÁMBRICAS (ACTUALIZADO A (3-10-06)
Fuente: HTTP://WWW.SYMBOL.COM.MX/INFO8.HTML

1.11. INTERCONEXIÓN WLAN

Ofrece acceso sin cables a todos los recursos y servicios de una red corporativa (LAN) en un edificio o todo un campus. Proporciona más libertad en el ambiente de trabajo. A través de una red sin cables los trabajadores pueden acceder a la información desde cualquierlugar de la compañía. Lo cual les ofrece numerosas ventajas:

- Acceso fácil y en tiempo real para realizar consultas desde cualquier lugar.
- Acceso mejorado a la base de datos.
- Configuración de red simplificada con mínima implicación MIS.
- Acceso independiente de la localización para administradores de redes.

1.12. VENTAJAS Y DESVENTAJAS

La informática inalámbrica no sólo ofrece la libertad de permanecer conectado a medida que se moviliza por una oficina o el hogar. Sino que también brinda la libertad de conectar un equipo portátil móvil a la Internet desde cualquier habitación en casa o desde cualquier lugar donde lo lleve.

El deshacerse de los cables puede ser complicado. Implica el tener que enfrentarse a distintos estándares inalámbricos y todo el hardware y software resultante.

No obstante, la industria inalámbrica estableció el estándar 802.11 b (o WLAN) como el predominante en 1999, lo cual ha reducido los precios a medida que la demanda ha aumentado. En un futuro no lejano, el equipo para redes WiFi diseñado para las empresas y los hogares tendrán precios que equivalen a los de las redes cableadas, siendo fáciles de comprar y configurar.

Entre otras ventajas importantes de las redes inalámbricas tenemos:

- Implementación de redes de área loca! inalámbricas en edificios históricos, de difícil acceso y en general en entornos en donde la solución cableada es inviable.
- Posibilidad de reconfiguración de la topología de la red sin añadir costos adicionales. Esta solución es muy típica en entornos cambiantes que necesitan una estructura de red flexible que se adapte a estos cambios.
- Redes locales para situaciones de emergencia o congestión de la red cableada.
- Estas redes permiten el acceso a la información mientras el usuario se encuentra en movimiento. Habitualmente esta solución es requerida en hospitales, fábricas, almacenes, etc.
- Generación de grupos de trabajo eventuales y reuniones ad-hoc. En estos casos no valdría la pena instalar una red cableada. Con la solución inalámbrica es viable implementar una red de área local aunque sea para un plazo corto de tiempo.
- En ambientes industriales con severas condiciones ambientales este tipo de redes sirve para interconectar diferentes dispositivos y máquinas.

- Interconexión de redes que se encuentran en lugares físicos distintos. Por ejemplo, se puede utilizar una red local inalámbrica para interconectar dos o más redes de área local cableada situadas en dos edificios distintos.

1.13. INTRODUCCIÓN A LA SEGURIDAD

1.13.1. Seguridad en Wlan

Uno de los problemas más graves a los cuales se enfrenta actualmente la tecnología WLAN es la seguridad. Un muy elevado porcentaje de redes son instaladas por administradores de sistemas y redes por su simplicidad de implementación sin tener en consideración la seguridad y, por tanto, convirtiendo sus redes en redes abiertas, sin proteger la información que por ellas circulan. Existen varias alternativas para garantizar la seguridad de estas redes. Las más comunes son la utilización de protocolos de cifrado de datos para los estándares WLAN como el WEP y el WPA que se encargan de codificar la información transmitida para proteger su confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPSEC (túneles IP) en el caso de las VPN y el conjunto de estándares IEEE 802.1X, que permite la autenticación y autorización de usuarios. Actualmente existe el protocolo de seguridad llamado *WPA2* (estándar 802.11i), que es una mejora relativa a WPA, es el mejor protocolo de seguridad para **WLAN** en este momento.

1.13.1. Dispositivos para WLAN

"Existen varios dispositivos que permiten interconectar elementos WLAN, de forma que puedan interactuar entre si. Entre ellos destacan routers, puntos de acceso, para la emisión de la señal WLAN y para la recepción se utilizan tarjetas para conectar a los PC, ya sean internas, como tarjetas PCI o bien USB (tarjetas de nueva generación que no requieren incluir ningún hardware dentro del ordenador). Los puntos de acceso funcionan a modo de emisor remoto, es decir, en lugares donde la señal WLAN del router no tenga suficiente radio. Los router son los que reciben la señal de la línea que ofrezca el operador de telefonía, se encargan de todos los problemas inherentes a la recepción de la señal, donde se incluye el control de errores y extracción de la información, para que los diferentes niveles de red puedan trabajar. En este caso el router efectúa el reparto de la señal, de forma muy eficiente. Además de routers, hay otros dispositivos que pueden encargarse de la distribución de la señal, como pueden ser hubs y switch".[12]

1.14. AMENAZAS

Los ataques activos buscan causar algún daño, como ser: perdida de confidencialidad, disponibilidad e integridad de información ó sistemas.

1.14.1. IP Spoofing: El atacante cambia su dirección IP para poder pasar por alto controles de acceso.

[12] http://es.wikipedia.org/wiki/Wi-Fi, Tecnologia Wireless Fidelity.

1.14.2. MAC Address Spoofing: El atacante cambia su dirección MAC para pasar por alto los controles de acceso de los Access Points. Como veremos mas adelante, la mayoría de los Access Points posee controles de acceso filtrando direcciones MAC.

1.14.3. ARP Poisoning: Todos los equipos conectados a una red tienen una tabla ARP que asocia direcciones MAC a direcciones IP. Este tipo de ataque busca modificar estas tablas para poder redirigir el tráfico de un equipo a otro de manera controlada.

1.14.4. Man in the middle: Este tipo de ataque se puede ejecutar una vez realizado un ARP Poisoning, en el cual se redirige todo el trafico saliente de un equipo (victima) a otro y este lo envía al destino original. Este tipo de ataque es transparente y la victima no se da cuenta que su trafico de red esta pasando por un tercero antes de llegar a destino.

1.14.5. MAC Flooding: Este ataque se consiste en inundar la red con direcciones IP falsas, causando que el Switch pase a funcionar en modo de Hub, ya que no soporta tanto tráfico.

1.14.6. Denial of Service: Este tipo de ataque busca dejar fuera de servicio a la red inalámbrica, utilizando todo el ancho de banda para enviar paquetes basura. También se utiliza normalmente para dejar fuera de servicio a servidores ó aplicaciones.

1.14.7. Injection: El atacante puede insertar paquetes en la red inalámbrica causando que todos los clientes se desconecten ó inundar la red con paquetes basura (generando un DoS).

1.14.8. Replay: El atacante captura paquetes y luego los reinserta en la red inalámbrica con o sin modificación.

1.14.9. Rouge AP: El atacante pone su propio Access Point y engaña a los clientes pensando que es el Access Point verdadero. De esta forma, posee todo el control del tráfico.

1.15. MÉTODOS PARA IMPLEMENTAR SEGURIDAD DE UNA RED INALÁMBRICA

1.15.1. Encriptación Wep

Se puede habilitar o deshabilitar WEP y especificar una clave de encriptación. Wired Equivalent Privacy (WEP) proporciona transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, supuestamente la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado. Simplemente recordar que este método de seguridad NO ES VÁLIDO si realmente quieres proteger la red de accesos no autorizados. Una clave WEP puede romperse en pocos minutos, sin necesidad de conocimientos avanzados de informática.

1.15.1.1. Encriptación Wep

1. Se calcula un CRC de 32 bits de los datos. Este CRC-32 es el método que propone WEP para garantizar la integridad de los mensajes (ICV, *Integrity Check Value*).
2. Se concatena la clave secreta a continuación del IV formado el *seed*.
3. El PRNG (*Pseudo-Random Number Generator*) de RC4 genera una secuencia de caracteres pseudoaleatorios (*keystream*), a partir del *seed*, de la misma longitud que los bits obtenidos en el punto 1.
4. Se calcula la O exclusiva (XOR) de los caracteres del punto 1 con los del punto 3. El resultado es el mensaje cifrado.
5. Se envía el IV (sin cifrar) y el mensaje cifrado dentro del campo de datos (*frame body*) de la trama IEEE 802.11.

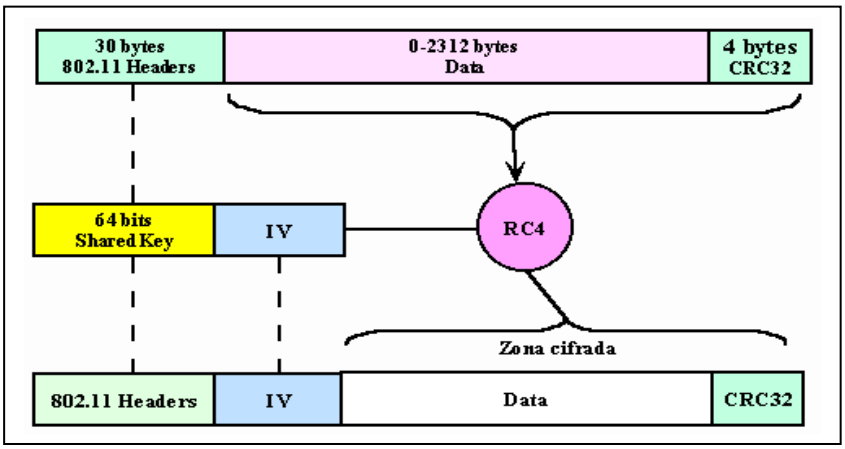


Gráfico 1.16: ALGORITMO DE ENCRIPTACION WEP
Fuente: HTTP://WWW.MONOGRAFIAS.COM/TRABAJOS18/PROTOCOLO-WEP/PROTOCOLO-WEP.

1.16. CRITERIOS Y COMENTARIOS DE VARIOS AUTORES SOBRE REDES INALÁMBRICAS Y SEGURIDADES EN LA MISMA

Según **MOREIRA** (Abril 2002)**,** define **REDES INALAMBRICAS** como: "Una de las tecnologías más prometedoras y discutidas en esta década es la de poder comunicar computadoras mediante tecnología inalámbrica. La conexión de computadoras mediante Ondas de Radio o Luz Infrarroja, actualmente está siendo ampliamente investigada. Las Redes Inalámbricas facilitan la operación en lugares donde la computadora no puede permanecer en un solo lugar, como en almacenes o en oficinas que se encuentren en varios pisos."

De acuerdo a lo expuesto por el autor se considera que, **REDES INALAMBRICAS** es un conjunto de ordenadores que mantiene una estricta relación entre si a través de ondas electromagnéticas, que permitirá mantener una comunicación eficaz entre usuarios; facilitando la operación en lugares donde la computadora no puede permanecer en un solo lugar.

Según **PERKINS** (Marzo 2003), **SEGURIDADES EN LAS REDES INALAMBRICAS** son**:** "Aquellas normas IEEE 802.11 que fueron diseñadas para sustituir a la capa física y MAC de la norma 802.3 (Ethernet), así, la única diferencia entre ambas es la manera en la que los dispositivos acceden a la red, por lo que ambas normas son perfectamente compatibles."

De acuerdo con el autor nosotros creemos que, **SEGURIDADES EN LAS REDES INALAMBRICAS** son normas que permite corregir errores en el flujo de la información que circula a través de la red

permitiendo de esta manera encontrar los errores y corregirlos; por lo tanto se hace necesario la implementación de seguridades en la red inalámbrica para el beneficio de la Fiscalía.

Según **VLADIMIROV** (Octubre 2006), **SEGURIDADES EN LAS REDES INALAMBRICAS** es**:** El motivo de la amplia cobertura de zonas de las redes 802.11 como uno de los motivos para tener presente un constante interés y preocupación por la seguridad, debido a que un atacante puede encontrarse en una zona donde nadie se lo espere encontrárselo y mantenerse suficientemente lejos del área física de la red, y aun estando protegidas con alguna tecnología como es WEP no están suficientemente protegidas por lo cual se recomienda implementar algún otro tipo de tecnología como WPA.

En consecuencia las seguridades en las redes inalámbricas han dejado de ser una utopia, ya que con el avance tecnológico y el aparecimiento de nuevas herramientas y dispositivos inalámbricos con estándares internacionales.

CAPITULO II

2. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

2.1. ENTREVISTAS AL PERSONAL DEL MINISTERIO PÚBLICO COTOPAXI SEDE LATACUNGA

2.1.1. Entrevista al señor Director de Informática del Ministerio Público Quito.

Como parte del desarrollo de la tesis se realizó una entrevista al Dr. Santiago Acurio del Pino en calidad de Jefe de Tecnologías de la Información y las Comunicaciones a nivel Nacional del Ministerio Público, en la cual se abordaron temas de tipo tecnológico y particularmente con la interconexión existente en Quito y el proyecto planteado por Latacunga con el fin de mejorar las actividades que se desarrollan en las distintas oficinas de este importante sector de la Justicia.

Para la Entrevista se planteó como principal objetivo conocer cuáles son las expectativas que se crean en las autoridades del Ministerio Público con la implementación de una Red Inalámbrica la misma que va a contar con seguridades que precautelen la información que en esta dependencia se genera.

El Director de Informática considera que es importante cooperar con el avance tecnológico y más aún si va en beneficio de esta importante dependencia, que se encarga de impartir justicia en nuestro país.

Afirma que a nivel nacional se está capacitando a los profesionales técnicos en lo que es la nueva era tecnológica, para que de esta manera se implemente a corto y mediano plazo proyectos que vayan en beneficio directo de quienes laboran en estas dependencias y que lógicamente sería un gran aporte para que se beneficien las personas o Público en general que visitan los Ministerios a nivel nacional.

Al momento el Departamento de Sistemas de Quito se encuentra probando las nuevas tendencias tecnológicas y esto ha sido de gran aporte para todos los usuarios que utilizan las instalaciones del Ministerio Público.

Manifiesta que se debe tomar en cuenta el principal objetivo el cual es llegar a comunicar permanentemente y con un buen ancho de banda la matriz de Quito y las distintas sedes ubicadas en todas las provincias.

El caso particular de Latacunga, al no contar con una edificación propia, cualquier instante por razones de mejora del servicio o por alguna otra situación se va a trasladar en un lugar diferente, en el caso concreto de cableado estructurado sería una gran pérdida para el Estado en su conjunto, por lo que la presentación de este tema de investigación le pareció muy válida ya que aprovechamos los recursos, no desperdiciamos cable UTP y podemos ofrecer movilidad a nuestros empleados.

Considera que todo lo que vaya con la tecnología siempre va a ser un aporte, pero siempre habrá personas o empleados renuentes al cambio que prefiere lo tradicional y en ocasiones realiza un doble trabajo según ellos por seguridad pero nosotros conocemos que no es así, en este mundo tecnológico se debe estar siempre preparados para lo que venga a nivel de tecnología o caso contrario nos quedaríamos a la vera del camino.

El Ministerio Público siempre y cuando la inversión sea justificada no hay problema alguno, y debemos aprovechar de que el estudio de factibilidad lo está realizando uno de nuestros empleados como parte de un proyecto de grado, que ya significaría un gran ahorro para nuestras dependencias.

Tecnológicamente se encuentra 100% probado que las redes inalámbricas son seguras entonces si hay instituciones como la IEEE que garantiza la integridad de la información se puede asumir que la implementación no causará problema alguno.

2.1.2. Análisis de la entrevista al señor Director de Informática del Ministerio Público Quito

Una vez revisada la entrevista realizada al Dr. En Jurisprudencia Santiago Acurio en calidad de Jefe del Departamento de Sistemas del Ministerio Público del Ecuador podemos concluir que la adopción de una red inalámbrica en el Ministerio Público de Cotopaxi se lo puede realizar sin ningún tipo de problema garantizaríamos la movilidad de los equipos de computo de un lado a otro dentro del edificio donde se encuentre funcionando esta dependencia publica, y otra de las bondades es que cuando se

mueva la dependencia hacia otro edificio no se va a perder la inversión que en ocasiones se realiza como es el cableado estructurado, etc.

La parte económica está cubierta ya que el Departamento nacional cubre la parte de equipos y hardware, la implementación e investigación la estaría cubriendo yo como parte de mi trabajo y la de investigación (Tesis de Grado.), la única debilidad que podríamos encontrar es la posible renuencia al cambio por parte de los empleados del Ministerio.

Esto es cuanto se pudo obtener de parte del Jefe de Sistemas dejándonos en claro que el apoyo de las autoridades es total y es la base fundamental para que el proyecto pueda tener el éxito deseado.

2.1.3. Encuestas al personal del Ministerio Público Cotopaxi sede Latacunga.

Las encuestas se los realizo a una población de 28 personas que labora en el Ministerio Público, las preguntas fueron sugeridas en base a la calidad de servicio que se presta por parte del Departamento de Sistemas en la actualidad y cual podría ser el valor agregado con la adopción de la red inalámbrica. Las preguntas estuvieron dadas para 4 respuestas com se puede observar (ver Anexo 2).´

Primera Pregunta:

¿Considera que el servicio que presta el Departamento de Sistemas es un buen aporte en su labor diaria?

Tabla 2.1: Resultados pregunta 1.

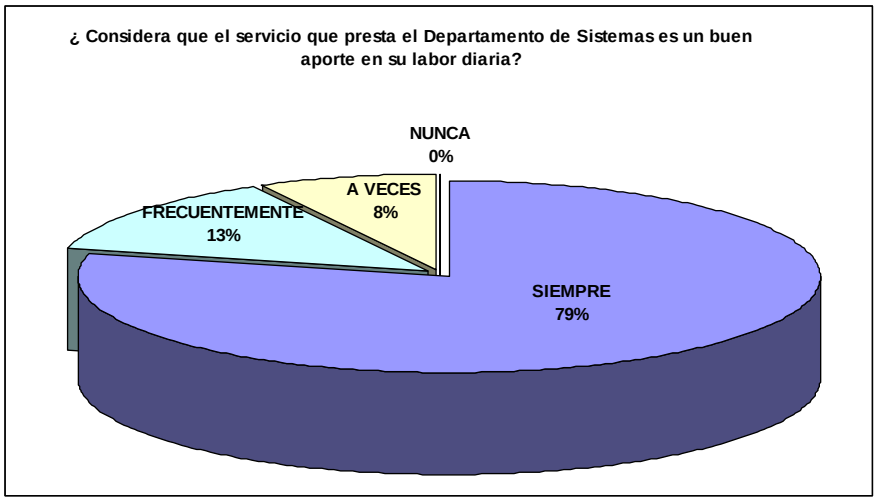
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿ Considera que el servicio que presta el Departamento de Sistemas es un buen aporte en su labor diaria?	30	5	3	0

Gráficamente y en porcentajes los empleados en esta pregunta se pronunciaron:

Grafico 2.1: Resultados pregunta 1.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 1

Como se pudo observar en el grafico 2.1. y dando lectura a los resultados de está pregunta podemos darnos cuenta que en un 79% está satisfecho con la labor que desempeña el Departamento de Sistemas y que las funciones que presta son las adecuadas, y apenas un 13% responde que frecuentemente es buena la labor que desempeñan los sistemas estos dos factores equivales a un claro 92% de satisfacción.

Segunda Pregunta:

¿Dentro del proceso de automatización que está involucrado el Ministerio Público considera que la parte informática debería estar inmiscuida?

Tabla 2.2: Resultados pregunta 2.

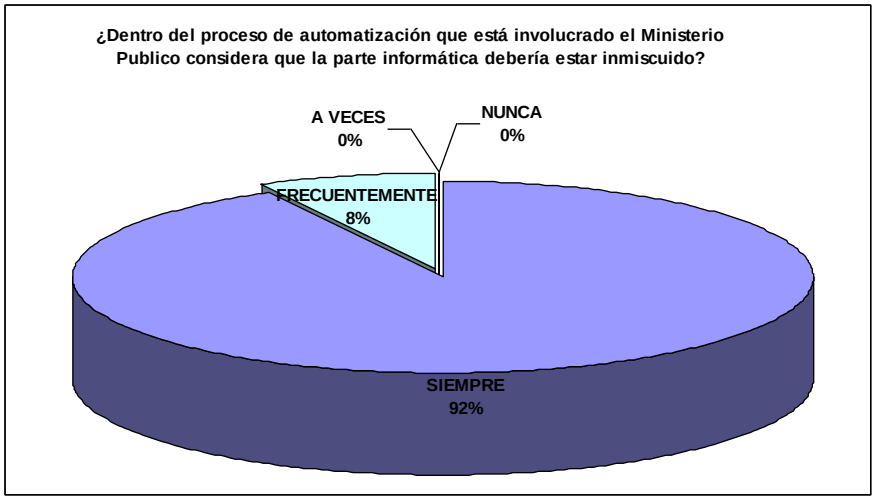
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Dentro del proceso de automatización que está involucrado el Ministerio Publico considera que la parte informática debería estar inmiscuido?	36	3	0	0

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.2: Resultados pregunta 2.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 2

En la pregunta 2 casi en su totalidad coincidió que el Departamento de Sistemas debe estar inmiscuido en todos los procesos de automatización que se lleven a cabo en el Ministerio sea que este directa o indirectamente involucrado.

Tercera Pregunta:

¿La utilización de un computador personal de última generación es de mucho aporte para el desenvolvimiento de sus actividades laborales?

Tabla 2.3: Resultados pregunta 3.

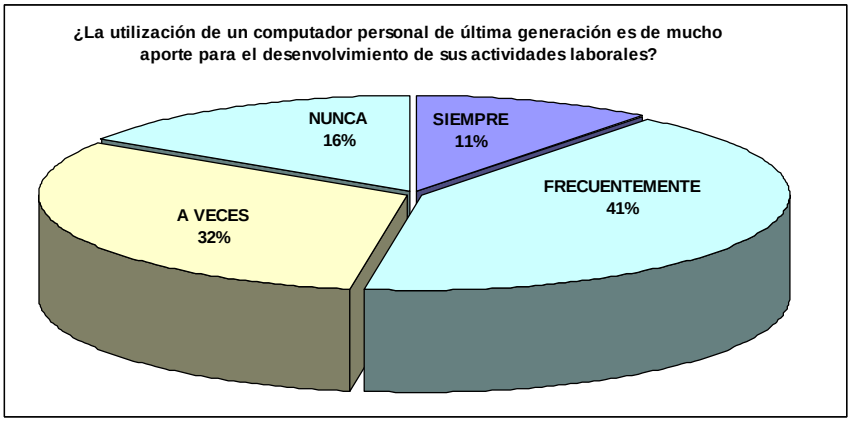
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿La utilización de un computador personal de última generación es de mucho aporte para el desenvolvimiento de sus actividades laborales?	4	16	12	6

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.3: Resultados pregunta 3.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 3

Para la tercera pregunta las actividades que se llevan a cabo en este sitio, se respondió que no es necesario en algunos de los casos ya que lo que mas se necesita que se tenga el Office para sus tareas, en cambio hubo un 11% que dice que todo trabajo debe ir a la par con

la tecnología y que esto se garantiza solamente con un computador de última generación.

Cuarta Pregunta:

¿La movilidad que podría tener con su equipo dentro de las dependencias del Ministerio Público de Cotopaxi, considera que seria un valor agregado al servicio informático de calidad del que recibe?

Tabla 2.4: Resultados pregunta 4.

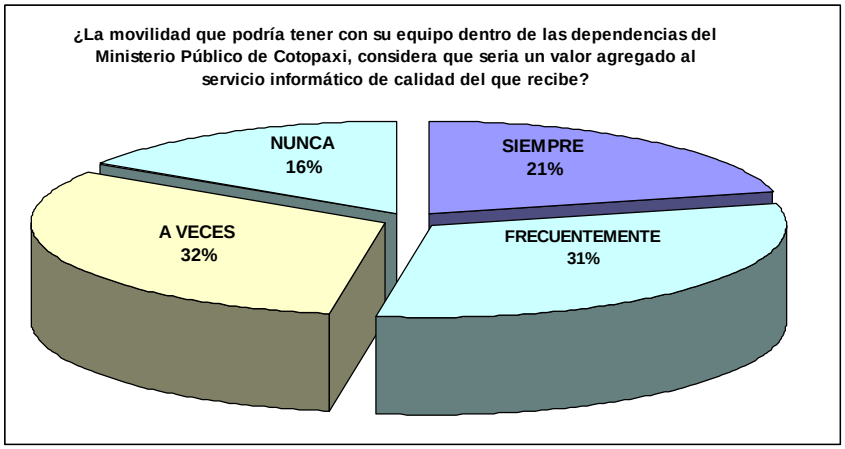
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿La movilidad que podría tener con su equipo dentro de las dependencias del Ministerio Público de Cotopaxi, considera que seria un valor agregado al servicio informático de calidad del que recibe?	8	12	12	6

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.4: Resultados pregunta 4.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 4

En la pregunta 4 consideran en un 21% que la movilidad es muy importante ya que con un computador personal o LAPTOP se puede conectar desde cualquier sitio del edifico donde funciona el Ministerio Público, los que no piensan así es porque para las actividades que realizan la ubicación de los computadores y sus sitios de trabajo son los más adecuados.

Quinta Pregunta:

¿Los comentarios que tiene de las Redes Inalámbricas y las bondades consideran que pueden ser implementadas en el Ministerio y ayudaría a optimizar los múltiples procesos que aquí se desarrollan?

Tabla 2.5: Resultados pregunta 5.

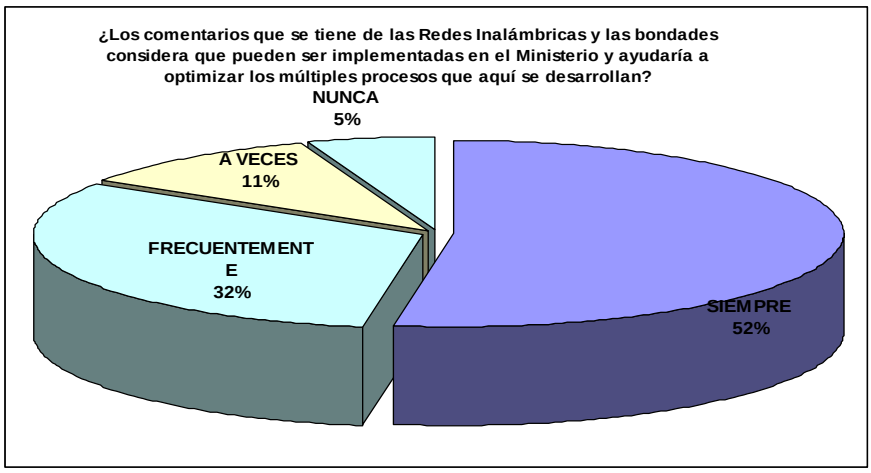
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Los comentarios que se tiene de las Redes Inalámbricas y las bondades considera que pueden ser implementadas en el Ministerio y ayudaría a optimizar los múltiples procesos que aquí se desarrollan?	20	12	4	2

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.5: Resultados pregunta 5.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 5

La quinta pregunta una vez partiendo de la parte de la movilidad pensó diferente y sostienen que la tecnología es importante y el estar a la par es muy importante ya que de esta manera se puede estar actualizado.

Sexta Pregunta:

¿Le preocupa a usted que pueda ser blanco de un ataque informático a través de la red inalámbrica?

Tabla 2.6: Resultados pregunta 6.

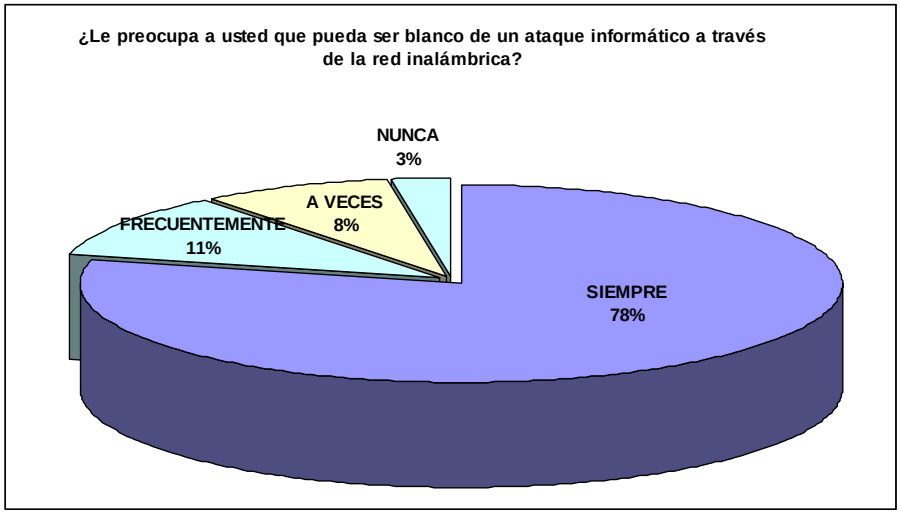
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Le preocupa a usted que pueda ser blanco de un ataque informático a través de la red inalámbrica?	30	4	3	1

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.6: Resultados pregunta 6.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 6

La pregunta 6 en un alto porcentaje considera que si puede sufrir alteración la información que maneja es preferible no poptar por está alternativa ya que manifiestan que aquí hay mucha información importante y no debe ser ventilada fuera de la oficina y peor aun si caería en manos que no debería.

Séptima Pregunta:

¿Con la implementación de las Redes Inalámbricas usted estaría preparada para poder adoptar está tecnología y los problemas que conlleva?

Tabla 2.7: Resultados pregunta 7.

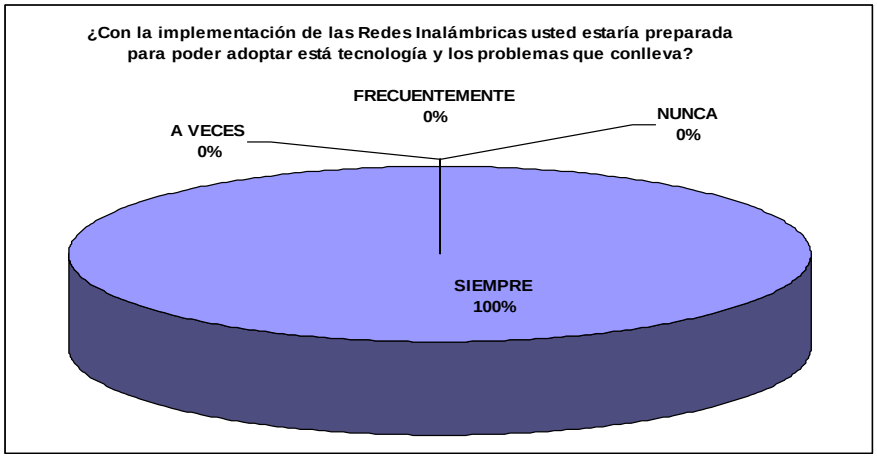
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Con la implementación de las Redes Inalámbricas usted estaría preparada para poder adoptar está tecnología y los problemas que conlleva?	38	0	0	0

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.7: Resultados pregunta 7.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 7.

La pregunta 7, aquí todos los encuestados coinciden que con una capacitación previa, con el compromiso de que no se pueda alterar ni perder la información los usuarios pueden adaptarse a los cambios que eso implica, hay que destacar que todos están dispuestos a colaborar con el avance de la tecnología y más aun si esto beneficia al sitio de trabajo que tienen.

Octava Pregunta:

¿Considera que la capacitación con está nueva tecnología es necesaria?

Tabla 2.8: Resultados pregunta 8.

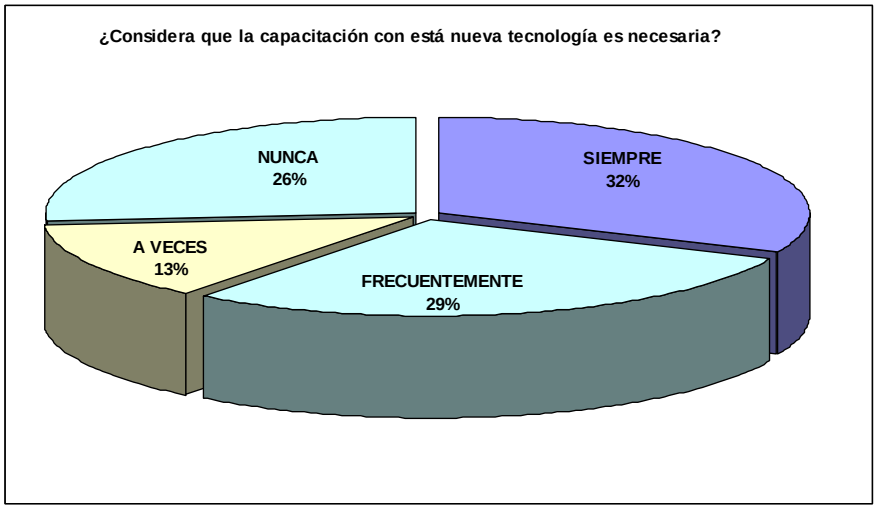
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Considera que la capacitación con está nueva tecnología es necesaria?	12	11	5	10

Gráficamente y en porcentajes los empleados en esta pregunta se pronunciaron:

Grafico 2.8: Resultados pregunta 8.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 8.

En esta última pregunta tenemos importantes porcentajes que no necesitan de capacitación ya que en alguna otra parte han recibido o conocen del funcionamiento, claro que como en todo existen personas que también necesitan de está capacitación para poder realizar su trabajo de buena manera.

2.1.4. Encuestas después de la Implementación de la conectividad y las seguridades de la Red Inalámbrica en el Ministerio Público

Al igual que las primeras encuestas realizadas, la población total encuestada es de 38 personas las mismas que emitieron lo siguiente:

Primera Pregunta:

¿Con las implementaciones realizadas mejoro el servicio que presta el Departamento de Sistemas y ahora realiza un mejor aporte en su labor diaria?

Tabla 2.9: Resultados pregunta 1.

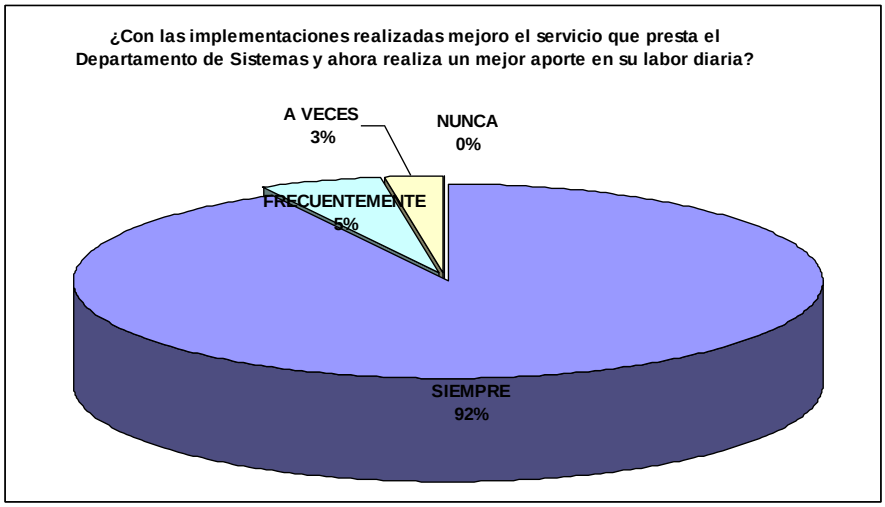
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Con las implementaciones realizadas mejoro el servicio que presta el Departamento de Sistemas y ahora realiza un mejor aporte en su labor diaria?	35	2	1	0

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.1: Resultados pregunta 1.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 1

Como se pudo observar en el grafico 2.9, en los resultados de está pregunta podemos darnos cuenta que los empleados del Ministerio están concientes de que los cambios han mejorado la atención que

presta el Departamento de Sistemas y que esto ha mejorado el desempeño de las funciones de todos.

Segunda Pregunta:

¿Con estas automatizaciones, que se han realizado en el Ministerio Publico considera que la parte informática garantiza un mejor desempeño de sus actividades?

Tabla 2.10: Resultados pregunta 1.

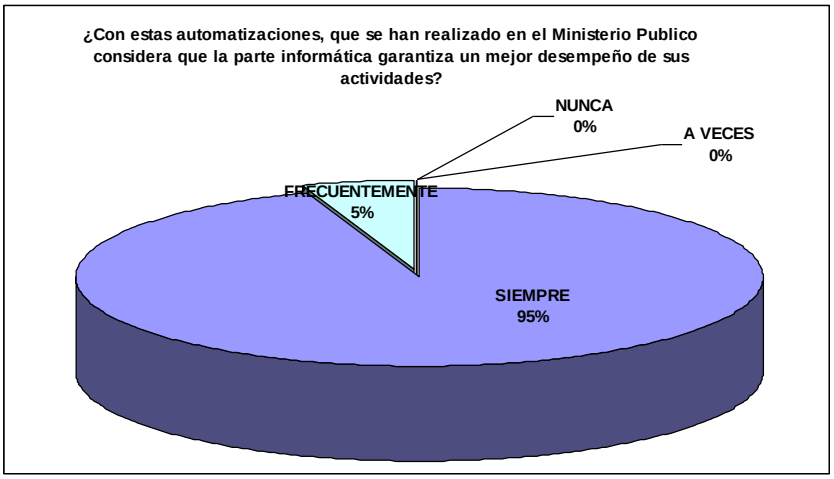
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Con estas automatizaciones, que se han realizado en el Ministerio Publico considera que la parte informática garantiza un mejor desempeño de sus actividades?	36	2	0	0

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.10: Resultados pregunta 1.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 2

Los resultados obtenidos en está pregunta nos damos cuenta que todo tipo de actualización siempre va a mejorar actividades de quienes las realizan y sobre todo mejoro en un alto porcentaje la visión que tenían del Departamento de Sistemas.

Tercera Pregunta:

¿La utilización de un computador personal de última generación es de mucho aporte para el desenvolvimiento de sus actividades laborales con esta nueva tecnología?

Tabla 2.11: Resultados pregunta 1.

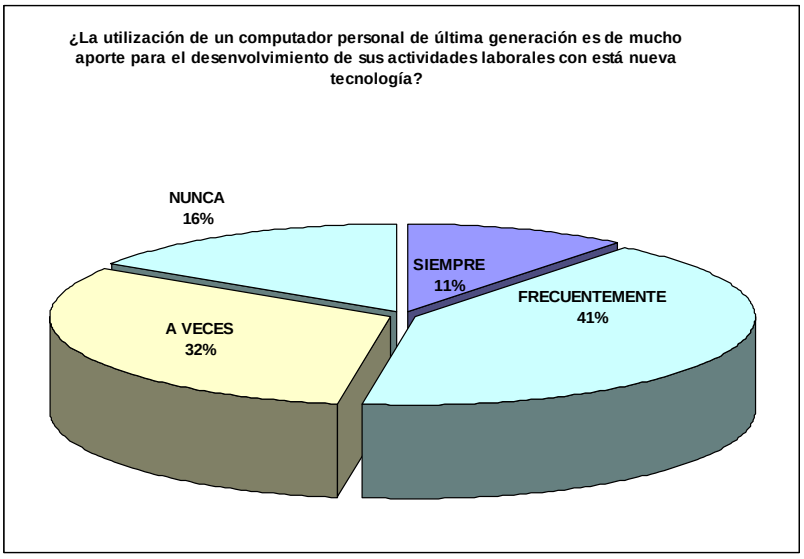
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿La utilización de un computador personal de última generación es de mucho aporte para el desenvolvimiento de sus actividades laborales con está nueva tecnología?	4	16	12	6

Gráficamente y en porcentajes los empleados en esta pregunta se pronunciaron:

Grafico 2.11: Resultados pregunta 3.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 3

Un 41% considera que se necesita de un computador de última generación para poder estar acorde con la tecnología y las actividades que desempeña, pero un 18% de igual manera no está de acuerdo que esto pueda influir en sus actividades diarias.

Cuarta Pregunta:

¿La movilidad que ahora tiene dentro de las dependencias del Ministerio Público de Cotopaxi, considera que es un valor agregado al servicio informático de calidad del que recibe?

Tabla 2.12: Resultados pregunta 4.

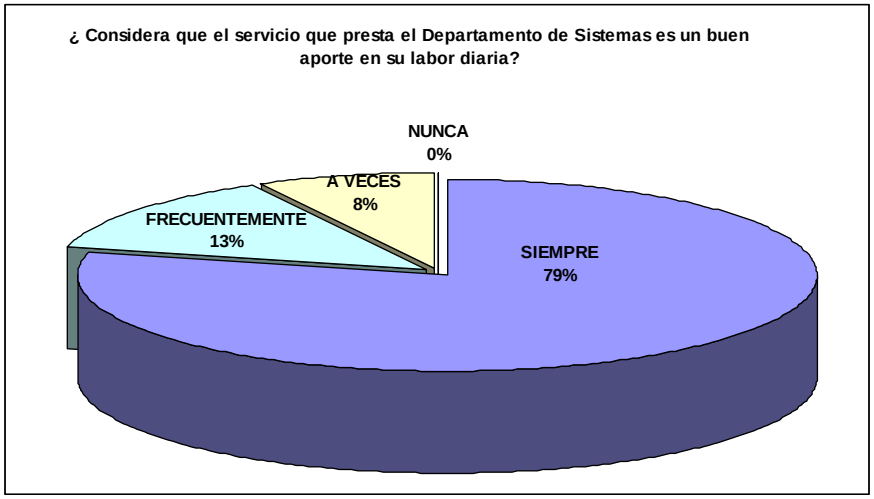
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿La movilidad que ahora tiene dentro de las dependencias del Ministerio Público de Cotopaxi, considera que es un valor agregado al servicio informático de calidad del que recibe?	14	12	6	6

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.12: Resultados pregunta 4.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 4

Un alto porcentaje de los usuarios de computadores y puntos de red Móvil considera que con las implementaciones son un gran aporte para todas las actividades de los empleados.

Quinta Pregunta:

¿Las Redes Inalámbricas y sus bondades consideran que pueden ser implementadas en otras dependencias o en su lugar de estudio u hogar y ayudaría en sus actividades diarias?

Tabla 2.13: Resultados pregunta 5.

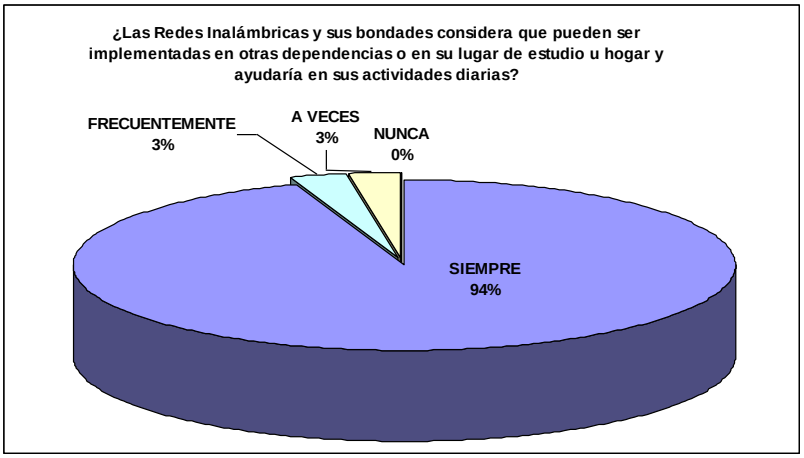
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Las Redes Inalámbricas y sus bondades considera que pueden ser implementadas en otras dependencias o en su lugar de estudio u hogar y ayudaría en sus actividades diarias?	36	1	1	0

Gráficamente y en porcentajes los empleados en esta pregunta se pronunciaron:

Grafico 2.13: Resultados pregunta 5.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 5

Todos quisieran tener en casa lo que disponen en la oficina y consideran que sería beneficioso que se adoptaran en otros sitios donde pueden restar servicios profesionales.

Sexta Pregunta:

¿Se siente tranquila una vez que se han realizado todo tipo de pruebas en las redes inalámbricas y que no han sido víctimas de ataque alguno?

Tabla 2.14: Resultados pregunta 6.

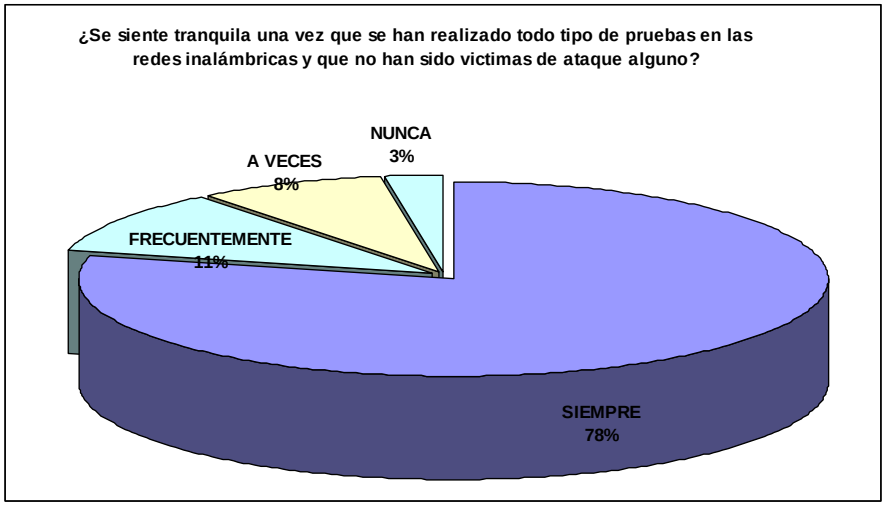
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Se siente tranquila una vez que se han realizado todo tipo de pruebas en las redes inalámbricas y que no han sido victimas de ataque alguno?	30	4	3	1

Gráficamente y en porcentajes los empleados en está pregunta se pronunciaron:

Grafico 2.14: Resultados pregunta 6.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 6

En algunos casos están conformes con las pruebas realizadas mientras que otras personas poco interés le ponen al asunto de la seguridad ya que manifiestan no tener actividades que puedan ser alterada o robadas.

Séptima Pregunta:

¿Con la implementación de las Redes Inalámbricas usted está preparada ya para ir a la par con la tecnología?

Tabla 2.15: Resultados pregunta 7.

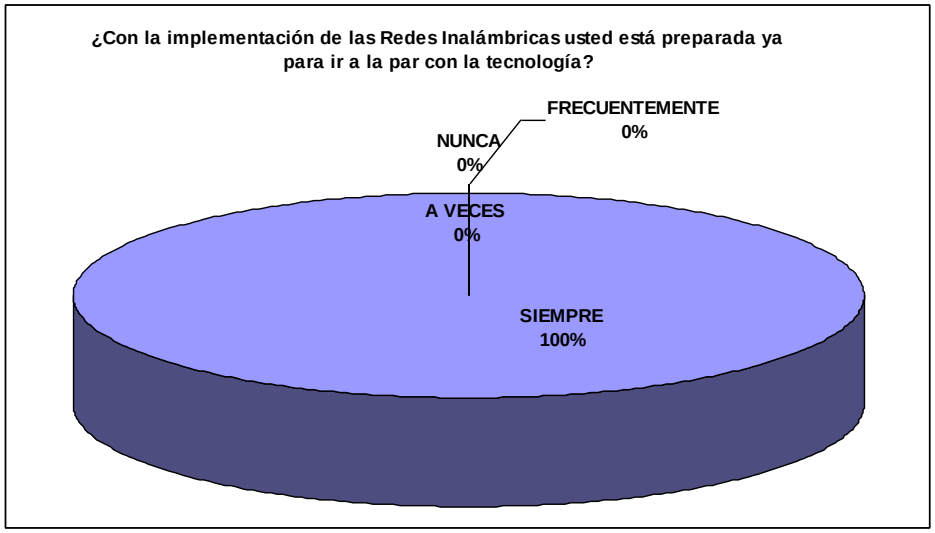
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Con la implementación de las Redes Inalámbricas usted está preparada ya para ir a la par con la tecnología?	38	0	0	0

Gráficamente y en porcentajes los empleados en esta pregunta se pronunciaron:

Grafico 2.15: Resultados pregunta 7.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 7

Las preguntas planteadas en esta encuesta son el resultado de la primera es así que en su totalidad los usuarios están capacitados para ir a la par con la tecnología.

Octava Pregunta:

¿Considera que falta aun más capacitación?

Tabla 2.16: Resultados pregunta 8.

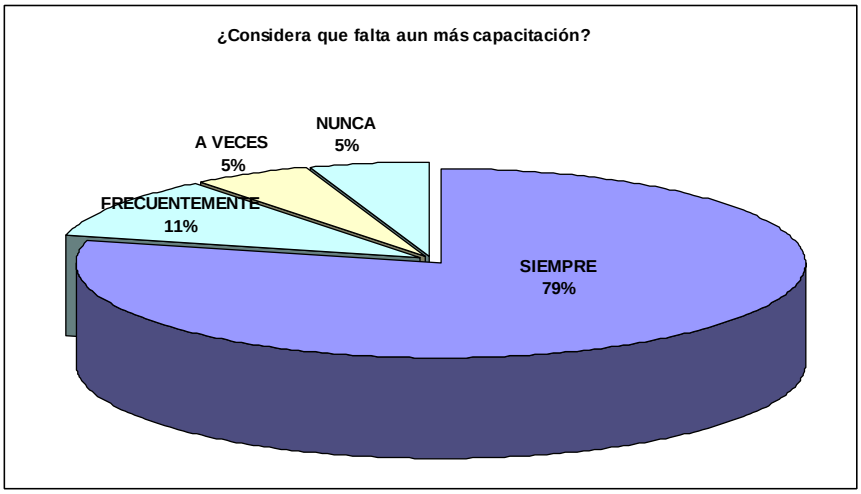
Fuente: El Investigador

PREGUNTA	SIEMPRE	FRECUENTEMENTE	A VECES	NUNCA
¿Considera que falta aun más capacitación?	30	4	2	2

Gráficamente y en porcentajes los empleados en esta pregunta se pronunciaron:

Grafico 2.16: Resultados pregunta 8.

Fuente: El Investigador



Análisis de la respuesta a la pregunta 8

En la última pregunta un alto porcentaje está consciente que necesita de más capacitación aduciendo que nunca es suficiente, por otro lado las capacitaciones se las hace en horarios fuera de oficina y no están de acuerdo ya que interfiere en sus actividades personales y/o profesionales.

2.1.5. Comprobación de la Hipótesis.

En el plan de tesis se planteó como hipótesis:

La implementación de la conectividad y seguridad para el enlace entre los usuarios que conforman el **Ministerio Público Cotopaxi sede Latacunga** garantizará que la información sea confiable y confidencial en tiempo real.

Viendo las limitaciones que tenía el Ministerio Público de Cotopaxi se planteo está investigación la misma que iba encaminada a mejorar el desempeño profesional de las personas que en esta dependencia trabaja al implantar una red inalámbrica y por

supuesto brindar las respectivas seguridades a la información y a los tramites que aquí se desarrollan.

Al tratarse de esta Nobel tecnología todos queremos adentrarnos pero pocos lo han conseguido con éxito, esto con respecto a la resistencia que se encuentra de parte de los empleados a querer adaptarse a nuevos procesos y a las capacitaciones que en ocasiones han causado malestar.

En nuestro caso se lo pudo realizar sin novedad alguna ya que la orden se la envío directamente de Quito y todos teníamos que sujetarnos a la nueva disciplina, el trabajo de parte del Departamento de Sistemas fue arduo y se conseguían uno a uno los objetivos planteados es así que ahora podemos gozar de esta tecnología y todos trabajan como si no hubiera pasado está actualización y sobre todo que los cambios hechos aquí han mejorado la manera de ver el trabajo que realiza el Departamento.

CAPITULO III

3. IMPLEMENTACIÓN DE LA CONECTIVIDAD Y SEGURIDAD DE LA RED INALÁMBRICA DEL MINISTERIO PÚBLICO DE COTOPAXI SEDE LATACUNGA

3.1. Análisis

Para poder realizar un análisis completo de la implementación de la red inalámbrica dentro del Ministerio Público de Cotopaxi tenemos que tener en cuenta algunos conceptos que vana a ser repetidos durante la fase de análisis e implementación, esto son:

3.1.1. Mecanismo de acceso

Hay de dos tipos:

Protocolos con arbitraje (FDMA - Frequency División Múltiple Access, TDMA - Time División Múltiple Access)

Protocolos de contienda (CDMA/CA - Carrier-Sense, Múltiple Access, Colusión Avoidance), COMA (Code División, Múltiple Access) y el CDMA/CD (detección de colisión).

3.1.1.1. Protocolos con arbitraje

La multiplexación en frecuencia (FDM) divide todo el ancho de banda asignado en distintos canales individuales.

Es un mecanismo simple que permite el acceso inmediato al canal, pero muy ineficiente para utilizarse en sistemas informáticos, los cuales presentan un comportamiento típico de transmisión de información por breves períodos de tiempo (ráfagas).

Una alternativa a este sería asignar todo el ancho de banda disponible a cada nodo en la red durante un breve intervalo de tiempo de manera cíclica. Este mecanismo, se llama multiplexación en el tiempo (TDM) y requiere mecanismos muy precisos de sincronización entre los nodos participantes para evitar interferencias. Este esquema ha sido utilizado con cierto éxito sobre todo en las redes inalámbricas basadas en infraestructura, donde el punto de acceso puede realizar las funciones de coordinación entre los nodos remotos.

3.1.1.2. Protocolos de acceso por contienda

Tienen similitudes al de Ethernet cableada de línea normal 802.3:

3.1.1.2.1. CSMA

(Code-division múltiple access = Acceso múltiple por división de tiempo).

Se aplica específicamente a los sistemas de radio de banda esparcida basados en una secuencia. En este esquema se asigna una secuencia distinta a cada nodo, y todos los nodos pueden conocer el conjunto completo de secuencias pertenecientes a los demás nodos.

Para comunicarse con otro nodo, el transmisor solo tiene que utilizar la secuencia del destinatario. De esta forma se pueden tener múltiples comunicaciones entre diferentes pares de nodos.

3.1.1.2.2. CSMA/CD

(Carrier Sense, Múltiple Access, Colusión Detection)

En medios de transmisión tales como radio e infrarrojos, no es posible transmitir y recibir al mismo tiempo, la detección de errores no funciona en la forma básica que fue expuesta para las LAN alambradas. Se diseñó una variación denominada detección de colisiones (peine) para redes inalámbricas.

En este esquema, cuando un nodo tiene una trama que transmitir, lo primero que hace es generar una secuencia binaria pseudoaleatoria corta, llamada peine la cual se añade al preámbulo de la trama.

A continuación, el nodo realiza la detección de la portadora si el canal está ubre transmite la secuencia del peine. Por cada "1" del peine el nodo transmite una señal durante un intervalo de tiempo corto. Para cada "O" del peine, el nodo cambia a modo de recepción. Si un nodo detecta una señal durante el modo de recepción deja de competir por el canal y

espera hasta que los otros nodos hayan transmitido su trama.

La eficiencia del esquema depende del número de bits de la secuencia del peine ya que si dos nodos generan la misma secuencia, se producirá una colisión.

3.1.1.2.3. CSMA/CA

(Carrier-Sense, Múltiple Access, Colusión Avoidance)

Es el más utilizado, este protocolo evita colisiones en lugar de descubrirlas.

En una red inalámbrica es difícil descubrir colisiones. Es por ello que se utiliza el CSMA/CA y no el CSMA/CD debido a que entre el final y el principio de una transmisión suelen provocarse colisiones.

En CSMA/CA, cuando una estación identifica el fin de una transmisión espera un tiempo aleatorio antes de transmitir su información, disminuyendo así la posibilidad de colisiones.

La capa MAC opera junto con la capa física probando la energía sobre el medio de transmisión de datos. La capa física utiliza un algoritmo de estimación de desocupación de canales (CCA) para determinar si el canal está vacío. Esto se cumple

midiendo la energía de la antena y determinando la fuerza de la señal recibida. Esta señal medida es normalmente conocida como RSSI.

Si la fuerza de la señal recibida está por debajo de un umbral especificado, el canal se considera vacío, y a la capa MAC se le da el estado del canal vacío para la transmisión de los datos. Si la energía RF está por debajo del umbral, las transmisiones de los datos son retrasadas de acuerdo con las reglas protocolares.

El Standard proporciona otra opción CCA que puede estar sola o con la medida RSSI. El sentido de la portadora puede usarse para determinar si el canal está disponible.
Esta técnica es más selectiva ya que verifica que la señal es del mismo tipo de portadora que los transmisores del 802. 11.

En comunicaciones inalámbricas, este modelo presenta todavía una deficiencia debida al problema conocido como de la terminal oculta (o nodo escondido).

3.1.2. Seguridad

En el estándar se dirigen suministros de seguridad como una característica optativa para aquellos afectados por la escucha secreta, es decir, por el "fisgoneo". Incluye dos aspectos básicos: autentificación y privacidad.

La seguridad de los datos se realiza por una compleja técnica de codificación, conocida como WEP (Wired Equivalent Privacy Algorithm).

WEP se basa en proteger los datos transmitidos en el medio RF, usando clave de 64 bits y el algoritmo de encriptación RC4 (desarrollado por RSA Security Inc.). La clave se configura en el punto de acceso y en sus estaciones (clientes wireless), de forma que sólo aquellos dispositivos con una clave válida puedan estar asociados a un determinado punto de acceso.

WEP, cuando se habilita, sólo protege la información del paquete de datos y no protege el encabezamiento de la capa física para que otras estaciones en la red puedan escuchar el control de datos necesario para manejar la red. Sin embargo, las otras estaciones no pueden distinguir las partes de datos del paquete.

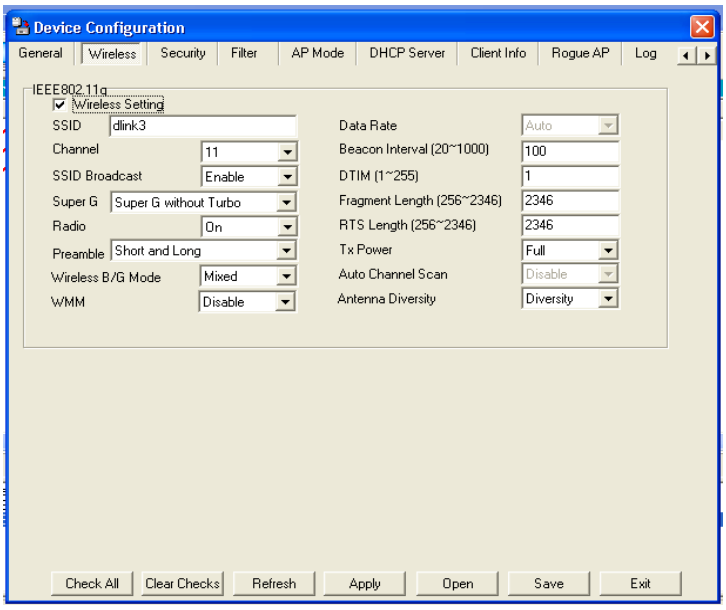
Se utiliza la misma clave de autentificación para encriptar y desencriptar los datos, de forma que solo las estaciones autorizadas puedan traducir correctamente los datos.

En el Ministerio Público se consideran 2 aspectos de seguridad a más del antes ya mencionado como lo es WEP, además tenemos las configuraciones propias del Acive Directory de Windows 2003, y el filtro por direcciones MAC de las tarjetas de red inalámbricas instaladas en las computadoras del Ministerio esto con el fin de prevenir posibles ataques a los casos que en las diferentes dependencias de tratar.

Todo esto se encuentra mejor explicado en la parte inferior de forma Gráfica.

Gráfico 3.1: Pantalla de configuración de Contraseñas en el AP

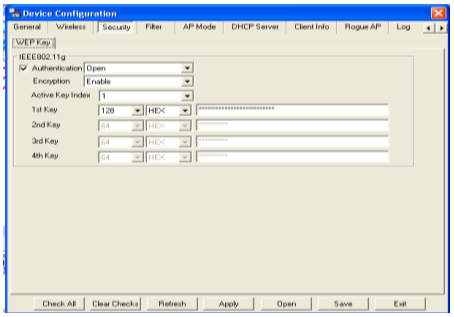
Fuente: El investigador



En la gráfica superior se muestra la pantalla de la configuración: SSID(**ESSID (Extended Service Set Identifier):** Nombre único de hasta 32 caracteres para identificar a la red wireless. Todos los componentes de la misma red WLAN deben usar el mismo), Channel(Canal: Una porción del espectro de radiofrecuencias que usan los dispositivos para comunicarse. El uso de diferentes canales ayuda a reducir interferencias canal de uso por defecto viene 6), SSID Broadcast (activar o desactivar el nombre la red), SuperG (Para transferencia de 108 mbps).

Gráfico 3.2: Pantalla de configuración de WEP

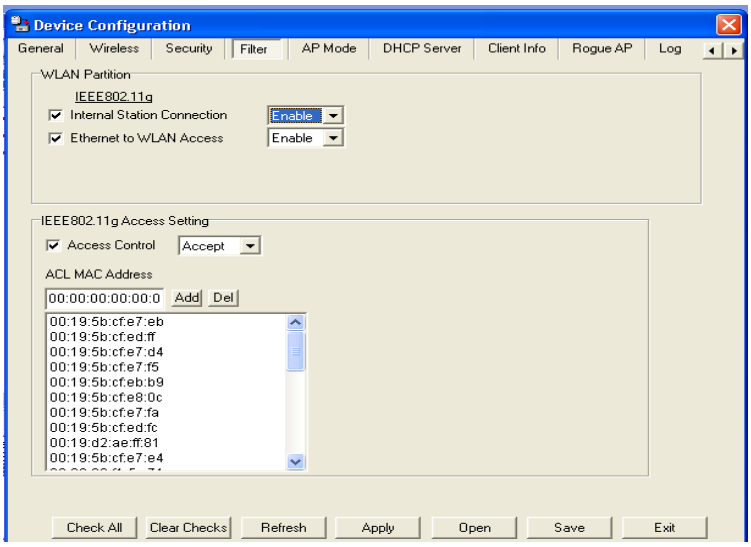
Fuente: El investigador



En la pantalla superior la filtración de claves WEP para los usuarios de la red inalámbrica en Hexadecimal o ASCII, y como se puede observar el estándar utilizado en este proyecto es el 802.11g que es el estándar que mas seguridades proporciona en la actualidad.

Gráfico 3.3: Pantalla de configuración de Filtración MAC.

Fuente: El investigador



En la gráfica superior se puede observar la tercera alternativa de encriptación el filtrar las macs de los equipos de la red de cada uno de los usuarios del Ministerio Público de Cotopaxi.

3.1.3. Funcionalidad adicional

En las LAN inalámbricas la capa de MAC, además de efectuar la función de controlar el acceso al medio, desempeña otras funciones;

Fragmentación

Control de flujo

Manejo de múltiples tasas de transmisión
Gestión de potencia

En los diferentes tipos de LAN por cable es posible usar tramas grandes gracias a errores de bit bajos. En las LAN inalámbricas, el multicamino y las interferencias pueden elevar considerablemente los valores de errores de bit.
Para poder transmitir eficientemente por estos medios, hay que reducir el tamaño de las tramas. La capa MAC se encarga de fragmentar las tramas en otras más pequeñas antes de transmitirlas por el medio inalámbrico.

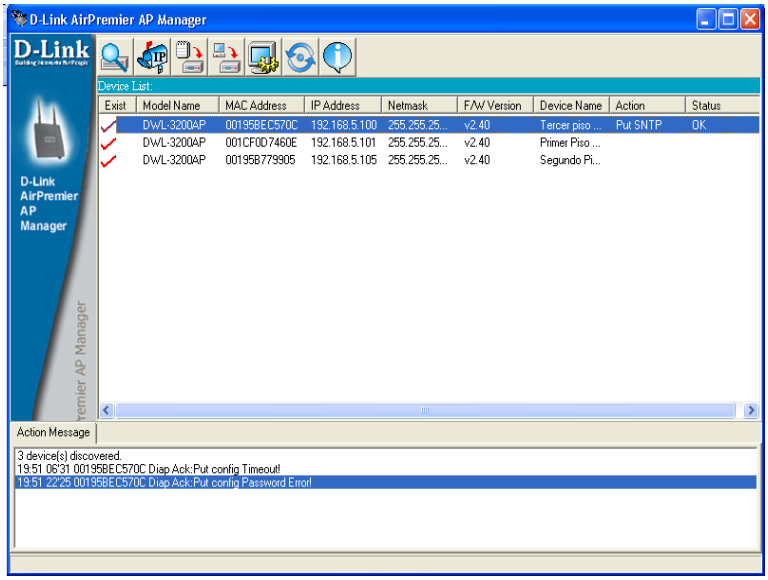
De la misma manera deberá ensamblar las tramas para obtener la trama original antes de entregarla a la capa superior.

También debe cumplir un control de flujo, cada vez que un segmento sea pasado a la capa física, deberá esperar que este sea transmitido antes de enviar el próximo segmento.

La gestión de la potencia se apoya en el nivel MAC para esas aplicaciones que requieren movilidad bajo el funcionamiento de la pila. Se hacen provisiones en el protocolo para que las estaciones portátiles pasen a "modo dormido" durante un intervalo de tiempo definido por la estación base.

Gráfico 3.4: Pantalla de Detección de los AP.

Fuente: El investigador



En la parte superior observamos un gráfico de la configuración de los Access Point mediante las direcciones MAC(Funcionalidad), esto con el fin de ver las replicas que tiene.

3.1.4. Pasos básicos para asegurar una WLAN

El propósito de asegurar correctamente un punto de acceso(AP) es cortar el paso desde el exterior a nuestra red a personas que no tienen el permiso de entrar, es decir asegurar que la información fluya internamente.

Una red wireless es por definición más difícil de proteger que una red

convencional o cableada entre otras cosas porque el medio es el aire y así como en una LAN tenemos unas tomas de red determinadas y controladas, en principio, en una WLAN se puede acceder desde cualquier punto que permita la antena.

A pesar de esto siempre se pueden establecer una serie de medidas básicas pero efectivas no en el 100% de los casos pero se impide el acceso a la gran mayoría de los intrusos.

Para establecer este nivel básico de seguridad se debe realizar los siguientes pasos:

3.1.4.1. Colocación de la antena

El primer paso para cerrar el acceso no autorizado a un punto de acceso es colocar la antena de éste, de manera que limite el alcance de la antena al área de trabajo.

Nunca hay que colocar una antena cerca de una ventana ya que el cristal no bloquea la señal. Un esquema ideal sería colocar la antena en el centro del área dejando que solo una leve señal escape a través de los muros o ventanas de la oficina o lugar de trabajo. Si es imposible controlar este factor todavía se pueden tomar otras medidas de seguridad adicionales.

Gráfico 3.5: Ubicación de los Access Point.

Fuente: El investigador

De acuerdo al número de usuarios en una oficina y como está se encuentre distribuida están ubicados los AP, cuando las oficinas no son muy grandes se procedió a colocar sobre las ventanas interiores del edificio para aprovechar el espacio de cobertura y que pueda abastecer las dos oficinas, como se muestra en la grafica siguiente:

Gráfico 3.6: Ubicación de los Access Point.

Fuente: El investigador

Gráfico 3.7: Ubicación de los Access Point.

Fuente: El investigador

Arquitectónicamente el edificio del Ministerio Público cuenta con 3 plantas en las cuales hemos distribuido de forma adecuada los Access Point para tratar de cubrir un amplio radio, y de está manera satisfacer las necesidades tecnológicas de los usuarios de la red inalámbrica.

3.1.4.2. Usar seguridad

La seguridad es el problema más importante al que se enfrenta actualmente la tecnología WiFi, ya que si no se utilizan los medios adecuados acceder a una red WiFi protegida puede resultar relativamente sencillo.

Un gran número de redes inalámbricas son instaladas por administradores de redes y sistemas sin tener en cuenta políticas de seguridad. Lo que se traduce en una red abierta que no protege la información que circula por ella.

Al diseñar una red WiFi es necesario combinar dos tipos de seguridades:

- Físicas.
- Lógicas, que son las que ya se encuentran detalladas en un ítem anterior.

Las seguridades Físicas están dadas por las bondades que nos puede ofrecer la edificación, ya que al ser funcional como es nuestro caso el Departamento de Sistemas cuenta con un plan de contingencia el mismo que va desde posibles desastres hasta invasión de un hacker.

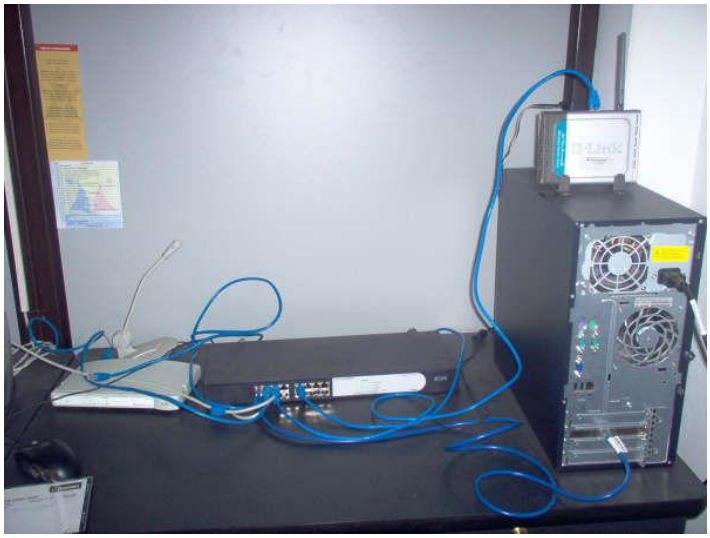
Al hablar de hackers no debemos dejar de lado que el ataque puede ser interno por lo que se tomo la decisión de que solo un cable conecte al primer AP, este a su vez vía inalámbrica conecte al segundo piso y este replique su señal hacia un piso más abajo, de está manera estaríamos cubriendo toda la edificación como se puede observar en los planos del edificio en el anexo 3.

Gráfico 3.8: Ubicación de los Access Point.
Fuente: El investigador

En la grafica anterior se encuentra el Access Point que hace de base para las comunicaciones con los otros AP's, es decir viene siendo una especie de Switch de Core y los que se encuentra en los otros pisos hacen de Switch de Enlace.

Gráfico 3.9: Ubicación de los Access Point.

Fuente: El investigador



3.1.4.3. Análisis de las pruebas con el Antivirus y los Firewalls

3.1.4.3.1. Symantec AntiVirus™ Enterprise Edition

El Symantec es una sola solución fácil de instalar que proporciona protección completa contra programas nocivos en todos los niveles de la red.

Symantec AntiVirus™ Enterprise Edition proporciona protección contra virus, filtrado de contenidos y prevención de spam en el gateway de Internet y los entornos Domino® y Exchange, además de protección contra virus y spyware para las estaciones de trabajo y los servidores de red de la empresa. Esta solución completa y fácil de instalar detecta y repara automáticamente los efectos del spyware, el adware, los virus y demás programas nocivos. La reparación de efectos secundarios mantiene en funcionamiento los sistemas cuando se producen interrupciones de la seguridad. La perspectiva completa de los clientes mediante la centralización de los registros, umbrales de alerta e informes gráficos ayuda a transformar los datos de seguridad en información procesable. La solución ahora ofrece soporte de cliente antivirus para Linux® (Red Hat® Enterprise 3.0, Kernel 2.4; SuSE Linux Enterprise Server 9, Kernel 2.6; Novell® Linux Desktop 9, Kernel 2.6).

- Un paquete integrado con soluciones galardonadas de Symantec: Mail Security para SMTP, Mail Security para Microsoft® Exchange, Mail Security para Domino, AntiVirus Corporate Edition y Web Security.

- Avanzada protección contra virus y monitoreo de toda la empresa desde una sola consola de administración.
- La protección de Symantec contra manipulaciones defiende frente a los accesos no autorizados y los ataques, a la vez que mantiene alejados a los virus que intentan desactivar las medidas de seguridad.
- Servicio complementario Symantec Premium AntiSpam integrado opcional para los productos Symantec Mail Security.

3.1.4.3.2. Firewalls

El hecho de disponer de una conexión a Internet puede ser causa de multitud de ataques a nuestro ordenador desde el exterior. Cuanto más tiempo permanezcamos conectados mayor es la probabilidad de que la seguridad de nuestro sistema se vea comprometida por un atacante desconocido.

Tan propio del espíritu comercial anglosajón, se designa a una utilidad informática que se encarga de aislar redes o sistemas informáticos respecto de otros sistemas informáticos que se encuentran en la misma red. Constituyen una especie de "barrera lógica" delante de nuestros sistemas que examina todos y cada uno de los paquetes de información que tratan de atravesarla. En función de unos criterios establecidos previamente deciden qué paquetes deben pasar y cuáles deben ser bloqueados. Muchos son capaces de filtrar el tráfico de datos que intenta salir de nuestra red al exterior, evitando así que los troyanos sean efectivos. En la figura se muestra gráficamente el concepto. El Firewall actúa de intermediario entre nuestra

red local (o nuestro ordenador) e Internet, filtrando el tráfico que pasa por él.

Un Firewall, como se ha dicho, intercepta todos y cada uno de los paquetes destinados a o procedentes de nuestro ordenador, y lo hace antes de que ningún otro servicio los pueda recibir. De esto extraemos la conclusión de que el Firewall puede controlar de manera exhaustiva todas las comunicaciones de un sistema a través de Internet.

Otra función útil de la mayoría de los Firewall es su capacidad para mantener un registro detallado de todo el tráfico e intentos de conexión que se han producido (lo que se conoce como un Log). Estudiando los Log es posible determinar los orígenes de posibles ataques, descubrir patrones de comunicación que identifican ciertos programas malignos (lo que se conoce como Malware), etc... Sólo los usuarios avanzados podrán sacar partido a estos registros, pero es una característica que se le puede exigir perfectamente a estas aplicaciones.

SOFTWARE UTILIZADO DENTRO DE LA RED SIMINPEC

El Ministerio Público requería contar con información estadística que refleje el estado de los casos, de modo que se pudiera proponer políticas de control, prevención y mejoramiento para el sistema de justicia nacional; para lo cual se ha desarrollado un Sistema Informático que permite el control de las denuncias en las diferentes etapas del proceso penal en las que intervienen los Agentes Fiscales.

Este sistema está orientado a coadyuvar en las actividades que se desarrollan en las diferentes Distritos del país, específicamente en las actuaciones de los fiscales mediante el registro de los datos relacionados con las denuncias, indagación e instrucción fiscal, audiencias, recursos y sentencias, con la ayuda de una Cableado estructurado o una red inalámbrica ya instalada.

DESCRIPCIÓN DEL SISTEMA

Entre las funciones y beneficios que cumple el sistema podemos mencionar:

- Mantener el seguimiento de las causas desde el ingreso al Ministerio Público hasta su finalización, sea dentro del mismo o en un Juzgado, de una forma automatizada.
- Almacenar los datos de denuncias, que incluirán información de Denunciante/Víctima y Denunciado(s).
- Realizar la clasificación de las denuncias según las Unidades para mejorar el proceso de sorteos.
- Realizar el sorteo de las denuncias para asignarlas a los Agentes Fiscales en la unidad correspondiente.
- Introducir información relevante de las causas en la etapa de la Indagación Previa y de la Instrucción Fiscal.
- Manejar información de medidas cautelares que el Agente Fiscal o el Juez soliciten, sea en la etapa de Indagación Previa o en la de Instrucción Fiscal.
- Informar con anticipación sobre el vencimiento de los plazos para el cumplimiento de las etapas procesales.

- Almacenar información característica del Dictamen Fiscal, así como la resolución del mismo.
- Ingresar la información proveniente de los juzgados con respecto a los dictámenes remitidos.
- Introducir los datos que se obtengan de la Audiencia Preliminar.
- Registrar la información relevante y necesaria en la etapa del Tribunal Penal.
- Optimizar el tiempo empleado para realizar búsquedas de las causas ya sea por el número de las mismas o por los nombres de los involucrados; es decir, por denunciante o por denunciado.
- Generar reportes de la información mas relevante de acuerdo a criterios proporcionados por el usuario.

3.1.4.3.3. USUARIOS DEL SISTEMA

Para el SIMINPEC, se han definido deferentes perfiles de usuarios en cada uno de los módulos de este sistema.

CADA USUARIO TIENE ACCESO A OPCIONES DEL SISTEMA DE ACUERDO AL ROL QUE DESEMPEÑA DENTRO DEL MINISTERIO PÚBLICO DESDE DE EL INGRESO DE LA DENUNCIA HASTA LA RESOLUCIÓN DE LA MISMA.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Las redes inalámbricas están tomando mucha importancia en las actividades institucionales de hoy en día. Para lograr ser competitivos se requiere tener un acceso a la información del Ministerio Público de Cotopaxi de una manera rápida y sin restricciones en cualquier momento y lugar.

2. La velocidad de las redes inalámbricas es satisfactoria cuando se trata de transmisión y acceso a archivos de datos. Esto no sucede cuando se trata de transferencia de imágenes o videos según las pruebas realizadas por parte del departamento de Sistemas del Ministerio antes de proceder con la implementación de este importante recurso.

3. Las seguridades dentro de las redes inalámbricas, al igual que una red cableada, tiene sus desventajas, pero actualmente se están estudiando mejoras para efectivizarlas y dar confianza a los usuarios de la misma.

4. Una red inalámbrica bien configurada, es tan eficiente como una red cableada. Pues podemos tener una comunicación de datos en tiempo real y seguro.

5. Si el diseño no es correcto al configurar e implantar una red inalámbrica, se puede interferir en otra red inalámbrica cercana.

6. Una red inalámbrica es mas útil en una Organización, que en una red casera, pues sus costos en la actualidad, no son muy accesibles para el hogar.

7. Los costos de mantenimiento en una red inalámbrica, son menores que los costos de una red cableada; ya que en una red cableada cualquier remodelamiento de un espacio físico contribuye al incremento de gastos.

8. Se debe tomar siempre en cuenta los estándares y normas internacionales para la configuración y administración de ciertos servicios con que cuentan los servidores, ya que de esta manera estaremos precautelando la información que se genera en los distintos departamentos.

9. El continuo avance de las tecnologías ha influenciado notablemente en la reestructuración de los estándares de la IEEE y de las normas ISO y dentro de estos se ha implementado el Código de Práctica para la Administración de la Seguridad de la Información.

10. La capacitación en el Ministerio Publico debe realizarse inmediatamente ya que está nueva tecnología ha ocasionado cierta preocupación entre los usuarios de los computadores, más al momento de imprimir ya que no saben como hacer.

RECOMENDACIONES

1. Se recomienda realizar mayores estudios sobre redes inalámbricas de parte del Departamento de Sistemas del Ministerio, ya que es una tecnología que avanza cada vez más en las empresas de renombre mundial.

2. Al utilizar redes inalámbricas, se recomienda que estas sean utilizadas para transferencias y acceso a archivos de datos, pues por el momento, es en este punto donde denota su mayor utilidad.

3. Se recomienda utilizar redes inalámbricas en medios en los que continuamente se realizan cambios de infraestructura dentro de un edificio, pues su costo a la larga es mucho más conveniente.

4. Se debe realizar un análisis de diseño antes de implementar una red inalámbrica, pues de su buen diseño y configuración depende de que no interfiera en otras redes cercanas.

5. Para un correcto y eficaz funcionamiento, se recomienda utilizar tecnología inalámbrica en Equipos con procesador de 5OOMhz o superior, 256 MB de memoria RAM o superior, Sistema Operativo Windows XP o superior.

6. Hay que manejarlas con mucha prudencia, ya que son herramientas que ayudan a la configuración de equipos hijos, tomando las características de la maquina host y mermando el rendimiento de ésta.

7. La adquisición de equipos sean estos servidores o equipos personales se lo debe realizar buscando cumplir con las expectativas de la empresa o institución donde se vaya a implementar la red inalámbrica.

8. Los servidores establecidos en el Ministerio Publico de Latacunga son los necesarios en la actualidad pero para un futuro con el crecimiento se debería pensar en incrementar muchos más recursos sobre todo para fomentar la investigación.

9. Los estándares aplicados en este proyecto de tesis están siempre en actualización por lo cual no se debe dejar de revisar dichas actualizaciones y aplicar a la institución donde se lo implemente para poder dar un mejor servicio a los usuarios y para mantener un mejor control sobre estos.

10. Se recomienda la capacitación en el manejo responsable de las redes inalámbricas que en la actualidad se encuentra implementado en el Ministerio Publico sede Latacunga.

11. Para evitar conflictos de incompatibilidad de equipos de red y otros problemas se recomienda se tome como política de equipos con recursos suficientes a fin de evitarnos contratiempos en las configuraciones.

PROPUESTA

Factibilidad Técnica de las WLAN en el Ministerio Público

Como se explicó en detalle en el Capitulo I las redes inalámbricas surgen para resolver el problema de compatibilidad que existía entre los productos de los principales fabricantes de soluciones inalámbricas. De esta forma, la marca WiFi(Utilizamos para la implementación de comunicaciones en el Ministerio Público) asegura que el usuario tiene la garantía de que los equipos con sello WiFi pueden trabajar juntos sin problemas independientemente del fabricante de cada uno de ellos.

WiFi permite crear redes de trabajo sin necesidad de utilizar **cables** para interconectar los distintos equipos y sistemas que forman parte de la red. Esta característica trae consigo un gran número de ventajas que diferencian las redes WLAN (Wireless Local Area Network) de las redes LAN (Local Area Network) cableadas.

Ventajas de la Implementación de una WLAN

- **Movilidad**: El usuario tiene acceso tanto a los recursos privados y públicos pertenecientes a la red desde cualquier lugar que pertenezca al área de cobertura de la red local WLAN, que es de gran beneficio para nosotros por los constantes cambios de edificios.

- **Flexibilidad**: Permite disponer de conectividad en aquellos lugares en los que realizar una conexión cableada es físicamente imposible o cuyo coste es prohibitivo. Además los usuarios pueden conectarse y desconectarse cuando sea necesario y de forma muy sencilla a distintas redes WLAN según se encuentren en un lugar o en otro, en distintos lugares de trabajo, aeropuertos, hoteles,…

- **Coste**: El coste y el tiempo de instalación disminuyen ya que no es necesario realizar la instalación de cableado. Es una solución óptima cuando de trata de conexiones temporales y que cambian de lugar.

- **Escalabilidad**: La topología de la red se puede modificar muy fácilmente, se pueden añadir nuevos usuarios y dispositivos a la red sin modificar a los ya existentes. Lo que supone además una mayor libertad cuando se producen cambios organizativos dentro de la empresa.

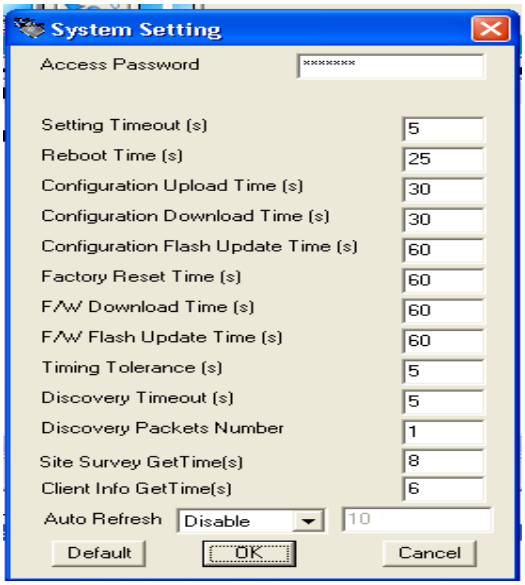
- **Compatibilidad**: Las redes WLAN son completamente compatibles con todos los servicios de las redes LAN cableadas, como por ejemplo la transmisión de voz (**VoIP**) y video por la red. Se pueden realizar llamadas a través de Internet utilizando teléfonos WiFi, siempre que se cuente con la arquitectura de red adecuada.

Configuraciones

Las configuraciones para las oficinas del Ministerio Público se lo realizo de acuerdo a los estándares que rigen la IEEE(Instituto de Ingenieros Eléctricos y Electrónicos), de igual manera se tomo como referencia las recomendaciones que vienen los manuales de los Access Point.

Gráfico 3.10: Configuración de los Access Point.

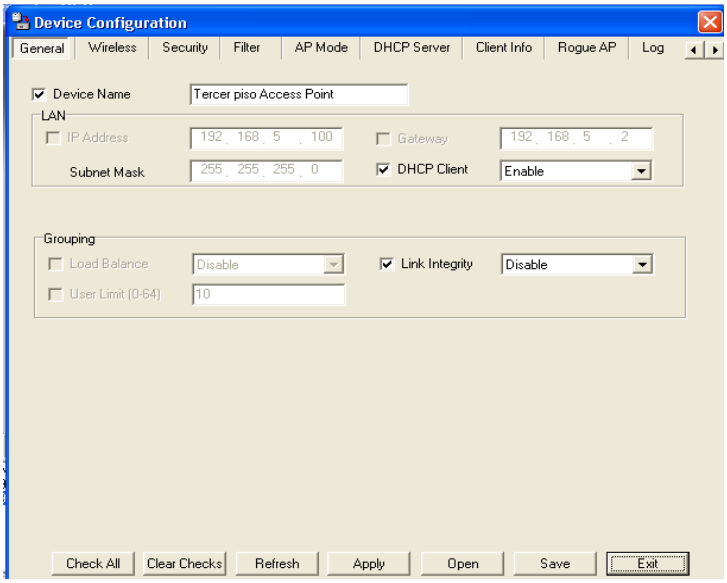
Fuente: El investigador



En la pantalla que se encuentra en la parte superior está la pantalla de configuración de passwords para el acceso o no al Access Point.

Gráfico 3.11: Configuración de los Access Point.

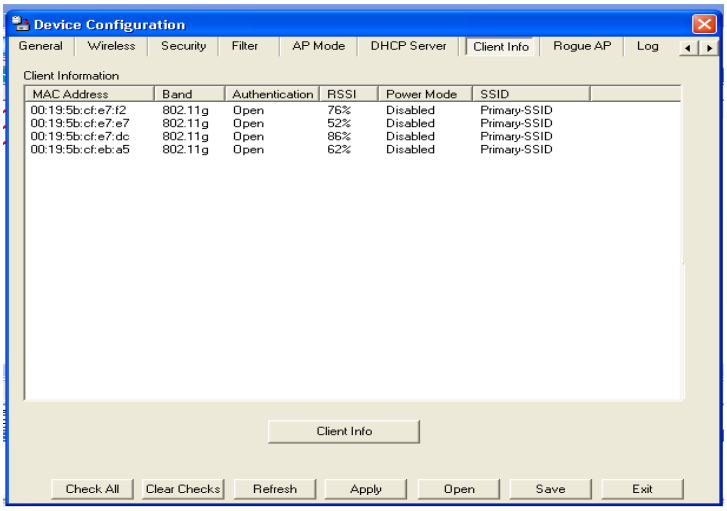
Fuente: El investigador



Este Gráfico nos muestra la pantalla principal de configuración de los AP que cuenta el Ministerio Público, que para nuestro caso el principal está con la IP 192.168.5.100, tenemos habilitada la opción de DHCP para la asignación de IP a todos los equipos que se conecten a la red inalámbrica.

Gráfico 3.12: Configuración de los Access Point.

Fuente: El investigador



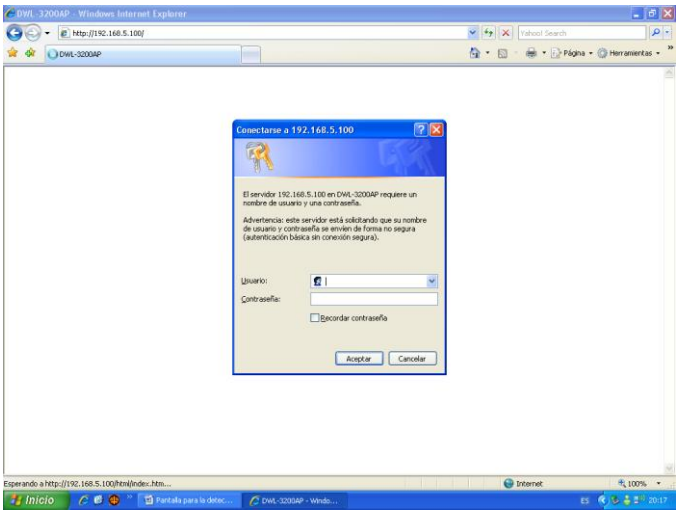
Una vez configurado el AP, debemos tener bajo administración todos los equipos que acceden al concentrador, esto se lo puede hacer mediante las direcciones IP o con las direcciones MAC de las tarjetas de red.

Configuración WEB

En la actualidad la gran mayoría de configuraciones de equipos se los hace remotamente, es así que la marca DLINK ofrece está opción de realizar configuraciones vía WEB.

Gráfico 3.13: Configuración Web de los Access Point.

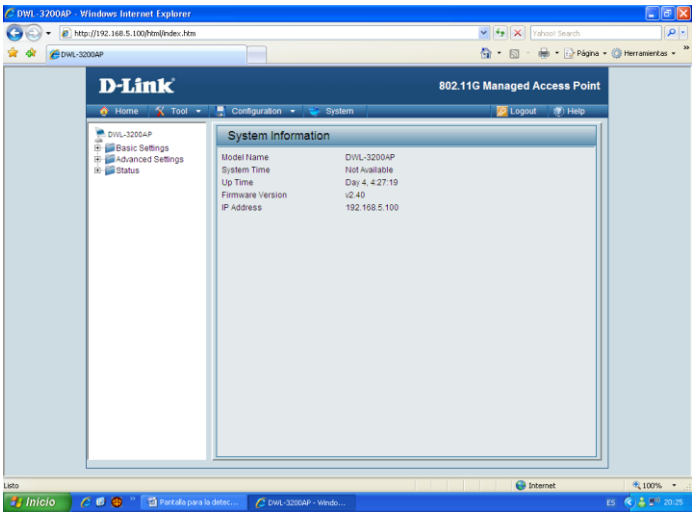
Fuente: El investigador



Pantalla de ingreso mediante contraseñas a la página de configuración vía Web del AP principal del Ministerio Público.

Gráfico 3.14: Configuración Web de los Access Point.

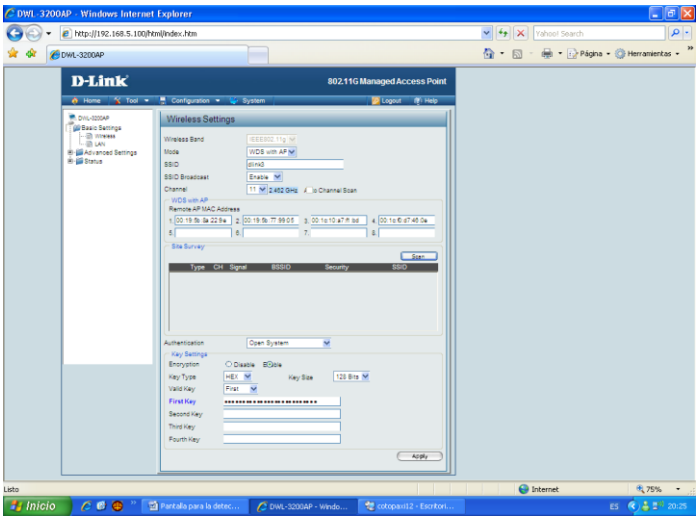
Fuente: El investigador



Pantalla principal de las configuraciones de los AP´s mediante paginas web, en esta se encuentra todas las opciones configurables de la red inalámbrica.

Gráfico 3.15: Configuración Web de los Access Point.

Fuente: El investigador



Pantalla para filtrado MAC, una vez ingresado aquí las direcciones de las tarjetas de red, la red inalámbrica le permitirá conectarse caso contrario no se lo podría hacer, ya que es una de las tres distintas formas de seguridades que se gestiona.

Funcionamiento

Para poder poner en práctica el funcionamiento debemos tener instalado en todos los computadores tarjetas de red inalámbricas, ya que es el elemento principal que se necesita para poder entrar dentro de la cobertura de las redes inalámbricas.

Gráfico 3.16: Instalación tarjeta de Red Inalámbrica.

Fuente: El investigador

En la grafica anterior se puede observar la instalación de la tarjeta de red de inalámbrica en el CPU, en la parte posterior se puede observar la antena de la tarjeta.

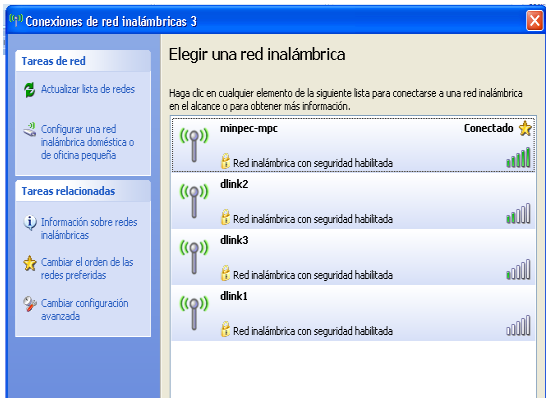
Gráfico 3.17: Configuración tarjeta de Red Inalámbrica.

Fuente: El investigador

En la gráfica anterior podemos observar como la tarjeta inalámbrica detecta la cobertura que tiene, que en nuestro caso dispone de 100Mbps para lo que es la red LAN.

Gráfico 3.18: Configuración tarjeta de Red Inalámbrica.

Fuente: El investigador

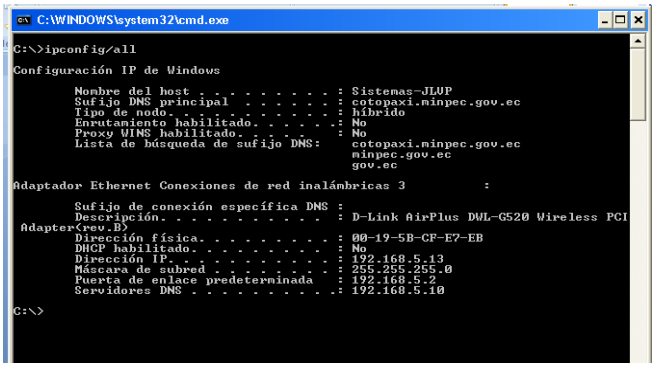


Nos brinda la opción de los 4 AP's con las que cuenta el Ministerio Público y dependiendo el radio de cobertura de cada uno de los dispositivos se puede acceder a la red inalámbrica como se puede observar en la gráfica anterior.

De igual manera podemos darnos cuenta que nuestros equipos disponen de un muy buen radio de cobertura el mismo que no está limitado para ningún número de usuarios.

Gráfico 3.18: Configuración Dirección IP de la Red Inalámbrica.

Fuente: El investigador



Podemos observar como el DHCP asigna la dirección IP dinámica a la computadora que solicita este servicio.

Diseño Físico de la Red Inalámbrica y Accesos

El diseño físico de la red tiene que ver con la interconexión de computadores y/o componentes digitales (Computadores, PDA, celulares, etc...) del Ministerio Público de Cotopaxi la misma que utiliza dispositivos de corto alcance los mismos que se encuentran interconectados entre si dentro de un rango no mayor a 10m, para que puede replicar la señal.

La distribución física de los equipos AP´s se lo ha hecho de forma que puedan ser vistos unos con otros es decir que permita las replicas de la señal dentro de todo el edificio, como lo muestra las figuras del anexo 3, en los cuales se encuentra dividido en 3 plantas y en todas y cada una de ellas se encuentran los AP y computadores clientes.

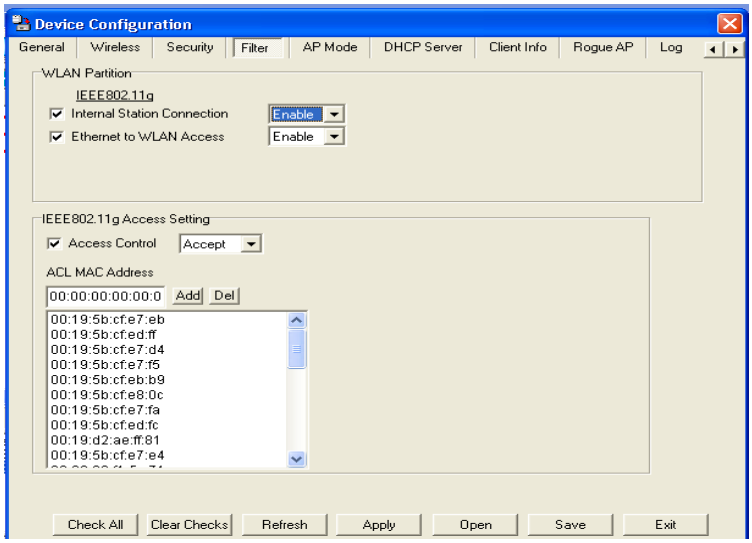
Es necesario dar a conocer que la señal alcanza incluso el exterior del edificio razón por la cual se ha tomado las seguridades anteriormente expuestas, ya que de está manera hemos evitado que se puedan dar los ataques de piratas informáticos (hackers).

Usar listas de control de acceso

Las listas de control de acceso están dadas de acuerdo al número de serie de la tarjeta de red conocidas también como direcciones MAC las mismas que son únicas y no hay parecidos con otros equipos que podrían invadir la privacidad de nuestra red.

Gráfico 3.19: Filtrado de Direcciones MAC

Fuente: El investigador

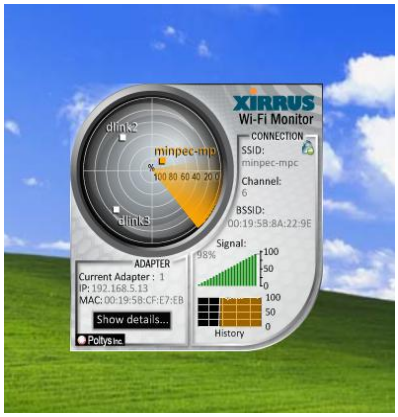


Se puede observar que de forma manual o automática se puede filtrar las direcciones MAC dentro de los Access Point para los equipos que se encuentren en la red.

Otra de las maneras es mediante el rastreo en forma de radar:

Gráfico 3.20: rastreo en forma de radar

Fuente: El investigador



Protocolo de Seguridad WEP instalado en el Ministerio

Al momento de la instalación de las seguridades que debería tener las redes inalámbricas del Ministerio Público se conocían las debilidades en cuanto a Seguridad Informática de las Redes Inalámbricas WIFI. Por este motivo se incluyó en el estándar 802.11b un mecanismo de seguridad que permita encriptar la comunicación entre los diversos elementos de una red inalámbrica WIFI. Esta protección se denominó WEP (Wired Equivalent Privacy). En español sería algo así como "Privacidad equivalente a la de una red cableada". El protocolo WEP se basa en el algoritmo de encriptación RC4.

La idea de los promotores del estándar 802.11b consistía en encriptar el tráfico entre Puntos de Acceso y estaciones móviles y compensar así la falta de seguridad que se obtiene al enviar la información por un medio compartido como es el aire. Es así como, todos los Puntos de Acceso y dispositivos WIFI incluyen la opción de encriptar las transmisiones con el Protocolo de Encriptación WEP.

Funcionamiento del protocolo WEP

Para poder entender el funcionamiento se dirá que hay que establecer una clave secreta en el Punto de Acceso, que es compartida con los clientes WIFI. Con esta clave, con el algoritmo RC4 y con un Vector de Inicialización (IV) se realiza la encriptación de los datos transmitidos por Radio Frecuencia.

A medida que fue aumentando la difusión de las Redes Inalámbricas WIFI, se fueron detectando graves problemas de seguridad informática en el Protocolo de Encriptación WEP, lo que generó hace unos años muy mala prensa a las redes inalámbricas WIFI. Ver: "De Nuevo: Las Redes Wireless no son Seguras"

El Vector de Inicialización IV, es demasiado corto pues tiene 24 bits y esto ocasiona que en redes inalámbricas WIFI con mucho tráfico se repita cada tanto.

Hay algunos dispositivos clientes (tarjetas, USB) muy simples que el primer IV que generan es cero y luego 1 y así sucesivamente. Es fácil de adivinar.

Las claves que se utilizan son estáticas y se deben cambiar manualmente. No es fácil modificarlas frecuentemente.

No tiene un sistema de control de secuencia de paquetes. Varios paquetes de una comunicación pueden ser robados o modificados sin que se sepa.

Esta situación generó la aparición de múltiples aplicaciones capaces de crackear la seguridad WEP en poco tiempo. Según la capacidad de los equipos utilizados y la habilidad del hacker y el tráfico de la red inalámbrica WIFI, se puede tardar desde 15 minutos a un par de horas en descifrar una clave WEP. Además del Airsnort mencionado en el artículo recomendado, están el WEPCrack, el NetStumbler, etc. En los últimos años hemos publicado en VIRUSPROT.COM, muchísimos artículos sobre este tema.

Análisis comparativo con otras técnicas y protocolos de seguridad en Redes Inalámbricas

El WPA y WPA2, son dos Protocolos de Encriptación que se desarrollaron para solucionar las debilidades detectadas en el protocolo de encriptación WEP. El nombre de WPA (WIFI Protected Access) que quiere decir en español: Acceso protegido WIFI, es un nombre comercial que promueve la WIFI Alliance.

La parte técnica está definida y estipulada en el estándar de seguridad IEEE 802.11i.

La WiFi Alliance, estaba interesada en buscar una rápida solución a los inconvenientes de WEP. Además se buscaba que la solución WPA, funcionara con los Puntos de Acceso y dispositivos WIFI, ya vendidos a miles y miles de usuarios. Por este motivo se decidió desarrollar dos soluciones. Una rápida y temporal que se denominó WPA y otra más definitiva para aplicar en nuevos Puntos de Acceso, y no en los existentes, que se llamó WPA2.

Los Puntos de Acceso existentes hasta ese momento (2001/2002) ya tenían la capacidad de su hardware ocupada al 90% con diversas funciones, por lo tanto cualquier modificación que se le hiciera al WEP, no podría requerir mucha capacidad de proceso.

Se desarrolló un protocolo temporal denominado TKIP (Temporal Key Integrity Protocol) que es una "envoltura" del WEP y es conocido como WPA. El WPA (primera fase del estándar 802.11i) fue aprobado en Abril de 2003. Desde Diciembre de 2003 fue declarado obligatorio por la WiFi Alliance. Esto quiere decir que todo Punto de Acceso Inalámbrico que haya sido certificado a partir de

esta fecha, ya debe soportar "nativamente" WPA. Todo Punto de Acceso anterior a Diciembre de 2003 puede soportar "nativamente" sólo WEP. Recuerde!: Todos los fabricantes miembros de la WiFi Alliance deben poner gratuitamente a disposición de sus clientes un "parche" para actualizar los Puntos de Acceso antiguos de WEP a WPA.

Mejoras a la Seguridad WIFI introducidas en WPA se incrementó el Vector de Inicialización (IV) de 24 bits a 48.

Se añadió una función MIC (Message Integrity Check) para controlar la Integridad de los mensajes. Detecta la manipulación de los paquetes.

Se reforzó el mecanismo de generación de claves de sesión.

Existen 2 versiones de WPA, una "home" o "Personal" que es para uso casero y de pymes, y otra más robusta denominada "Enterprise". No vienen activadas por defecto y deben ser activadas durante la configuración. Los Puntos de Acceso antiguos "emparchados" o actualizados de WEP a WPA se vuelven más lentos, generalmente y, si bien aumenta la seguridad, disminuye el rendimiento

Ahora vamos a realizar un estudio del protocolo WPA2, que no se lo pudo adoptar por carecer de los equipos pero que tiene algunas desventajas con respecto al WEP que adoptamos.

WPA2, es el nombre que le dio la WIFI Alliance a la segunda fase del estándar IEEE 802.11i. La seguridad es muchísimo más robusta que la que ofrece WPA. WPA2 ya no se basa en un parche temporal sobre el algoritmo RC4 y, en su lugar, utiliza el algoritmo de encriptación AES - recomendado por el NIST , de los más fuertes y difíciles de crackear en la actualidad. Este algoritmo de encriptación requiere un hardware más robusto, por lo tanto los Puntos de Acceso antiguos no se pueden utilizar con WPA2. Las primeras certificaciones de Puntos de Acceso compatibles con WPA2, se han hecho en Septiembre de 2004. Esto era voluntario,

pero WPA2 es requisito obligatorio para todos los productos WIFI, desde Marzo de 2006.
La implementación de protección que se aplica en el estándar de seguridad Wifi 802.11i, se conoce con el acrónimo CCMP y está basada, como ya se comentó, en el algoritmo de encriptación AES (ver: Rijndael). El cifrado que se utiliza es simétrico de 128 bits - ver: Criptografía Simétrica y Asimétrica - y el Vector de Inicialización (IV) tienen una longitud de 48 bits.

Otra de las técnicas es la utilización de las VPN añade bastante seguridad a las redes inalámbricas pero tiene ciertas desventajas. Una de ellas es la económica pues cada túnel tiene un costo para la empresa y cuando se trata de proteger a cientos o miles de usuarios de una red inalámbrica WIFI, las VPN se convierten en extremadamente costosas. Otro inconveniente es que las VPN han sido pensadas y diseñadas para conexiones "dial-up" punto a punto, pero las redes inalámbricas WIFI transmiten ondas de RF (irradian) por el aire que es un medio compartido, como se explicó en el capítulo de Tecnología WIFI . En la siguiente tabla, se detallan muy brevemente las desventajas de proteger una red inalámbrica WIFI con VPN.

Para un número grande de clientes WIFI, suele ser una solución bastante costosa.

Están diseñadas para proteger a partir de la capa 3 del modelo OSI, pero las redes inalámbricas WIFI (802.11) funcionan en capa 2.

Por lo tanto, las VPN pueden ser una buena solución cuando ya están siendo utilizadas en la organización y se necesita proteger a los primeros usuarios de WIFI. En cuanto se masifica la utilización de las redes inalámbricas WIFI, su gestión se complica y los costos aumentan de manera innecesaria.

Por último tenemos al Servidor RADIUS

RADIUS es el acrónimo de Remote Authentication Dial In User Service. Sus diversas funciones y características están definidas en varias RFC de la IETF. Algunas de las importantes son: RFC 2058, 2138 y 2548 . Como su nombre lo indica es un servidor que tiene la función de autenticar a los usuarios que se conectan remotamente.

Originalmente estaba pensado para accesos por líneas cableadas, pero cuando se modificó el estándar 802.1x para seguridad WIFI, se adaptó también como herramienta de autenticación para las redes inalámbricas wifi.

El servidor RADIUS cumple varias funciones en la arquitectura de seguridad de una red inalámbrica WIFI, las cuales se detallan a continuación:

Funciones del Servidor RADIUS en Redes Inalámbricas WIFI

El servidor RADIUS generalmente es un software aunque existen algunos aplicaciones. Las versiones servidor de Windows 2000 y Windows 2003 incluyen un servidor RADIUS, que se denomina IAS - Internet Access Server. Este, como la mayoría de los servidores RADIUS tiene varias limitaciones de plataforma, S.O, etc. que se comentarán más adelante.

Como se vio, el servidor RADIUS tiene la función de Autenticar y de Autorizar a los clientes de WIFI. Los servidores RADIUS más completos incluyen una tercera función que es el Accounting, por eso se denominan "AAA" o "Triple A".

Para finalizar, digamos que en lo que respecta a Seguridad WIFI, los Servidores RADIUS, además de autenticar y autorizar el acceso de usuarios añaden otras ventajas muy relevantes:

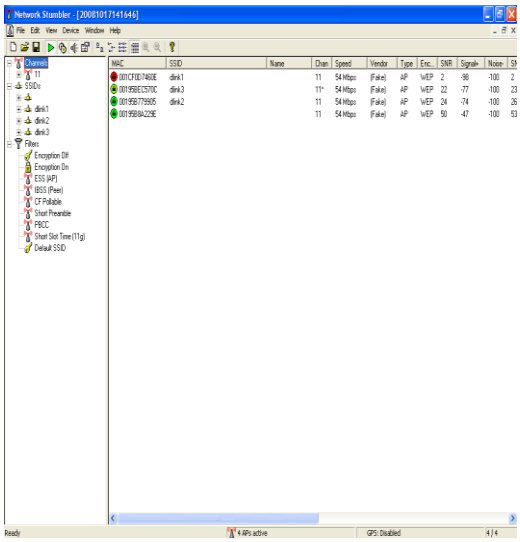
Análisis de las seguridades implementadas

Network Stumbler es un scanner Wireless para plataforma Windows, y es el programa que utilizaremos para localizar las redes fig. 3.21 wireless con nuestra tarjeta de red. Es un programa basado en consola de monitoreo con muchas opciones que nos da información como la dirección MAC, el nombre de la red, la velocidad de la red, en algunos casos nos da la información o nombre del fabricante del Acces Point, el tipo de encriptación, entre otros datos.

El Netstumbler sólo detecta las redes que hacen Broadcast de SSID, no detecta redes Hidden o Cloacked. Para entender mejor este trabajo vamos a explicar de forma muy general algunos parámetros utilizados en el programa Network Stumbler (Netstumbler).

Gráfico 3.20: rastreo en forma de radar

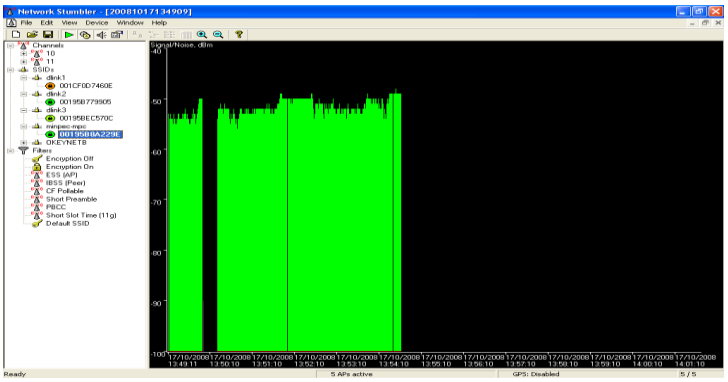
Fuente: El investigador



En el siguiente grafico nos muestra el porcentaje o la intensidad de la señal de conectividad de la tarjeta inalámbrica con el Access Point el mismo que esta deshabilitado el SSID BROADCATS.

Gráfico 3.21: Porcentaje de la Intensidad de la Señal

Fuente: El investigador



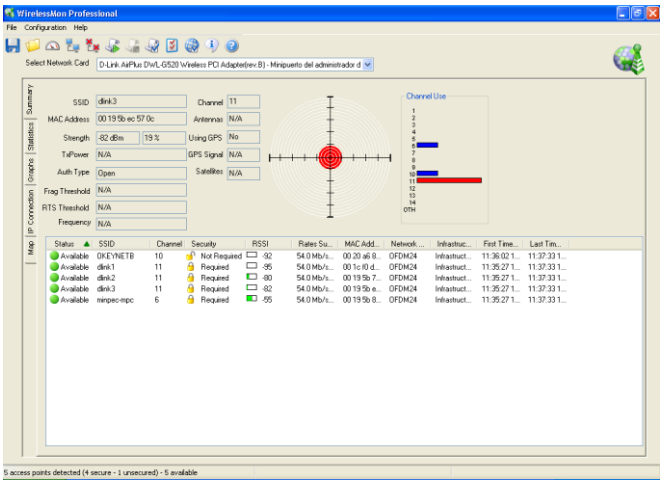
Wirelessmon

Con este software podemos ver las redes inalámbricas que están dentro del alcance de nuestra antena de la tarjeta de red inalámbrica.

En este grafico se muetra la señal de intensida de cada uno los acces point que nuestra tarjeta de red inalambrica puede capatr o estan al alance en el mismo que esta habilitadoi el SSID (minpec-mpc) para que todas las personas puedan ver el nombre de nuestro Access Point.

Gráfico 3.22: Habilitación del SSID

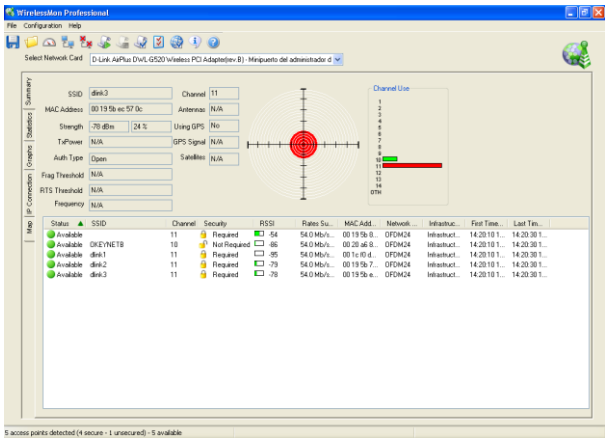
Fuente: El investigador



En este otro grafico esta deshabilitado el SSID (minpec-mpc)

Gráfico 3.23: Deshabilitar del SSID

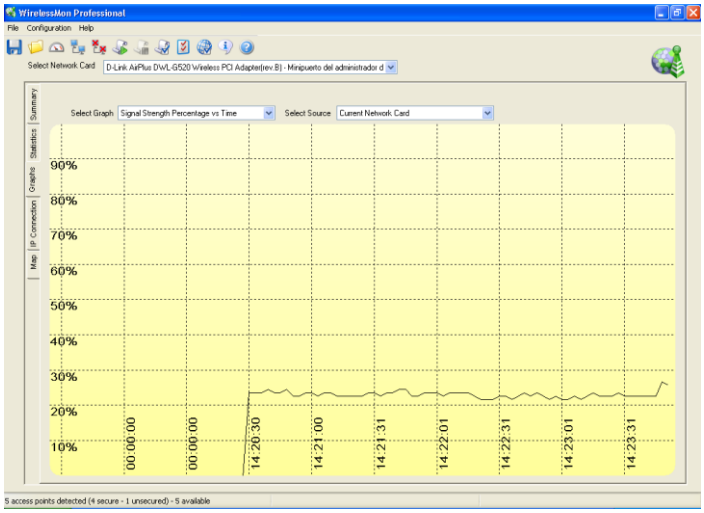
Fuente: El investigador



En este otro mostramos la representación grafica de intensidad de señal conectada al Access Point Dlink3.

Gráfico 3.24: Intensidad de la Señal

Fuente: El investigador



GLOSARIO DE TÉRMINOS Y SIGLAS

Acceso Físico

Es el medio utilizado para obtener información de las oficinas, salas de cómputo, escritorios y archivos.

Acceso Lógico

Es el medio utilizado para obtener información de las bases de datos y sistemas de información de la organización.

Activos

Son los recursos de la organización. Existen varios tipos de activos como son: Los recursos de información (bases de datos, los documentos de sistemas), los recursos de software (software de sistemas operativos, herramientas de desarrollo), activos físicos (equipamiento informático, equipos de comunicaciones, otros) y servicios (iluminación, energía eléctrica, etc.)

Amplitud de banda

La amplitud de banda especifica la cantidad de datos que pueden transmitirse en una cantidad de tiempo fija. En el caso de los dispositivos digitales, la amplitud de banda se define en bits por segundo (bps) o bytes por segundo.

ASIC

Circuito integrado específico de una aplicación. Chip personalizado diseñado para una aplicación específica.

Asignaciones de amplitud de banda

La cantidad de amplitud de banda asignada a una aplicación, usuario o interfaz específicos.

Anomalía

Irregularidad en el funcionamiento de un sistema, de un software, de un control, etc.

Camino Forzado

Ruta limitada entre una Terminal de usuario y los servicios del computador. Evita que los usuarios seleccionen rutas fuera de la trazada entre su Terminal y los servicios a los cuales esta autorizado a acceder.

Canal Oculto

Es un cauce de comunicación que permite a un proceso receptor y a un emisor intercambiar información de forma que viole la política de seguridad del sistema; esencialmente se trata de un método de comunicación que no es parte del diseño original del sistema pero que puede utilizarse para transferir información a un proceso o usuario que a priori no estaría autorizado a acceder a dicha información.

Clave Pública

Clave que puede ser revelada a cualquier persona.

Clave Secreta

Clave que debe mantenerse en secreto.

Código Troyano

Es un programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas acciones que afectan a la confidencialidad del usuario afectado.

Comercio Electrónico

Consiste en la compra, venta, marketing y suministro de información complementaria para productos o servicios a través de redes informáticas.

Computación Móvil

Se define como la serie de artefactos y equipos portátiles, hardware, que hacen uso de la computación para lograr su funcionamiento, así, se tiene a las computadoras portátiles, los teléfonos celulares, los cuadernos de notas computarizados, las calculadoras de bolsillo, etc.

Criptografía

Dícese de la ciencia que estudia la forma de codificar y descodificar documentos, de forma que sólo puedan ser leídos por la persona que posee la clave de descodificación.

Capa 2

Capa de vínculo de datos o capa MAC. Contiene la dirección física de un cliente o estación de servidor. El proceso de la capa 2 es más rápido que el de la capa 3 porque hay menos información que deba procesarse.

Capa 4

Establece una conexión y garantiza que todos los datos lleguen a su destino. Los paquetes inspeccionados en el nivel de la capa 4 se analizan y las decisiones se reenvían en función de sus aplicaciones.

Capa MAC

Subcapa de la capa de control de vínculo de datos (DTL).

Class of Service (Clase de servicio)

La clase de servicio es el esquema de prioridad 802.1p. La CoS proporciona un método para asignar etiquetas a los paquetes con información sobre la prioridad. Un valor de CoS situado entre 0 y 7 se agrega al encabezado de la capa 2 de los paquetes, donde cero es la prioridad más baja y siete es la más alta.
Transmisión de superposición de dos o más paquetes que colisionan. Los datos transmitidos no pueden utilizarse, y la sesión se reinicia.

Dirección IP

Dirección del protocolo de Internet. Dirección exclusiva asignada a un dispositivo de red con dos o más LAN o WAN interconectadas.

Dirección MAC

Dirección Media Access Control. La dirección MAC es una dirección específica del hardware que identifica cada nodo de red.

DSCP

DiffServe Code Point (DSCP). DSCP proporciona un método de asignación de etiquetas de paquetes IP con información de prioridad QoS.

Evaluación de Riesgos

Es un proceso dirigido a estimar la magnitud de aquellos riesgos que no hayan podido evitarse, obteniendo la información necesaria para que el empresario esté en condiciones de tomar una decisión apropiada sobre la necesidad de adoptar medidas preventivas y, en tal caso, sobre el tipo de medidas que deben adoptarse. La evaluación de riesgos consta de una fase llamada de análisis de riesgos (identificación de peligros y estimación de los riesgos) y una fase posterior de valoración de riesgos y de control de riesgos si fuese posible.

Evidencia

Datos, registros, declaraciones de hecho o cualquier otra información que respaldan la existencia o veracidad de algo.

HONEYPOTS (Tarro de Miel)

Recurso de red destinado ha ser atacado o comprometido. Los Honeypots son los encargados de proporcionar información valiosa sobre los posibles atacantes en potencia a nuestra red antes de que comprometan sistemas reales. Es decir el objetivo de los Honeypots es recibir los ataques, no recoger información para demandar a los atacantes del Honeypot.

HONEYNETS (Tarro de Miel)

Es un tipo de Honeypot. Específicamente es un Honeypot altamente interactivo diseñado para la investigación y la obtención de información sobre atacantes. Un Honeynet es una arquitectura, no un producto concreto o un

software determinado. Y consiste no en falsear datos o engañar a un posible atacante (como suelen hacer algunos Honeypot), sino que el objetivo principal es recoger información real de cómo actúan los atacantes en un entorno de verdad.

Incidente

Dícese del fallo que sucede en un equipo o sistema de manera temporal o aleatoria, sin que existan unos motivos claros para ello.

Procesamiento de Información

Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida.
Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados.

Seguridad Informática

Conjunto de técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionales. Estos daños incluyen el acceso a bases de datos de personas no autorizadas, el mal funcionamiento del hardware y la perdida física de datos.

Seguridad de la Información

La seguridad de la información consiste en proteger uno de los principales activos de cualquier empresa: la información. La seguridad de la información

es requisito previo para la existencia a largo plazo de cualquier negocio o entidad. La información es usada en cada uno de los ámbitos empresariales, los cuales dependen de su almacenamiento, procesado y presentación.

Servicio de Información

Un servicio para los sistemas que proporciona un sistema de base de datos para los archivos de configuración comunes.

Servicio de Red

Es un servicio para que cualquier máquina de la red puede comunicarse con otra distinta y esta conectividad permite enlazar redes físicamente independientes.

Sistema de Información

Conjunto de elementos, ordenadamente relacionados entre sí que aporta al sistema objeto, es decir, a la organización a la cual sirve y le marca directrices de funcionamiento, la información necesaria para el cumplimiento de sus fines, para lo cual tendrá que recoger, procesar y almacenar la información, facilitando la recuperación de la misma.

Sistema Informático

Es aquel sistema que se encarga del manejo de información en la computadora, a través de la cual el usuario controla las operaciones que realiza el procesador.

Sistema Operativo

Termino que se utiliza para referirse al conjunto de programas interrelacionados, que se dedican a controlar las funciones básicas del sistema, las operaciones de bajo nivel y el manejo de archivos sin necesidad de que intervenga un operador.

Software Malicioso

Software que ha sido deliberadamente diseñado para producir un resultado defectuoso o dañoso para el usuario. Incluye tanto la categoría genérica de los virus informáticos, como la del llamado spyware.

Trabajo Remoto

Se refiere al trabajo que una persona realiza por fuera de su puesto de trabajo normal.

Utilitarios del Sistema

Reconstruir índices, compactar y validar bases de datos, validar consistencia de datos, cambiar fecha de operación y del sistema, importar y exportar datos entre empresas, transferir productos, precios, existencias de almacén y acceso al generador de reportes.

TFTP

Protocolo trivial de transferencia de archivos. Utiliza el protocolo de datos de usuario (UDP) sin características de seguridad para transferir archivos.

Trama

Los paquetes que contienen el encabezado y la información de cola que requiere el medio físico.

Tramas gigantes

Permiten transportar datos idénticos en menos tramas. Las tramas gigantes reducen el coste, necesitan un tiempo de procesamiento inferior y garantizan menos interrupciones.

Velocidad de puerto

Indica la velocidad del puerto. La velocidad de los puertos incluye:

Ethernet 10 Mbps
Fast Ethernet 100 Mbps
Gigabit Ethernet 1000 Mbps

4.4.- BIBLIOGRAFÍA

- **Andrew Tanenbaum,** Redes de Computadores, Cuarta Edición 2004
- **Tyson Creer,** Así son las Intranets, Segunda Edición. 2002
- Building Cisco Multilayer Switched Networks; Cisco System, Cisco Press, 2000.
- Cisco CCNA Exam #640-607; Cisco System, Cisco Press, 2002.
- Implementing Cisco Quality of Service v 2.0; Cisco System, Cisco Press, 2003.
- **VLADIMIROV ANDREW A. (2005)**, Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, España.
- **ANSI/IEEE STD 802.11, 1999** Edition. [1]"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"
- **Hills. "Large-Scale Wireless LAN Design**". IEEE Communications Magazine, vol. 39, nº 11, noviembre 2001.

4.4.1. - WEB BIBLIOGRAFÍA

- http://www.linuxparatodos.com/honeypot.htm
- http://www.linuxparatodos.com/ids.htm
- http://www.linuxparatodos.com/ips.htm
- http://lauca.usach.cl/~lsanchez/Vlan/
- http://www.eduangi.com/documentos/3_CCNA2.pdf
- http://www.avantel.net/~rcruz/Cap3qosrba.pdf
- http://www.lavioleta.net/Capitulo1.htm
- http://www.commlogik.com.ar/cisco.html
- http://informatica.uv.es/doctorado/SST/docto-2-qos.ppt#389,2,Sumario
- http://www.3com.es/news/reportajes/pdfs/switching_comunicaciones_world.pdf

- http://dmi.uib.es/~loren/docencia/webxtel/bibliografia/tutorial%20VLAN.pdf
- http://net21.ucdavis.edu/newvlan.htm
- http://www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/vlan.html
- http://iie.fing.edu.uy/~rgaglian/Docs/VPLS.pdf
- http://www.emagister.com/frame.cfm?id_user=889302005026967485067487070455 5&id_centro=57953030052957564866666952674548&id_curso=65425040050167555457685550674555&url_frame=http://www.emagister.com/public/pdf/comunidad_emagister/01793120043168694849677065484567-config-ciscos.pdf
- http://www.it.iitb.ac.in/~it605/resources/Local/Docs/VLAN/VLANIntro.pdf
- http://www.isa.uniovi.es/docencia/redes/tema4.pdf
- http://www.mythdragon.com/QoS/documents/QoS%20routing%20for%20support%20MM%20apps.pdf
- http://www.alcatel.ch/com/en/appcontent/apl/A0506-Broadband_QoS-ES_tcm172-287901635.pdf
- http://www.adictosaltrabajo.com/linux/proxy.htm
- http://www.adictosaltrabajo.com/linux/proxyinverso.htm
- http://www.adictosaltrabajo.com/linux/firewall.htm
- http://www.adictosaltrabajo.com/linux/cortafuegos.htm
- http://www.monografias.com/proxy.htm
- http://www.monografias.com/firewall.htm
- http://www.cudi.edu.mx/primavera_2005/presentaciones/felipe_alvarez.pdf
- http://www.si.uji.es/bin/ponencies/ipp.pdf
- http://www.idg.es/comunicaciones/especial-avether160/Pag08.pdf
- http://www.iec.uia.mx/proy/titulacion/proy14/vpnprin.htm

ANEXOS 1

COSTO DE MATERIALES UTILIZADOS EN LA IMPLANTACIÓN DE RED INALÁMBRICA

Cantidad	Producto	P. Unitario	Total
1	Switch 3COM, 24 puertos	145	145
50	Cable UTP Cat. 5e	0,6	30
3	Access Point D-LINK 3200	225	675
1	Access Point D-LINK 2100	170	170
30	Tarjeta de red CNET	15	450
Subtotal			**1470,00**
IVA			**176,4**
TOTAL			**1646,4**

SUMINISTROS

Cantidad	Producto	P. Unitario	Total
2	Resmas de papel bond A4	3,5	7
4	Esferográficos	0,3	1,2
10	Carpetas de cartón	0,3	3
300	Impresiones	0,15	45
800	Copias	0,03	24
5	Anillados	1	5
Subtotal			**85,2**
IVA			**10,224**
TOTAL			**95,424**

Costo total: $ 1.741,82 (mil setecientos cuarenta y un dólares con 82/100)