Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

TECNOLOGÍAS PARA BRINDAR SEGURIDAD EN REDES INALÁMBRICAS: UN ENFOQUE PARA CONSEGUIR UNA RED INALÁMBRICA MÁS SEGURA

Juan Pablo Porón Lara

Asesorado por el Ing. Marlon Antonio Pérez Turk

Guatemala, octubre de 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

TECNOLOGÍAS PARA BRINDAR SEGURIDAD EN REDES INALÁMBRICAS: UN ENFOQUE PARA CONSEGUIR UNA RED INALÁMBRICA MÁS SEGURA

TRABAJO DE GRADUACIÓN
PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JUAN PABLO PORÓN LARA
ASESORADO POR EL ING. MARLON ANTONIO PÉREZ TURK

AL CONFERÍRSELE EL TÍTULO DE
INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, OCTUBRE DE 2006

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Lic. Amahán Sanchez Alvarez
VOCAL III	Ing. Julio David Galicia Celada
VOCAL IV	Br. Kennet Issur Estrada Ruiz
VOCAL V	Br. Elisa Yazminda Vides Leiva
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Javier Gramajo López
EXAMINADOR	Ing. Cesar Augusto Fernández Cáceres
EXAMINADOR	Inga. Virginia Victoria Tala Ayerdi
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

TECNOLOGÍAS PARA BRINDAR SEGURIDAD EN REDES INALÁMBRICAS: UN ENFOQUE PARA CONSEGUIR UNA RED INALÁMBRICA MÁS SEGURA,

tema que me fuera asignado por la Dirección de la Escuela de Ciencias y Sistemas, con fecha enero de 2006.

JUAN PABLO PORÓN LARA

DEDICATORIA A:

Dios

Por darme la vida, las oportunidades y sobre todo por haberme acompañado en este camino hacia el saber.

Mis padres

Rodolfo Porón Castillo y María Hortensia Lara Fuentes, por brindarme su apoyo incondicional en todo momento porque esta meta alcanzada es el fruto de sus esfuerzos y sacrificios.

Mis hermanos

Américo, Antonio, Mirna, Alicia, Flor de María, por su apoyo.

Mis abuelos

Socorro Porón Agreda (Q.E.P.D.) María Alicia Castillo Alvarado (Q.E.P.D.) por sus consejos y apoyo moral.

Mis sobrinos

Con cariño especial.

Mi asesor

Ing. Marlon Antonio Pérez Turk, por compartir su experiencia y asesorar este trabajo.

Mis amigos

Por su amistad y tantos momentos compartidos. Porque cada uno de ellos alcance sus metas.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Access Point Punto de acceso, es el dispositivo que hace de puente entre la red cableada y la red inalámbrica. Se puede pensar que es, de alguna manera, la antena que se encarga de la conexión.

Ad-Hoc Tipo de modo de operación de las redes inalámbricas *de equipo a equipo*, las estaciones inalámbricas se conectan, directamente, entre sí, no mediante puntos de acceso inalámbricos.

Algoritmo Conjunto de sentencias o instrucciones en lenguaje nativo, los cuales expresan la lógica de un programa.

Algoritmo MD5 Algoritmo de encriptación de 128-bits del tipo EAP creado en 1991 por el profesor Ronald Rivest para RSA *Data Security*, Inc. empleado para crear firmas digitales. Emplea funciones *hash* unidireccionales, es decir, que toma un mensaje y lo convierte en una cadena fija de dígitos. Cuando se utiliza una función *hash* de una dirección, se puede comparar un valor *hash* frente a otro que esté decodificado con una llave pública para verificar la integridad del mensaje. Basado en nombre de usuario y contraseña, el primero se envía sin protección. Sólo autentica el cliente frente al servidor, no el servidor frente al cliente.

Ancho de banda	*Bandwidth* en inglés. Cantidad de bits que pueden viajar por un medio físico –cable coaxial, par trenzado, fibra óptica, etc– de forma que mientras mayor sea el ancho de banda más rápido se obtendrá la información. Se mide en millones de bits por segundo (Mbps).
ATM	Modo de transferencia asincrónica. Protocolo para conexiones de alta velocidad que se utiliza con el fin de transportar muchos tipos de tráfico de red diferentes. ATM empaqueta los datos en una celda de longitud fija de 53 *bytes* que se puede intercambiar, rápidamente, entre conexiones lógicas de una red.
Base de datos	Es un almacenamiento colectivo de las bibliotecas de datos que son requeridas y organizadas para cubrir sus requisitos de procesos y recuperación de información.
Bit	Dígito binario. Unidad mínima de almacenamiento de la información cuyo valor puede ser 0 ó 1 –falso o verdadero respectivamente.
Bluetooth	Estándar de transmisión de datos inalámbrico vía radiofrecuencia de corto alcance –unos 10 metros. Permite la comunicación entre videocámaras, celulares y computadoras que tengan este protocolo,

	para el intercambio de datos digitalizados: vídeo, audio, texto, etc.
Broadcasting	Es la distribución de señales de audio y video a un número de destinatarios, los oyentes o televidentes según el medio, conformando una audiencia masiva. Esta audiencia puede ser el público en general o un subgrupo relativamente grande del mismo.
Byte	Grupo de bits adyacentes operados como una unidad, grupos de 8 bits.
CBC-MAC	*Counter Mode Cipher Block Chaining-Message Authentication Code,* es un algoritmo de cifrado utilizado con el método AES.
CCMP	*Counter-Mode Cipher Block Chaining Message Authentication Code Protocol*, es un protocolo de encripción inalámbrico basado en *Advanced Encryption Standard* (AES) y definido en la especificación IEEE 802.11i. CCMP usa un bloque de clave simétrica en el modo de cifrar que proporciona integridad y confidencialidad.
CDMA	Acceso Múltiple por División de Códigos, es una tecnología utilizada para transmitir llamadas inalámbricas asignándoles códigos. Las llamadas son esparcidas en el más amplio rango de canales disponibles. Entonces, los códigos permiten que

	muchas llamadas viajen en la misma frecuencia y también guían a esas llamadas al teléfono receptor correcto.
CD-ROM	*Compact Disc Read Only Memory* es un medio de almacenamiento de sólo lectura.
Certificado digital	Acreditación emitida por una entidad o un particular debidamente autorizada garantizando que un determinado dato –una firma electrónica o una clave pública, pertenece realmente a quien se supone. Por ejemplo, *Verisign* y *Thawte*.
Checksum	Suma de chequeo, es un contador que recoge la suma de los resultados de aplicar un determinado algoritmo a cada octeto de la información a comprobar.
Chip	Es una pastilla o *chip* en la que se encuentran todos o casi todos los componentes electrónicos necesarios para realizar alguna función. Estos componentes son transistores en su mayoría, aunque, también, contienen resistencias, diodos, condensadores, etc.
Cliente	Computadora o programa que se conecta a servidores para obtener información. Un cliente sólo obtiene datos, no puede ofrecerlos a otros clientes sin depositarlos en un servidor. La mayoría de las

	computadoras que las personas utilizan para conectarse y navegar por Internet son clientes.
CRC	Acrónimo de *Cyclic Redundancy Checking* –Control de Redundancia Cíclica. Número de control utilizado para comprobar otra serie de valores. Utilizado ampliamente en la tecnología de ordenadores: comprobación del estado de un archivo, chequeo de virus, mecanismos anticopia, protección de datos, generación y chequeo de claves, validación de tarjetas, etc.
CRC – 32	El CRC de 32 bits tiene actualmente un uso muy extendido, incluso hasta en el Departamento de Defensa de los EUA. Se considera, actualmente, como el método más eficiente de comunicación digital en materia de detección y corrección de errores. Se puede implementar ya sea mediante un circuito cableado (*hardware*) o empleando un algoritmo de procesamiento digital (*software*).
Datagrama	Agrupamiento lógico de información enviada como unidad de la capa de red en un medio de transmisión, sin el establecimiento de un circuito virtual.
DHCP	Un estándar propuesto en RFC 1541 para transferir información de configuración de red desde un servidor central a los dispositivos cuando estos se inicializan. Típicamente, estos datos incluyen una

dirección IP para la máquina que el servidor puede cambiar y alojar sobre la marcha bajo DCHP.

DSSS *Direct Sequence Spread Spectrum* o Espectro Amplio mediante Secuencia Directa, a diferencia de la técnica de transmisión de Espectro Amplio (*Spread Spectrum*) FHSS, DSSS no precisa enviar la información a través de varias frecuencias sino mediante transmisores; cada transmisor agrega bits adicionales a los paquetes de información y únicamente el receptor que conoce el algoritmo de estos bits adicionales es capaz de descifrar los datos. Es, precisamente, el uso de estos bits adicionales lo que permite a DSSS transmitir información a 10Mbps y una distancia máxima entre transmisores de 150 metros. Un estándar que utiliza DSSS es IEEE 802.11b.

Ethernet Estándar IEEE 802.3 para redes de contención. *Ethernet* utiliza una topología en bus o estrella, y depende de la forma de acceso conocida como acceso múltiple con detección de portadora y colisiones –CSMA/DC, *Carrier Sense Multiple Access with Collision Detection*– para regular el tráfico en la línea de comunicaciones. Los nodos de la red se vinculan mediante cable coaxial, cable de fibra óptica o cable de par trenzado. Los datos se transmiten en tramas de longitud variable que contienen información de entrega y de control, cuyo tamaño

puede ser de hasta 1.500 bytes. El estándar *Ethernet* permite la transmisión de banda base a una velocidad de 10 megabits –10 millones de bits– por segundo.

Fast Ethernet — *Fast Ethernet* o *Ethernet* de alta velocidad es el nombre de una serie de estándares de IEEE de redes *Ethernet* de 100 Mbps. En su momento el prefijo *fast* se le agregó para diferenciarlas de la *Ethernet* regular de 10 Mbps. *Fast Ethernet* no es hoy por hoy la más rápida de las versiones de *Ethernet*, siendo actualmente *Gigabit Ethernet* y 10 *Gigabit Ethernet* las más veloces.

FCC — Agencia gubernamental de los EE.UU. para la regularización de las comunicaciones por radio, televisión, cable y satélite.

Firewall — Conjunto de programas de protección y dispositivos especiales que ponen barreras al acceso exterior a una determinada red privada. Es utilizado para proteger los recursos de una organización de consultas externas no autorizadas.

Firmware — Son pequeños programas que, por lo general, vienen en un chip en el *hardware*, como es el caso de la ROM BIOS.

Frame Relay	Protocolo de enlace mediante circuito virtual permanente muy usado para dar conexión directa a *Internet*. Se puede recrear un *frame relay* usando *tunneling*.
FTP	Miembro del conjunto de protocolos TCP/IP que se utiliza para copiar archivos entre dos equipos en Internet. Ambos equipos deben admitir sus funciones FTP correspondientes: uno debe ser un cliente FTP y el otro un servidor FTP.
Gateway	Dispositivo conectado a múltiples redes TCP/IP físicas y capaz de enrutar o transportar paquetes IP de unas a otras. Una puerta de enlace o *gateway* traduce los distintos protocolos de transporte o formatos de datos –por ejemplo IPX e IP– y, generalmente, se agrega a las redes por su capacidad de traducción.
GHz	El *Gigahercio* (GHz) es un múltiplo de la unidad de medida de frecuencia (Hercio) y equivale a 109 hercios.
GPRS	Servicio General de Radio por Paquetes: es una tecnología de paquetes que permite las comunicaciones de datos GSM y por *Internet* inalámbrico de alta velocidad. Hace uso muy eficiente del espectro de radio disponible y los usuarios pagan sólo por el volumen de datos enviados y recibidos.

GPS	*Global Positioning System* o Sistema de Posicionamiento Global: Sistema mundial de navegación por satélite, conformado por 24 satélites orbitando la tierra y sus receptores en la superficie de la tierra. Los satélites GPS, constantemente, transmiten señales digitales de radio, con información utilizada para rastrear ubicaciones, navegación y otras tecnologías de ubicación o mapeo.
GSM	Sistema Global para Comunicaciones Móviles. Sistema compatible de telefonía móvil digital desarrollado en Europa con la colaboración de operadores, administraciones Públicas y empresas. Permite la transmisión de voz y datos. Existe compatibilidad entre redes y, por ende, un teléfono GSM puede funcionar teóricamente en todo el mundo
Header	Parte inicial de un paquete que precede a los datos propiamente dichos y que contiene las direcciones del remitente y del destinatario, control de errores y otros campos.
Hexadecimal	Sistema de numeración en base 16 representado por los dígitos 0 a 9 y las letras mayúsculas o minúsculas de la A –equivalente al valor decimal 10– a la F, equivalente al valor decimal 15.

HiperLAN Es un estándar global para anchos de banda inalámbricos LAN que operan con un rango de datos de 54 Mbps en la frecuencia de banda de 5 GHz.

HiperLAN2 La versión 2 de HiperLAN fue diseñada como una conexión inalámbrica rápida para muchos tipos de redes. Por ejemplo: red *back bone* UMTS, redes ATM e IP. También funciona como una red doméstica como HIPERLAN/1. HIPERLAN/2 usa la banda de 5 GHz y una velocidad de transmisión de hasta 54 Mbps.

Home RF Estándar que se basa en el teléfono inalámbrico digital mejorado –*Digital Enhaced Cordless Telephone*, DECT– que es un equivalente al estándar de los teléfonos celulares GSM. Transporta voz y datos por separado

Host Servidor que provee de la información que se requiere para realizar algún procedimiento desde una aplicación cliente a la que se tiene acceso de diversas formas (ssh, FTP, www, email, etc.). Al igual que cualquier computadora conectada a *Internet*, debe tener una dirección o número IP y un nombre.

HUB El punto central de conexión para un grupo de nodos; útil para la administración centralizada, la capacidad de aislar nodos de problemas y ampliar la cobertura de una LAN.

IEEE — *Institute of Electrical and Electronics Engineers*, organización formada por ingenieros, científicos y estudiantes involucrados en el desarrollo de estándares para, entre otros campos, las comunicaciones. Este organismo utiliza los números y letras en una clasificación jerárquica para diferenciar grupo de trabajo y sus normas. Así, el subgrupo 802 se encarga de las redes LAN y WAN, y cuenta con la subsección 802.11 para las redes WLAN. Más información en http://www.ieee.org.

Infrared — Es una frecuencia en el espectro electromagnético en el rango apenas debajo de la de la luz roja. Los objetos irradian infrarrojo en proporción con su temperatura. La radiación infrarroja se divide en las categorías basadas en longitud de onda.

Internet — La red de computadoras más extendida del planeta, que conecta y comunica a más de 50 millones de personas. Nació a fines de los años sesenta como ARPANet y se convirtió en un revolucionario medio de comunicación. Su estructura técnica se basa en millones de computadoras que ofrecen todo tipo de información. Estas computadoras, encendidas las 24 horas, se llaman servidores y están interconectadas entre sí en todo el mundo a través de diferentes mecanismos de líneas dedicadas. Sin importar qué tipo de computadoras son, para intercomunicarse utilizan el protocolo TCP/IP. Las computadoras que

	utilizan las personas para conectarse y consultar los datos de los servidores se llaman clientes, y acceden en general a través en un tipo de conexión llamado *dial-in*, utilizando un módem y una línea telefónica.
IP	Protocolo de *Internet* definido en el RFC 791. Confirma la base del estándar de comunicaciones de *Internet.* El IP provee un método para fragmentar y rutear la información. Es inseguro, ya que, no verifica que todos los fragmentos del mensaje lleguen a su destino sin perderse en el camino. Por eso, se complementa con el TCP.
IP número o dirección	IP *Address*. Dirección numérica asignada a un dispositivo de hardware conectado a Internet, bajo el protocolo IP. La dirección se compone de cuatro números, y cada uno de ellos puede ser de 0 a 255, las direcciones IP se agrupan en clases.
IPSec	IP *Security*, representa la tendencia a largo plazo hacia las redes seguras, es un conjunto de servicios de protección y protocolos de seguridad basados en criptografía. Como no requiere cambios en los programas o en los protocolos, se puede implementar fácilmente en las redes existentes.
IPX	El Intercambio de paquetes entre redes es un protocolo de red de *NetWare* encargado de dirigir y enrutar los paquetes dentro de las redes de área

	local (LAN) y entre ellas. IPX no garantiza que un mensaje llegue completo, sin pérdida de paquetes.
ISM	*Industrial, Scientific and Medical band,* son bandas de frecuencias reservadas originalmente para uso no comercial con fines industriales, científicos y médicos. Posteriormente, se empezaron a usar para sistemas de comunicación tolerantes a fallos que no necesitaran licencias para la emisión de ondas.
Kbps	Kilobits por segundo. Unidad de medida que comúnmente se usa para medir la velocidad de transmisión por una línea de telecomunicación, como la velocidad de un cable módem por ejemplo.
LAN	*Local Area Network* o Red de área local. Es una red de ordenadores que se extiende en un área relativamente pequeña, generalmente, confinada a un único edificio o a un grupo de edificios.
Laptop	Computadora portátil que pesa aproximadamente dos o tres kilogramos. Existen distintos modelos, desde las *notebooks* comunes hasta las multimedia, dotadas de parlantes, lectora de CD-ROMs, monitor color, etc. Según su capacidad, tienen una autonomía de corriente eléctrica de dos a seis horas de duración. A raíz de que la tecnología compacta es bastante cara, estos equipos suelen costar

prácticamente, el doble que sus pares de escritorio, comparando sistemas de capacidades equivalentes.

Linux Versión *freeware* del conocido sistema operativo Unix. Es un sistema multitarea multiusuario de 32 bits para computadores personales.

Dirección MAC *Media Access Control* o Control de Acceso al Medio. Es una de las dos direcciones que tiene cada ordenador conectado en red, siendo la otra la dirección IP. La dirección de Control de Acceso al Medio es un único identificador de 48-bits que se escribe normalmente como 12 caracteres hexadecimales agrupados en pares (e. g., 00-00-0c-34-11-4e). Normalmente, está dirección es otorgada por el fabricante de la tarjeta de interface de red y no cambia nunca. Representa la dirección física de un dispositivo de datos y se utiliza como una ayuda para los *routers* que tratan de identificar máquinas en grandes redes.

Mbps Megabits por Segundo. Unidad de medida de la capacidad de transmisión por una línea de telecomunicación donde cada megabit está formado por 1.048.576 bits.

MHz Megahertz (MHz) es una unidad de frecuencia equivalente a un millón de *hertz* o ciclos por segundo. Las comunicaciones inalámbricas móviles en los

	Estados Unidos ocurren en las bandas de 800 MHz, 900MHz y 1900MHz.
Microsoft	Compañía creadora de los sistemas operativos Windows 95, 98, NT, 2000, XP; de los controles Active X, y del navegador IE de WWW entre otros recursos. Fundado por Bill Gates. http://www.microsoft.com/
Módem	Dispositivo que permite transmitir y recibir información en un equipo a través de una línea telefónica. El módem transmisor traduce los datos digitales de los equipos a señales analógicas que se pueden transmitir a través de la línea telefónica. El módem de destino vuelve a traducir las señales analógicas recibidas a formato digital.
mW	Unidad de poder en electricidad equivalente a un millón de *watts*.
NetBEUI	Es un acrónimo de *NetBIOS Extended User Interface* –Interface extendida de Usuario de NetBios. Es un protocolo de comunicación utilizado por las antiguas redes basadas en LAN *Manager.* Es muy rápido en pequeñas redes que no lleguen a la decena de equipos y que no muevan ficheros de gran tamaño.
NIC	*Network Interface Card* o Tarjeta de Interface de Red. Dispositivo que envía y recibe datos entre el

	ordenador y el cable de red. Cada ordenador conectado a la red debe estar provisto de una de estas tarjetas.
NIS	*Network Information Service* –Servicio de Información en la Red. Servicio utilizado por administradores UNIX con el objetivo de gestionar bases de datos distribuidas en una red.
Nodo	Cada una de las computadoras individuales u otros dispositivos de la red.
OCDE	Organización para la Cooperación y el Desarrollo Económico (OCDE) es una organización corporación internacional compuesta por 30 países desarrollados cuyo objetivo es coordinar, sus políticas económicas y sociales. Fundada en 1961. La sede central de la OCDE se encuentra en la ciudad de París.
ODBC	Son las siglas de *Open DataBase Connectivity*, un estándar de acceso a Bases de Datos desarrollado por *Microsoft Corporation*, el objetivo de ODBC es hacer posible el acceder a cualquier dato de cualquier aplicación, sin importar qué Sistema Gestor de Bases de Datos –DBMS por sus siglas en Inglés– almacene los datos, ODBC logra esto al insertar una capa intermedia llamada manejador de Bases de Datos, entre la aplicación y el DBMS, el propósito de esta capa es traducir las consultas.

OFDM	*Orthogonal Frequency Division Multiplexing*, técnica de modulación FDM –empleada por el 802.11a wi-fi– para transmitir grandes cantidades de datos digitales a través de ondas de radio. OFDM divide la señal de radio en múltiples subseñales más pequeñas que luego serán transmitidas de manera simultánea en diferentes frecuencias al receptor. OFDM reduce la cantidad de ruido –*crosstalk*– en las transmisiones de señal.
PAN	Conjunto de dispositivos informáticos que una persona puede llevar incorporados en su vestimenta o en su cuerpo, conectados entre sí y con otras redes.
PC	*Personal Computer*, ordenador personal; nombre –registrado– con que bautizó IBM en 1,981 al que se convertiría en estándar de la informática de usuario; por extensión, cualquier ordenador compatible de otra marca basado en principios similares.
PC-*Cards*	Dispositivo extraíble, aproximadamente, del tamaño de una tarjeta de crédito, que se puede conectar a una ranura PCMCIA de un equipo portátil. Los dispositivos PCMCIA pueden ser módems, tarjetas de red y unidades de disco duro.

PCI	*Peripheral Component Interconnect* o Conector de Componentes Periféricos, es una especificación desarrollada por Intel *Corporation* que define un sistema de bus local que permite la instalación de hasta 10 tarjetas de expansión compatibles con PCI en el equipo.
PCMCIA	Tarjeta estandarizada de expansión, del tamaño de una tarjeta de crédito, utilizada en ordenadores personales. En telecomunicaciones, uno de sus principales usos es la transmisión de mensajes, datos y faxes a través de computadoras portátiles y teléfonos móviles.
PDA	*Personal Digital Assistant*, asistente personal digital. En un principio se propuso como una especie de agenda electrónica, para mantener contactos, calendarios de tareas y notas, pero pronto se amplió su capacidad a aspectos muy diversos, como la informática móvil y las aplicaciones multimedia.
Peer to Peer	Red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red. Este modelo de red contrasta con el modelo cliente-servidor la cual se rige de una arquitectura monolítica donde no hay distribución de tareas entre sí, solo una simple comunicación entre

	un usuario y una terminal en donde el cliente y el servidor no pueden cambiar de roles.
Plug and Play	Conjunto de especificaciones desarrolladas por Intel que permiten a un equipo detectar y configurar automáticamente un dispositivo, e instalar los controladores de dispositivo correspondientes.
QAM-64	La Modulación de Amplitud en Cuadratura o QAM es una modulación digital en la que el mensaje está contenido tanto en la amplitud como en la fase de la señal transmitida. Se basa en la transmisión de dos mensajes independientes por un único camino. Esto se consigue modulando una misma portadora, desfasada 90º entre uno y otro mensaje. Esto supone la formación de dos canales ortogonales en el mismo ancho de banda, con lo cual se mejora en eficiencia de ancho de banda que se consigue con esta modulación.
RAS	*Remote Access Server* o Servidor de Acceso Remoto, servidor dedicado a la gestión de usuarios que no están en una red, pero necesitan acceder, remotamente, a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

Red	Grupo de equipos y otros dispositivos, como impresoras y escáneres, conectados mediante un vínculo de comunicaciones, lo que permite la interacción de todos los dispositivos entre sí. Las redes pueden ser grandes o pequeñas, y estar conectadas siempre mediante cables o temporalmente mediante líneas telefónicas o transmisiones inalámbricas. La red más grande es *Internet*, que es un grupo mundial de redes.
RFC	*Requests for Comments*. Serie de documentos iniciada en 1967 la cual describe el conjunto de protocolos de *Internet* y experimentos similares. No todos los RFC –en realidad muy pocos de ellos describen estándares de *Internet* pero todos los estándares *Internet* están escritos en formato RFC.
Roaming	Nombre dado a la acción de moverse del área de cobertura de un Punto de Acceso a otro sin pérdida de conectividad, de forma que el usuario no lo percibe.
Router	Equipo informático conectado a una red con el fin de “encaminar” o dirigir los mensajes a una u otra red, aunque estas sean diferentes. De esta forma, permite la interconexión de varias redes de comunicaciones. Se utiliza para establecer determinadas medidas de seguridad, de forma que se permita o impida el acceso a ciertas redes, o se limite su acceso.

Slot Ranura del ordenador en la que se pueden insertar nuevas tarjetas para ofrecer más utilidades.

Sniffer Programa y/o dispositivo que monitoriza la circulación de datos a través de una red. Los *sniffers* pueden emplearse tanto con funciones legítimas de gestión de red como para el robo de información. Los *sniffers* no autorizados pueden ser extremadamente peligrosos para la seguridad de una red ya que virtualmente es casi imposible detectarlos y pueden ser emplazados en cualquier lugar, convirtiéndolos en un arma indispensable de muchos piratas informáticos.

Switch *Switch* o Conmutador, es un dispositivo de interconexión de redes de ordenadores/computadoras que opera en la capa 2 –nivel de enlace de datos– del modelo OSI –*Open Systems Interconection*. Este interconecta dos o más segmentos de red, funcionando de manera similar a los puentes, *bridges*, pasando datos de una red a otra, de acuerdo con la dirección MAC de destino de los *datagramas* en la red.

TCP *Transmission Control Protocol* o protocolo de control de transmisión. Conjunto de protocolos de comunicación que se encargan de la seguridad y la integridad de los paquetes de datos que viajan por Internet. Complemento del IP en el TCP/IP.

TCP/IP *Transmission Control Protocol / Internet Protocol* o protocolo de control de transmisión / protocolo *Internet*. Usados para organizar computadoras en redes. Norma de comunicación en *Internet*, compuesta por dos partes: el TCP/IP. El IP desarma los envíos en paquetes y los rutea, mientras que el TCP se encarga de la seguridad de la conexión, comprueba que los datos lleguen todos, completos, y que compongan finalmente el envío original.

Tercera generación Más conocido como 3G, es un término general que se refiere a la capacidad incrementada y los datos de alta velocidad, hasta 2 megabits, vía redes digitales inalámbricas y aparatos telefónicos.

TIC Siglas de Tecnologías de la Información y de las Comunicaciones.

TKIP *Temporal Key Integrity Protocol* o Protocolo de Integridad de Clave Temporal, algoritmo empleado por el protocolo WPA para mejorar la encriptación de los datos en redes *wireless*. Sus principales características son la renovación automática de la clave de encriptación de los mensajes y un vector de inicialización de 48 bits, lo que elimina el problema del protocolo WEP.

TLS	*Transport Layer Security*, protocolo del tipo EAP que garantiza la privacidad y la seguridad de datos entre aplicaciones cliente/servidor que se comunican vía *Internet*. Trabaja en dos niveles: El protocolo de registro TLS - situado en el nivel superior de un protocolo de transporte seguro como TCP asegura que la conexión es privada empleado encriptación simétrica de datos y asegura que la conexión es fiable. También se utiliza para la encapsulación de protocolos de nivel superior, tales como el TLS *handshake Protocol*. Y, el protocolo de *handshake* TLS - permite la autenticación entre el servidor y el cliente y la negociación de un algoritmo de encriptación y claves criptográficas antes de que el protocolo de la aplicación transmita o reciba cualquier dato. TLS es un protocolo independiente que permite que protocolos de niveles superiores se sitúen por encima de él de manera transparente
Trama	Conjunto de bits que forman un bloque de datos básico. Generalmente, una trama contiene su propia información de control, en la que se incluye la dirección del dispositivo al que está siendo enviado. Desde uno de los componentes de equipo de red, los cuadros pueden ser unidestinados –enviados a un solo dispositivo– multidestinados –enviados a dispositivos múltiples– o difundidos –enviados a todos los dispositivos.

Túnel	Conexión lógica a través de la que se encapsulan los datos. Normalmente, los datos se encapsulan y se cifran, y el túnel es un vínculo seguro y privado entre un usuario remoto o un host y una red privada.
USAID	Siglas de Agencia para el Desarrollo Internacional de los Estados Unidos.
USB	*Universal Serial Bus* o Bus Serie Universal. Bus externo compatible con instalaciones *Plug and Play*. Con USB, puede conectar y desconectar dispositivos sin tener que cerrar o reiniciar el equipo. Puede utilizar un único puerto USB para conectar hasta 127 dispositivos periféricos, como altavoces, teléfonos, unidades de CD-ROM, *joysticks*, unidades de cinta, teclados, escáneres y cámaras. Los puertos USB suelen encontrarse en la parte posterior del equipo, junto al puerto serie o al puerto paralelo.
UTP	Es un tipo de cableado estructurado –sistema de cableado para redes interiores de comunicaciones– basado en cable de par trenzado sin blindaje –UTP - *Unshielded Twisted Pair*. Se encuentra normalizado de acuerdo a la norma TIA/EIA-568-B.
VLAN	Red de Área Local Virtual. Agrupación lógica de *hosts* en una o varias redes de área local (LAN) que permite la comunicación entre *hosts* como si estuvieran en la misma LAN física.

VSAT	Las redes *Very Small Aperture Terminals* (VSAT) son redes privadas de comunicación de datos vía satélite para intercambio de información punto-punto o, punto-multipunto –*broadcasting*– o interactiva.
WAN	*Wide Area Network* o red de área amplia. Resultante de la interconexión de varias redes locales localizadas en diferentes ciudades o países, comunicadas a través de conexiones públicas.
Wi-Fi	Acrónimo de *Wireless Fidelity*, un estándar de red inalámbrica 802.11. Una red Wi-Fi también se puede usar para permitir la conexión a una red de área local (LAN) mayor, una red de área extensa (WAN) o *Internet*.
WiMax	Siglas de "*Worldwide Interoperability for Microwave Access*", grupo no lucrativo formado en abril de 2003 iniciativa de Intel, Nokia, Fujitsu, entre otras que certifica la interoperabilidad de los productos con tecnología inalámbrica. Más información en http://www.wimaxforum.org.
WLAN	Acrónimo en inglés para *Wireless Local Area Network*. Red inalámbrica de área local permite que un usuario móvil pueda conectarse a una red de área local (LAN) por medio de una conexión inalámbrica de radio.

WWW	*World Wide Web* o W3. Conjunto de servidores que proveen información organizada en *sites*, cada uno con cierta cantidad de páginas relacionadas. La *Web* es una forma novedosa de organizar toda la información existente en *Internet* a través de un mecanismo de acceso común de fácil uso, con la ayuda del hipertexto y la multimedia. El hipertexto permite una gran flexibilidad en la organización de la información, al vincular textos disponibles en todo el mundo. La multimedia aporta color, sonido y movimiento a esta experiencia. El contenido de la *Web* se escribe en lenguaje HTML y puede utilizarse con intuitiva facilidad mediante un programa llamado navegador. Se convirtió en el servicio más popular de la red y se emplea, cotidianamente, para los usos más diversos: desde leer un diario de otro continente hasta participar de un juego grupal.
XOR	Operador a nivel de bits: suma lógica exclusiva, que da como resultado 1 si los dos bits son distintos y 0 si los dos bits son iguales.

RESUMEN

El uso de las redes ha crecido y se ha extendido por todas partes del mundo de forma notoria, todo esto debido a que son eficaces, ya que, todos los usuarios que están conectados a una red sea pública o privada pueden utilizar y compartir los mismos recursos, lo que aumenta la productividad y disminuye costos.

Anteriormente, los cables que conectaban a los equipos eran difíciles de colocar, resultaban antiestéticos, pero actualmente con las redes inalámbricas todo esto se ha vuelto mucho más sencillo y barato.

Las redes inalámbricas van ganando rápidamente adeptos como una tecnología madura y fiable que permite resolver los inconvenientes derivados de la propia naturaleza del cable como medio físico de enlace en las comunicaciones.

Sin embargo, actualmente, las políticas de seguridad para las redes inalámbricas son dejadas por un lado, poniendo en riesgo información crítica para las empresas que utilizan este tipo de redes.

En este trabajo se explican las diversas metodologías para brindar seguridad en redes inalámbricas, teniendo como objetivo guiar en la elección de las tecnologías de seguridad más apropiadas para un proyecto específico. Finalmente, se analiza la situación actual de Guatemala en la implementación de redes inalámbricas.

OBJETIVOS

Generales

- Realizar un análisis de las distintas tecnologías que existen actualmente para brindar seguridad en redes inalámbricas, para guiar en la elección de las tecnologías de seguridad mas optimas para un proyecto específico.

Específicos

1. Dar a conocer las distintas tecnologías para brindar seguridad en redes inalámbricas.
2. Estudiar la seguridad en redes inalámbricas y las soluciones existentes.
3. Realizar un análisis de la infraestructura necesaria para la implementación de las tecnologías de seguridad enfocadas en Guatemala.
4. Evidenciar los problemas que conllevan la utilización de una tecnología no apta para cierto tipo de implementación.
5. Describir las vulnerabilidades a las que se esta expuesto sin un adecuado sistema de seguridad en redes inalámbricas.

INTRODUCCIÓN

En los últimos años las redes de área local inalámbricas –*Wireless Local Area Network* / WLAN– han estado ganando mucha popularidad, que se ve acrecentada conforme sus prestaciones aumentan y se descubren nuevas aplicaciones para ellas.

Por lo general, al implementar un sistema de redes inalámbricas y tratar de asegurar la información que viaja en dicha red, se utiliza el método de cifrado WEP –*Wired Equivalent Privacy*. La utilización frecuente del método de cifrado WEP, surge debido al desconocimiento de otras alternativas que podrían ser más útiles y adaptarse mejor a las características del sistema de red inalámbrico.

Si las características más importantes para asegurar un sistema de red inalámbrico son deficientes, el resultado será el establecimiento de políticas de seguridad deficientes.

Esto se podría evitar, si antes de iniciar la implementación de políticas de seguridad se eligen las metodologías de seguridad en redes inalámbricas adecuadas, las cuales satisfagan las características del sistema de red inalámbrico. Este documento pretende servir de ayuda en la elección de las metodologías de seguridad en redes inalámbricas, dando a conocer las ventajas y desventajas que tienen cada una de las metodologías de seguridad (WEP, WPA, VPN, etc.).

Así, también, muestra la situación de la implementación de redes en el ambiente Guatemalteco, sus potenciales usuarios y el crecimiento de la tecnología inalámbrica en dicho país.

1 REDES INALÁMBRICAS

1.1 ¿Qué es una red inalámbrica?

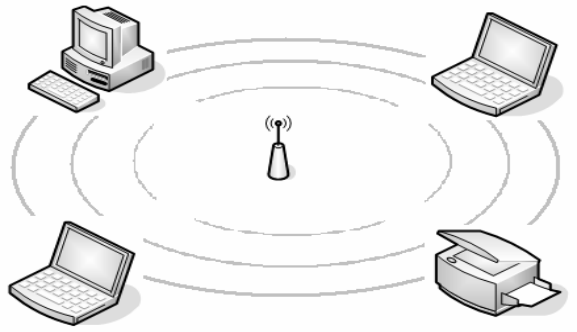
Una definición no muy formal de red inalámbrica podría ser la siguiente: es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a la LAN (*Local Area Network*) cableada o como una extensión de ésta.

Utiliza tecnología de radio frecuencia que permite mayor movilidad a los usuarios al minimizarse las conexiones cableadas. La WLAN (*Wireless Local Area Network*) va adquiriendo importancia en muchos campos donde el estar sin ataduras de cables es algo primordial, como almacenes o empresas de manufacturación, en los que se transmite la información en tiempo real a una terminal central.

También son muy populares en los hogares para compartir un acceso a *Internet* entre varias computadoras.

Una definición más formal podría ser la siguiente: es un sistema de comunicaciones que transmite y recibe datos utilizando ondas electromagnéticas, en lugar del par trenzado, coaxial o fibra óptica utilizado en las LAN convencionales, y que proporciona conectividad inalámbrica de igual a igual (*peer to peer*), dentro de un edificio, de una pequeña área residencial/urbana o de un campus universitario.

Figura 1. Esquema de una red inalámbrica

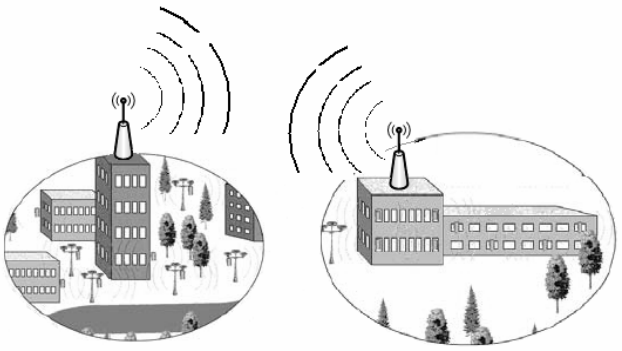


1.1.1 Tipos de redes inalámbricas

1.1.1.1 Red de área ancha (*Wide Area Network* / WAN)

Es un tipo de red que abarca un área geográfica relativamente extensa y permite a múltiples computadoras conectarse en una misma red a través de conexiones satelitales o antenas de radio. Para que la comunidad satelital sea efectiva generalmente se necesita que los satélites permanezcan estacionarios con respecto a su posición sobre la tierra, si no es así, las estaciones en la tierra los perderían de vista.

Figura 2. Ejemplo de una red inalámbrica WAN



Fuente: ***Fundamentals of Wireless LANs v1.1***. www.cisco.com. (06/10/2004)

1.1.1.2 Red de área local (*Local Area Network* / LAN)

Las redes LAN permiten conectar un grupo de computadoras dentro de un área relativamente limitada menor a la de las WAN, para compartir archivos, servicios, impresoras y otros recursos.

En general este tipo de redes utilizan señales de radio para su comunicación, las cuales son captadas por PC *Cards*, tarjetas PCMCIA conectadas a *laptops* o a *slots* PCI para PCMCIA de PC de escritorio.

Este tipo de redes soportan generalmente tasas de transmisión entre los 11 Mbps y 54 Mbps y tienen un rango de entre los 30 a 300 metros, con señales capaces de atravesar paredes.

Figura 3. Ejemplo de una red inalámbrica LAN

Fuente: **Redes Inalámbricas.**
http://www.maestrosdelweb.com/editorial/redeswlan/. (05/07/2004)

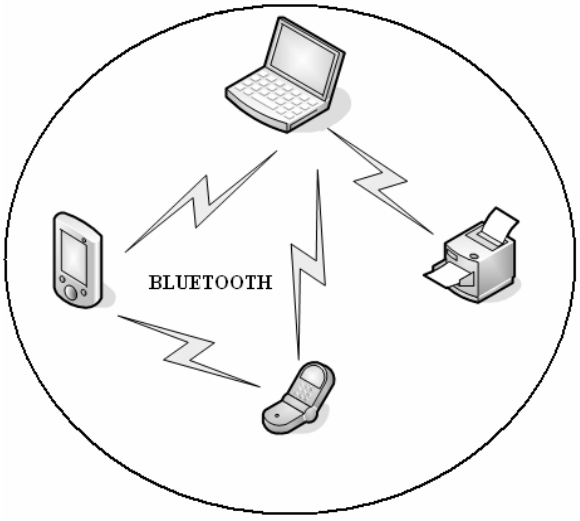
1.1.1.3 Red de área personal (*Personal Area Network* / PAN)

Este tipo de red permite interconectar dispositivos electrónicos dentro de un rango de pocos metros, para comunicar y sincronizar información.

La líder en esta área es el estándar *Bluetooth*, una tecnología de radio de corto alcance (2.4 GHz) que simplifica las comunicaciones entre dispositivos de red y otros ordenadores.

Debido a que no fue diseñada para soportar grandes cargas de tráfico, no es una buena alternativa para sustituir redes locales o amplias.

Figura 4. Ejemplo de una red inalámbrica PAN



1.1.1.4 Tabla comparativa de tecnologías inalámbricas

La siguiente tabla muestra la comparación de las tecnologías inalámbricas más usadas.

Tabla I. Resumen de tipos de redes inalámbricas

	WAN	LAN	PAN
Estándares	GSM, GPRS, CDMA, 2.5-3G	802.11a, 11b, 11g HiperLAN2	*Bluetooth*/Infrared
Ancho de Banda	9.6 a 384 Kbps	2 a 54+ Mbps	< 1 Mbps
Alcance	Largo	Medio	Corto / Muy Corto
Aplicaciones	Telefonia movil, Celular, Satelite, GPS	Redes Corporativas	Domésticas, PDA's, Entorno Oficina

1.1.2 Características principales de una red inalámbrica

1.1.2.1 Basada en estándares

El Wi-Fi (*Wireless Fidelity*) es un robusto estándar de redes, comprobado a nivel de la industria de transmisión de datos, que asegura que los productos inalámbricos ínter-operarán con otros productos certificados con el estándar Wi-Fi de otros fabricantes de redes.

Con un sistema basado en el estándar Wi-Fi, los usuarios gozarán de compatibilidad con el mayor número de productos inalámbricos y evitarán los altos costos y la selección limitada de las soluciones patentadas de un solo fabricante.

Además, la selección de una solución inalámbrica basada en estándares, que sea totalmente ínter-operable con redes *Ethernet* y *Fast Ethernet*, le permitirá al usuario que su red inalámbrica trabaje sin interrupciones con su sistema existente de LAN tradicional.

1.1.2.2 Instalación simple

La solución inalámbrica debe ser del tipo *plug and play*, tomando solamente unos minutos para su instalación.

Al conectar la red inalámbrica, los usuarios empezaran a gozar de inmediato de los servicios en red. Para obtener una instalación aún más fácil, la solución inalámbrica deberá soportar el protocolo de configuración dinámica de *host* (*Dynamic Host Configuration Protocol* / DHCP), el cual asignará automáticamente direcciones IP a los clientes inalámbricos.

En lugar de instalar un servidor DHCP en algún aparato independiente para obtener esta capacidad de ahorro de tiempo, los usuarios deben seleccionar dispositivos inalámbricos (A*ccess Point*, S*witch*, *Hub*, *Router*) que ofrezcan servidores DHCP incorporados.

Si un usuario está agregando un sistema inalámbrico a su red *Ethernet*, sería una buena opción potenciar un punto de acceso a través de cables estándares de *Ethernet*, esto le permitirá hacer que el punto de acceso funcione utilizando un voltaje bajo de corriente en el mismo cable que es usado para transmitir datos: eliminando la necesidad de tener una toma de poder local y un cable para cada dispositivo de puntos de acceso.

1.1.2.3 Robusta y confiable

Considere soluciones inalámbricas robustas que tengan alcances de por lo menos 100 metros. Estos sistemas les ofrecerán a los empleados de una compañía una considerable movilidad dentro sus instalaciones.

Un usuario puede optar por un sistema superior que automáticamente detecte el ambiente, para seleccionar la mejor señal de frecuencia de radio disponible y obtener máximos niveles de comunicaciones entre el punto de acceso y las PC *Cards*.

Para garantizar una conectividad a las velocidades más rápidas posibles (incluyendo largo alcance o ambientes ruidosos) el usuario deberá asegurarse que su nuevo sistema pueda hacer cambios dinámicos de velocidad, basándose en las diferentes intensidades de señal y distancias del punto de acceso.

Además, el usuario debe seleccionar PC *Cards* inalámbricas para computadoras portátiles que ofrezcan antenas retractables para prevenir rupturas durante la movilización de los aparatos.

1.1.2.4 Escalabilidad

Un buen dispositivo inalámbrico (A*ccess Point*, S*witch*, *Hub*, *Router*) deberá soportar aproximadamente 60 usuarios simultáneos, permitiéndole expandir su red con efectividad de costos, con simplemente instalar tarjetas inalámbricas en computadoras adicionales e impresoras listas para ser conectadas a la red.

Las impresoras u otros dispositivos periféricos que no puedan conectarse en red tradicional, se conectan a la red inalámbrica con un adaptador USB inalámbrico o un *Ethernet Client Bridge*.

1.1.2.5 Facilidad de uso

Si un usuario planea conectar múltiples dispositivos inalámbricos a una red existente de cables, considere una solución que ofrezca conexiones automáticas a la red.

Cuando un usuario se desplace fuera de los límites de un dispositivo inalámbrico al campo de otro, una capacidad automática de conexión a la red transferirá sus comunicaciones (sin interrupciones) al siguiente aparato, aún al cruzar límites de *routers*, sin siquiera tener que reconfigurar la dirección IP manualmente.

Esto resulta ser especialmente útil para aquellas compañías con múltiples instalaciones que están conectadas por medio de una red de área amplia (WAN). Como resultado, los usuarios podrán movilizarse libremente (dentro de sus instalaciones y más allá) y permanecer conectados a la red.

1.1.2.6 Seguridad

Si un usuario escoge una solución inalámbrica que ofrezca múltiples niveles de seguridad, incluyendo autenticación de usuarios con por lo menos 40 *bits* de encriptación.

Tanto para su facilidad de uso como para una protección más rigurosa, seleccione una solución superior que automáticamente genere una clave nueva de 128 *bits* para cada sesión de red inalámbrica, sin tener que ingresar la clave manualmente.

Además, el usuario debe considerar un sistema que ofrezca autenticación del usuario, requiriendo que los trabajadores presenten una contraseña antes de acceder la red.

1.2 Principios de las redes inalámbricas de área local (*Wireless Local Area Network* / WLAN)

1.2.1 Clasificación según normalización IEEE

En 1989, en el seno de IEEE 802, se forma el comité IEEE 802.11, que empieza a trabajar para tratar de generar una norma para las WLAN, pero no es hasta 1994 cuando aparece el primer borrador, y habría que esperar hasta el año 1999 para dar por finalizada la norma.

Actualmente son cuatro los estándares reconocidos dentro de esta familia; en concreto, la especificación 802.11 original; 802.11a, que define una conexión de alta velocidad basada en ATM; 802.11b, el que goza de una más amplia aceptación y que aumenta la tasa de transmisión de datos propia de 802.11 original, y 802.11g, compatible con él, pero que proporciona aún mayores velocidades.

1.2.1.1 Estándar WLAN 802.11a

El IEEE ratificó en julio de 1999 el estándar 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.

Debido al alcance limitado a 50 metros, esto implica tener que montar más puntos de acceso (*Access Points*) que si se utilizará 802.11b para cubrir la misma área, con el coste adicional que ello supone.

La banda de 5 GHz que utiliza se denomina UNII (Infraestructura de Información Nacional sin Licencia), que en los Estados Unidos está regulada por la FCC, a la cual ha asignado un total de 300 MHz, cuatro veces más de lo que tiene la banda ISM, para uso sin licencia, en tres bloques de 100 MHz, siendo en el primero la potencia máxima de 50 mW, en el segundo de 250 mW, y en el tercero puede llegar hasta 1W, por lo que se reserva para aplicaciones en el exterior.

1.2.1.2 Estándar WLAN 802.11b

Un poco más tarde, en el año 1999, se aprobó el estándar 802.11b, una extensión del 802.11 para WLAN empresariales, con una velocidad de 11 Mbit/s (otras velocidades normalizadas a nivel físico son: 5.5 - 2 y 1 Mbit/s) y un alcance de 100 metros.

Este tipo de estándar al igual que *Bluetooth* y *Home RF*, también emplea la banda de ISM de 2.4 GHz, pero en lugar de una simple modulación de radio digital y salto de frecuencia (FH / *Frequency Hopping*), utiliza una la modulación linear compleja (DSSS).

Permite mayor velocidad, pero presenta una menor seguridad, y el alcance puede llegar a los 100 metros, suficientes para un entorno de oficina o residencial.

1.2.1.3 Estándar WLAN 802.11g

El IEEE también ha aprobado en el año 2003 en el estándar 802.11g, compatible con el 802.11b, capaz de alcanzar una velocidad doble, es decir hasta 22 Mbit/s o llegar, incluso a 54 Mbit/s, para competir con los otros estándares que prometen velocidades mucho más elevadas pero que son incompatibles con los equipos 802.11b ya instalados, aunque pueden coexistir en el mismo entorno debido a que las bandas de frecuencias que emplean son distintas. Por extensión, también se le llama Wi-Fi.

1.3 *Hardware* necesario para crear redes inalámbricas

1.3.1 Puntos de acceso

La infraestructura de un punto de acceso es simple: "Guardar y Repetir", son dispositivos que validan y retransmiten los mensajes recibidos. Estos dispositivos pueden colocarse en un punto en el cual puedan abarcar toda el área donde se encuentren las estaciones. Las características a considerar son:

- La antena del repetidor debe de estar a la altura del techo, esto producirá una mejor cobertura que si la antena estuviera a la altura de la mesa.

- La antena receptora debe de ser más compleja que la repetidora, así aunque la señal de la transmisión sea baja, ésta podrá ser recibida correctamente.

Una red inalámbrica se crea con uno o más puntos de acceso que actúan como *hubs*, enviando y recibiendo señales de radio desde o hacia computadoras personales equipadas con PC *Cards* inalámbricas para clientes.

El punto de acceso puede ser un aparato en sí que forma parte de la base de la red o se conecta por medio de cables a una red de área local (LAN) convencional. Los usuarios pueden enlazar múltiples puntos de acceso a una LAN, creando segmentos inalámbricos en todas sus instalaciones.

Figura 5. Punto de Acceso Inalámbrico

Fuente: ***Wireless Access Point*.**
http://www.3com.com/products/en_US/detail.jsp?tab=features&3C12058. (11/07/2006)

1.3.2 PC *Cards*

Para comunicarse con el punto de acceso, cada computadora portátil o de escritorio necesita una tarjeta especial para redes inalámbricas.

Al igual que las tarjetas de interfaz para redes (NICs) de las redes tradicionales, estas tarjetas permiten que los aparatos se comuniquen con el punto de acceso.

Se instalan fácilmente en las ranuras PC de las computadoras portátiles, las ranuras PCI de los dispositivos de escritorio, o se enlazan a puertos USB.

Una característica exclusiva que presenta la PC *Card* inalámbrica de uno de los fabricantes líder, es una pequeña antena que se retrae cuando no se encuentra en uso. Esto resulta muy beneficioso, dado el nivel de movilidad de las computadoras portátiles. Además, un usuario puede conectar cualquier otro dispositivo que no tenga una ranura para Tarjetas PC o PCI a su red inalámbrica.

Cuando elija una tarjeta de red, deberá considerar lo siguiente:

- La velocidad de su concentrador, conmutador o servidor de impresora *Ethernet* (10 Mbps) o *Fast Ethernet* (100 Mbps).

- La distancia a la cual estarán ubicados los puntos de acceso.

- La capacidad de recepción que tenga la tarjeta, la capacidad de recepción puede variar dependiendo de cada fabricante.

Tabla II. Comparativa entre dispositivos inalámbricos

	Dispositivos PCI	Dispositivos USB	Dispositivos PCMCIA
Portabilidad	Escasa	Alta	Alta
Configuración	Media	Alta	Media
Soporte	Medio	Alta	Alta

1.3.2.1 Dispositivos PCI

Las tarjetas de red inalámbricas PCI (Interconexión de componente periférico) se utilizan en todos las computadoras de escritorio regularmente. Este tipo de tarjeta al igual que otros tipos de tarjetas se insertan en los *slots* (ranuras) de la computadora, y se coloca la antena que sobresale de la tarjeta en un lugar óptimo para recibir la señal, es recomendado colocar la antena receptora en un lugar sin obstáculos o posibles interferencias.

Figura 6. Dispositivo PCI

Fuente: ***Fundamentals of Wireless LANs v1.1***. www.cisco.com. (06/10/2004)

1.3.2.2 Dispositivos USB

Las tarjetas USB se pueden utilizar ya sea en computadoras de escritorio o computadoras portátiles, este tipo de tarjetas han surgido de la necesidad de la portabilidad.

Para colocar una tarjeta de este tipo simplemente hay que conectarla al puerto USB correspondiente y se tendrá una tarjeta de red lista para ser utilizada, mientras que las tarjetas PCI para su colocación requieren de destapar el case (caja contenedora de todos los dispositivos de la computadora como disco duro, CD-ROM, memoria, etc.) del computador para poder insertarla en un *slot* disponible.

Figura 7. Dispositivo USB

Fuente: ***Wireless* USB.**
http://www.3com.com/products/en_US/detail.jsp?tab=features&3C10055. (11/07/2006)

1.3.2.3 Dispositivos PCMCIA

Este tipo de tarjetas son utilizadas para las computadoras portátiles, ya que este tipo de computadoras por su compacto tamaño necesitan de tarjetas igualmente compactas.

Figura 8. Dispositivo PCMCIA

Fuente: ***Wireless* PC *Card*.**
http://www.3com.com/products/en_US/detail.jsp?tab=features&3CRGPC10075. (11/07/2006)

1.4 Modos de operación para las redes inalámbricas

Las configuraciones o arquitecturas de red que pueden generarse con las WLAN's, son diversas debido a que los estándares IEEE802.11 e *HiperLAN*, son capaces de soportar diferentes configuraciones en función de cómo sean los equipos y requerimientos de cada sistema. Así la complejidad, la capacidad y la exigencia de servicio determinan el tipo de arquitectura a elegir.

Las redes inalámbricas pueden construirse con o sin Punto de Acceso (AP), esto es lo que determina si es una "Infraestructura" o una "*Ad-Hoc*" respectivamente.

1.4.1 Modo de operación *Ad-Hoc*

La configuración de red más básica de una WLAN es la llamada de igual a igual o *Ad-Hoc*. Esta consiste en una red de dos o más terminales móviles equipados con la correspondiente tarjeta de red inalámbrica, de forma que la comunicación se establece entre los nodos, comunicándose directamente entre sí.

Para que la comunicación entre estaciones sea posible hace falta que se vean mutuamente de manera directa, es decir, que cada una de ellas esté en el rango de cobertura radioeléctrica de la otra.

Las redes de tipo *Ad-Hoc* son muy sencillas de implementar y no requieren ningún tipo de gestión administrativa. La coordinación se da de forma distribuida, ya que son las estaciones las encargadas de la gestión de la comunicación.

Es una configuración muy flexible, pero requiere un número no elevado de terminales y gran control de potencia que evite alta interferencia y radiación. Un ejemplo de ello puede ser un grupo de usuarios, con portátiles en una sala de reuniones.

Figura 9. Topología de red modo Ad-Hoc

Fuente: **Diseño de las redes WLAN, topologías.**
http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/topologias.htm. (30/01/2002)

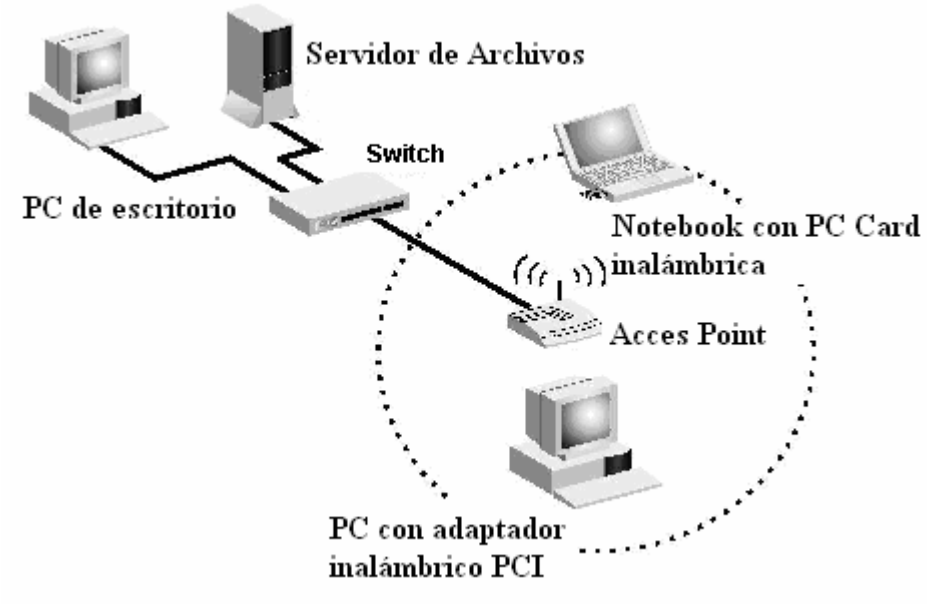
1.4.2 Modo de operación infraestructura

Para aumentar el alcance de una red del tipo *Ad-Hoc* hace falta la instalación de un punto de acceso (*Access Point* / AP). Con este nuevo elemento se logra doblar el alcance de la red inalámbrica (ahora la distancia máxima permitida conexiones no solo entre estaciones, sino entre cada estación y el punto de acceso).

Además, los puntos de acceso se pueden conectar a otras redes, y en particular a una red fija, con lo cual un usuario puede tener acceso desde su terminal móvil a otros recursos de la red cableada, esta disposición se denomina cableada.

Para dar cobertura en una zona determinada habrá que instalar varios puntos de acceso, con antenas omnidireccionales, para así poder cubrir la superficie necesaria con las celdas de cobertura que proporciona cada punto de acceso y ligeramente solapadas para permitir el paso de una celda a otra sin perder la comunicación (*roaming*).

Figura 10. Topología de red de infraestructura



Fuente: **Diseño de las redes WLAN, topologías.**
http://lwwa175.servidoresdns.net:9000/proyectos_wireless/Web/topologias.htm. (30/01/2002)

2 MÉTODOS DE CIFRADO Y AUTENTICACIÓN

2.1 Métodos de cifrado

La seguridad en la transferencia de información es un aspecto que cobra especial relevancia cuando se habla de redes inalámbricas. Para tener acceso a una red cableada es imprescindible una conexión física al cable de la red. Sin embargo, en una red inalámbrica desplegada en una oficina un tercero podría acceder a la red sin ni siquiera estar ubicado en las dependencias de la empresa, bastaría con que estuviese en un lugar próximo donde le llegase la señal.

Es por ello que con el tiempo se han descubierto métodos los cuales tienen como función principal el cifrado de la información que viaja en las redes inalámbricas.

2.1.1 Privacidad equivalente al cable (*Wired Equivalent Privacy* / WEP)

WEP es el algoritmo opcional de seguridad para brindar protección a las redes inalámbricas, incluido en la primera versión del estándar IEEE 802.11, mantenido sin cambios en las nuevas 802,11a y 802.11b, con el fin de garantizar compatibilidad entre distintos fabricantes.

El WEP es un sistema de encriptación estándar implementado en la MAC y soportado por la mayoría de las soluciones inalámbricas.

WEP está diseñado para evitar el acceso a una red por parte de intrusos que cuenten con computadoras dotadas de dispositivos inalámbricos compatibles capaces de examinar el tráfico que fluye a través de la red.

2.1.1.1 Funcionamiento de WEP

WEP utiliza una clave secreta compartida entre una estación inalámbrica y un punto de acceso.

Todos los datos enviados y recibidos entre la estación y el punto de acceso pueden ser cifrados utilizando esta clave compartida.

El estándar 802.11 no especifica cómo se establece la clave secreta, pero permite que haya una tabla que asocie una clave exclusiva con cada estación. En la práctica general, sin embargo, una misma clave es compartida entre todas las estaciones y puntos de acceso de un sistema dado.

Para proteger el texto cifrado frente a modificaciones no autorizadas mientras está en tránsito, WEP aplica un algoritmo de comprobación de integridad (CRC-32) al texto en claro, lo que genera un valor de comprobación de integridad (conocido como ICV por sus siglas en inglés). Dicho valor de comprobación de integridad se concatena con el texto en claro.

El valor de comprobación de integridad es, de hecho, una especie de huella digital del texto en claro. El valor ICV se añade al texto cifrado y se envía al receptor junto con el vector de inicialización.

El receptor combina el texto cifrado con el flujo de clave para recuperar el texto en claro. Al aplicar el algoritmo de integridad al texto en claro y comparar la salida con el vector ICV recibido, se puede verificar que el proceso de descifrado ha sido correcto o que los datos han sido corrompidos.

Si los dos valores de ICV son idénticos, el mensaje será autenticado, en otras palabras las huellas digitales coinciden.

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red.

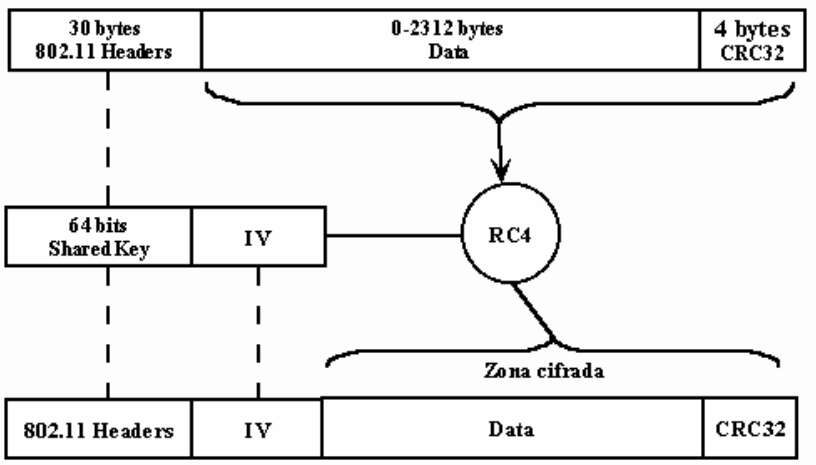
De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN.

Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (*challenge*). La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse.

El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red.

Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

Figura 11. Algoritmo de encriptación de WEP



Fuente: **Protocolo de seguridad WEP.**
http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml. (30/09/2005)

2.1.1.2 Características de WEP

De acuerdo con el estándar, WEP debe proporcionar confidencialidad, autentificación y control de acceso en redes WLAN.

WEP utiliza una misma clave simétrica y estática en las estaciones y el punto de acceso. El estándar no contempla ningún mecanismo de distribución automática de claves, lo que obliga a escribir la clave manualmente en cada uno de los elementos de red.

Esto genera varios inconvenientes, por un lado, la clave está almacenada en todas las estaciones, aumentando las posibilidades de que sea comprometida. Y por otro, la distribución manual de claves provoca un aumento de mantenimiento por parte del administrador de la red, lo que conlleva, en la mayoría de ocasiones, que la clave se cambie poco o nunca.

2.1.1.3 Vulnerabilidades de WEP

La implementación del vector de inicialización (IV por sus siglas en inglés) en el algoritmo WEP tiene varios problemas de seguridad. Ya que el vector de inicialización (IV) es la parte que varía de la clave para impedir que un posible atacante recopile suficiente información cifrada con una misma clave.

Sin embargo, el estándar 802.11 no especifica cómo manejar el vector de inicialización (IV), se indica que debería cambiarse en cada trama para mejorar la privacidad, pero no obliga a ello.

Queda abierta a los fabricantes la cuestión de cómo variar el IV en sus productos. La consecuencia de esto es que buena parte de las implementaciones optan por una solución sencilla: cada vez que arranca la tarjeta de red, se fija el IV a 0 y se incrementa en 1 para cada trama.

Esto ocasiona que las primeras combinaciones de IVs y clave secreta se repitan muy frecuentemente. Más aún, si se tiene en cuenta que cada estación utiliza la misma clave secreta, por lo que las tramas con igual clave se multiplican en el medio.

Por otro lado, el número de IVs diferentes no es demasiado elevado (2^{24}), por lo que terminarán repitiéndose en cuestión de minutos u horas.

El tiempo será menor cuanto mayor sea la carga de la red. Lo ideal sería que el IV no se repitiese nunca, pero como se ve, esto es imposible en WEP.

La cantidad de veces que se repite un mismo IV dependerá de la implementación elegida para variar el IV por el fabricante (secuencial, aleatoria, etc.) y de la carga de la red.

2.1.2 Acceso protegido Wi-Fi (Wi-Fi *Protected Access* / WPA)

WPA es un sistema para asegurar redes inalámbricas (Wi-Fi), creado para corregir las vulnerabilidades del sistema WEP. WPA implementa la mayoría del estándar IEEE 802.11i, y fue creado como una medida intermedia para ocupar el lugar de WEP mientras 802.11i era preparado.

2.1.2.1 Características de WPA

Las principales características de WPA son la distribución dinámica de claves, utilización más robusta del vector de inicialización (mejora de la confidencialidad) y nuevas técnicas de integridad y autentificación.

- Aparece como solución provisional a la aprobación final de 802.11i (WPA2).
- También conocido como WEP2.
- Distribución dinámica de claves: duración limitada (TKIP).
- Vector de inicialización más robusto: 48 bits, minimizando la reutilización de claves.
- Técnicas de integridad y autenticación.

2.1.2.2 Mejoras de WPA con respecto a WEP

Una de las mejoras sobre WEP es dado por el Protocolo de Integridad de Clave Temporal (*Temporal Key Integrity Protocol* / TKIP), que cambia claves dinámicamente a medida que el sistema es utilizado.

Cuando esto se combina con un vector de inicialización (IV) mucho mas grande, evita los ataques de recuperación de clave (ataques estadísticos) a los que es susceptible WEP.

Adicional a la autenticación y cifrado, WPA también mejora la integridad de la información cifrada.

El chequeo de redundancia cíclica (*Cyclic Redundancy Check* / CRC) utilizado en WEP es inseguro, ya que es posible alterar la información y actualizar el CRC del mensaje sin conocer la llave WEP.

WPA implementa un chequeo de integridad del mensaje (*Message Integrity Check* / MIC) que recibe el nombre "Michael".

Adicionalmente WPA incluye protección contra ataques de repetición (*replay attacks*), ya que incluye un contador de tramas.

2.1.2.3 Protocolo de cifrado TKIP

Con este protocolo se pretende resolver las deficiencias del algoritmo WEP y mantener la compatibilidad con el hardware utilizado actualmente mediante una actualización del *firmware*.

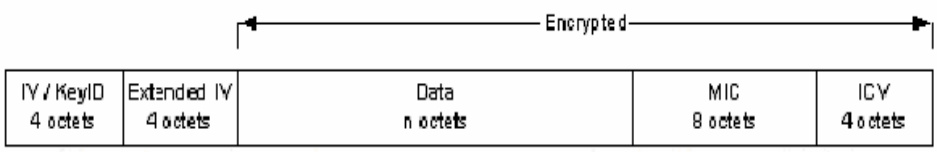
El protocolo de Integridad de Clave Temporal (TKIP) está compuesto por los siguientes elementos:

- Un código de integración de mensajes (MIC), encripta el *checksum* incluyendo las direcciones físicas (MAC) del origen y del destino y los datos en texto claro de la trama 802.11. Esta medida protege contra los ataques por falsificación.

- Contramedidas para reducir la probabilidad de que un atacante pueda aprender o utilizar una determinada llave.

- Utilización de un IV (vector de inicialización) de 48 bits llamado TSC (TKIP *Sequence Counter*) para proteger la red contra ataques por repetición, descartando los paquetes recibidos fuera de orden.

Figura 12. Estructura de encriptación de TKIP



Fuente: **Seguridad en redes inalámbricas**.
www.shellsec.net/documentacion.php?id=6. (20/09/2005)

2.1.2.4 Modos de funcionamiento

Según la complejidad de la red, un punto de acceso compatible con WPA puede operar en dos modalidades:

- **Modalidad de red empresarial**: Para operar en esta modalidad se requiere de la existencia de un servidor *RADIUS* en la red. El punto de acceso emplea entonces 802.1x y EAP para la autenticación, y el servidor RADIUS suministra las claves compartidas que se usarán para cifrar los datos.

- **Modalidad de red casera, o PSK (*Pre-Shared Key* / PSK):** WPA opera en esta modalidad cuando no se dispone de un servidor RADIUS en la red. Se requiere entonces introducir una contraseña compartida en el punto de acceso y en los dispositivos móviles. Solamente podrán acceder al punto de acceso los dispositivos móviles cuya contraseña coincida con la del punto de acceso. Una vez logrado el acceso, TKIP entra en funcionamiento para garantizar la seguridad del acceso. Se recomienda que las contraseñas empleadas sean largas (20 o más caracteres), porque ya se ha comprobado que WPA es vulnerable a ataques de diccionario si se utiliza una contraseña corta.

2.1.3 WPA2

WPA2 incluye el nuevo algoritmo de cifrado AES (*Advanced Encryption Standard*), desarrollado por el NIS.

Se trata de un algoritmo de cifrado de bloque que utiliza a su vez el algoritmo RC4 con claves de 128 bits. Requerirá un hardware potente para realizar sus algoritmos. Este aspecto es importante puesto que significa que dispositivos antiguos sin suficientes capacidades de proceso no podrán incorporar WPA2.

2.1.3.1 Sistema de integridad CCMP

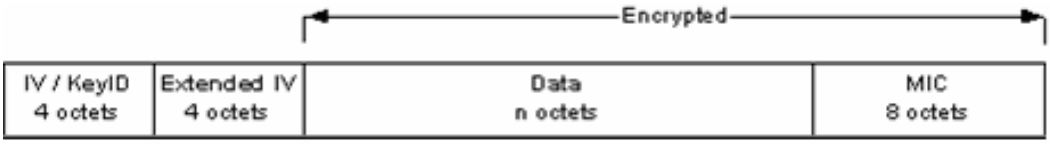
CCMP (*Counter Mode with CBC-MAC Protocol*) es un protocolo complementario al TKIP (*Temporal Key Integrity Protocol*) y representa un nuevo método de encriptación basado en AES (*Advanced Encryption Standards*), cifrado simétrico que utiliza bloques de 128 bits, con el algoritmo CBC-MAC.

Así como el uso del TKIP es opcional, la utilización del protocolo CCMP es obligatorio si se está utilizando 802.11i.

AES (*Advanced Encryption Standard*), es un algoritmo simétrico de bloque con claves de 128 bits. La implementación de este algoritmo es la causa de requerir hardware más potente. Se requiere un nuevo chip en las tarjetas para la criptografía necesaria de este protocolo.

En la siguiente figura se puede observar el formato tras la encriptación CCMP:

Figura 13. Estructura de encriptación CCMP



Fuente: **Seguridad en redes inalámbricas**.
www.shellsec.net/documentacion.php?id=6. (20/09/2005)

CCMP utiliza un IV de 48 bits denominado Número de Paquete (PN) utilizado a lo largo del proceso de cifrado, junto con la información para inicializar el cifrado AES para calcular el código de integración de mensajes (MIC) y la encriptación de la trama.

En el proceso de encriptación CCMP, la encriptación de los bloques utiliza la misma llave temporal tanto para el cálculo del MIC como para la encriptación del paquete.

Como en TKIP, la llave temporal se deriva de la llave principal obtenida como parte del intercambio en 802.1x. Cabe destacar que, el cálculo del MIC y la encriptación se realizan de forma paralela.

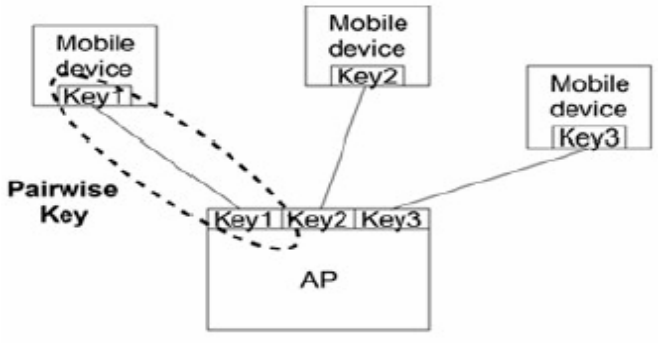
El MIC se calcula a partir de un IV formado por el PN y datos extraídos de la cabecera de la trama. El IV se convierte en un bloque AES y su salida a través de la operación XOR conformará el siguiente bloque AES.

2.1.3.2 Tipos de claves

Para la gestión de claves, WAP2 incluye dos tipos:

- ***Pairwise Key Hierarchy*** **(PKH):** Funciona del Punto de Acceso hacia el cliente o punto a punto.

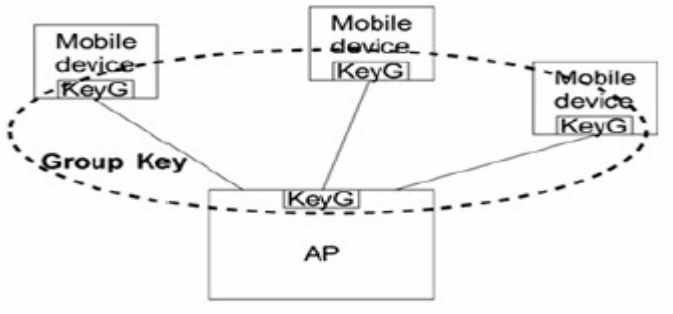
Figura 14. Funcionamiento de PKH



Fuente: **Seguridad en redes Wi-Fi**.
http://inestable.org/files/SeguridadWiFiInestable2005-1.pdf. (30/01/2005)

- ***Group Key Hierarchy* (GKH):** Funciona del Punto de Acceso a todos los clientes o broadcasting.

Figura 15. Funcionamiento de GKH



Fuente: **Seguridad en redes Wi-Fi**.
http://inestable.org/files/SeguridadWiFiInestable2005-1.pdf. (30/01/2005)

2.1.4 Tabla comparativa entre los métodos de cifrado

La siguiente tabla muestra la comparación de algunos de los métodos de cifrado más usados.

Tabla III. Comparativa de métodos de cifrado

	WEP	WPA	WPA2
Cifrado	RC4	RC4	AES
Tamaño de la llave	40 Bits	128 Bits de Encripción y 64 Bits de Autenticación	128 Bits
Vida de la llave	24 Bit-IV	48 Bit-IV	48 Bit-IV
Empaquetada	Concatenada	Función de mezclar	No necesita
Integridad de los datos	CRC-32	Michael	CCM
Integridad de la cabecera	Ninguno	Michael	CCM
Ataques por repetición	Ninguno	Secuencia de IV	Secuencia de IV
Administración de llaves	Ninguno	Basado en EAP	Basado en EAP

2.2 Métodos de autenticación

2.2.1 Protocolo de autenticación extensible (Extensible Authentication Protocol / EAP)

EAP es el protocolo que realiza la autenticación de los usuarios según un determinado mecanismo, en función de las distintas variantes que existen de este protocolo.

Utilizando 802.1X se evita que la asociación de usuarios no autorizados con cualesquiera de los puntos de acceso de la red.

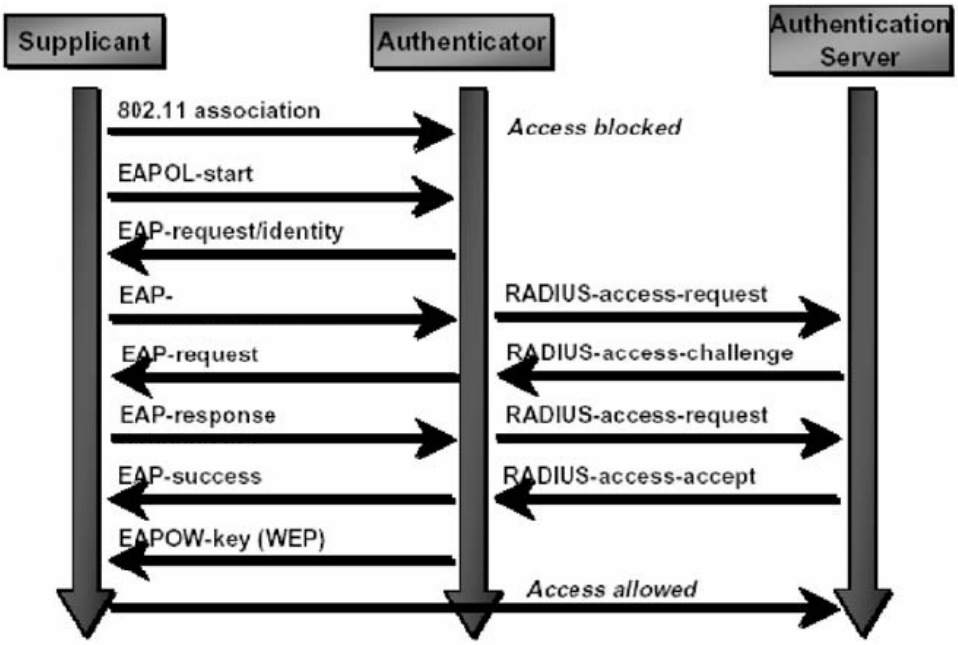
Antes de permitir que un usuario se asocie con un punto de acceso, éste debe proporcionar una identificación (usuario/contraseña, certificado, etc.) válida dentro de la base de datos de usuarios de la red.

De esta forma se evita el posible ataque a elementos de red por parte de cualquier usuario no autorizado.

2.2.1.1 Funcionamiento de EAP

El proceso de autenticación que se sigue antes de dar acceso a la red a un usuario autorizado se muestra en la siguiente figura.

Figura 16. Funcionamiento de EAP con 802.11



Fuente: **Soluciones de seguridad en redes inalámbricas**. http://portal.astic.es/NR/rdonlyres/3429B178-FC84-4A1C-BF99-05FDE7AED4D7/0/mono04.pdf. (01/12/2004)

2.2.1.2 Tipos de mensajes EAP

El protocolo EAP permite cuatro tipos de mensajes, los cuales forman parte del proceso de autenticación de un usuario específico.

- **Petición (*Request Identity*):** usado para el envío de mensajes del punto de acceso al cliente.

- **Respuesta (*Identity Response*):** usado para el envío de mensajes del cliente al punto de acceso.

- **Éxito (*Success*):** enviado por el punto de acceso para indicar que el acceso está permitido.

- **Fallo (*Failure*):** enviado por el punto de acceso para el rechazo del acceso.

2.2.2 Protocolos de autenticación basados en EAP

2.2.2.1 EAP – TLS

Estándar de autenticación que utiliza certificados tanto en servidor como en cliente. Utiliza túneles TLS encriptados para el intercambio de claves públicas, definido según RFC 2176.

Esta es una solución completa basada en certificados, siendo un estándar independiente de la tarjeta del cliente, sistema operativo o RADIUS utilizado.

2.2.2.2 EAP – MD5

En este tipo de autenticación se emplea un nombre de usuario y una contraseña para el proceso de autenticación. La contraseña se transmite cifrada con el algoritmo MD5.

Su gran inconveniente consiste en el bajo nivel de seguridad que maneja, ya que es susceptible a ataques de diccionario (un atacante puede ensayar a cifrar múltiples contraseñas con MD5 hasta que encuentre una cuyo texto cifrado coincida con la contraseña cifrada capturada anteriormente).

Además, el cliente no tiene manera de autenticar al servidor (no se podría garantizar que el cliente se está conectando a la red adecuada) y el esquema no es capaz de generar claves WEP dinámicas. Por estos problemas, EAP-MD5 ha caído en desuso.

2.2.2.3 EAP – PEAP

Propuesta realizada por *Cisco* y *Microsoft* para simplificar los requisitos necesarios que inicialmente necesita EAP-TLS. Solución válida en entornos *Cisco-Microsoft*, pero todavía no está soportada por la mayoría de los fabricantes.

Este tipo de solución se ajusta a entornos empresariales que aún no disponen de la posibilidad de tener un certificado digital en cada uno de las computadoras de la red, realizando la autenticación de usuarios contra un servidor Windows (*Active Directory* o *Windows NT*), RADIUS o incluso contra los puntos de acceso de *Cisco* (solución limitada a 50 usuarios).

2.2.2.4 EAP – TTLS

Actualmente este tipo de autenticación se encuentra en estado de borrador, pretende ser una simplificación de EAP-TLS evitando la utilización de certificados en los clientes, utilizando, por ejemplo, la autenticación de usuario/contraseña del dominio de *Windows* para autorizar a los clientes.

2.2.2.5 EAP – LEAP

Protocolo de autenticación propietario de *Cisco Systems* que permite la autenticación de usuarios y servidor sin la necesidad de utilizar certificados digitales, únicamente utiliza autenticación mediante usuario/contraseña, la cual puede ser válida dentro de la base de datos de otro servidor (*Windows NT*, *Windows Active Directory*, ODBC).

2.2.3 Kerberos

Kerberos es un servicio de autenticación desarrollado en MIT (*Massachusetts Institute of Technology*), diseñado por Miller y Neuman en el contexto del proyecto *Athena* en 1987. Esta basado en el protocolo de distribución de claves presentado por Needham y Schroeder en 1978.

2.2.3.1 ¿Qué hace kerberos?

Cada usuario tendrá una clave y cada servidor tendrá una clave, y Kerberos tiene una base de datos que las contendrá a todas.

En el caso de ser un usuario, la clave será derivada de su contraseña y estará encriptada, mientras que en el caso del servidor, la clave se generará aleatoriamente.

Los servicios de red que requieren autenticación y los usuarios que requieran estos servicios, se deben registrar con Kerberos. Las claves privadas se negocian cuando se registran.

Como Kerberos administra todas las claves privadas, puede crear mensajes que validen en un servidor que un usuario es realmente quien dice ser y viceversa.

La otra función de Kerberos es generar las llamadas claves de sesión, que serán compartidas entre un cliente y un servidor, y nadie más. La clave de sesión podrá ser usada para encriptar mensajes que serán intercambiados entre ambas partes.

El almacenamiento de la base de datos y la generación de claves, se lleva a cabo en un servidor que se denomina Servidor de Autenticación (AS por las siglas en inglés de *Authentication Server*).

2.2.3.2 Niveles de protección que ofrece kerberos

2.2.3.2.1 Autenticación

La autenticación es el proceso para establecer que el usuario es quien dice ser. Puede ser que la autenticidad se establezca al inicio de la conexión de red y luego se asuma que los siguientes mensajes de una dirección de red determinada se originan desde la parte autenticada.

2.2.3.2.2 Integridad de datos

Asegura que los datos no se modifican en el traslado de una computadora a otra. Se requiere autenticación de cada mensaje, sin importar el contenido del mismo, estos se denominan mensajes seguros.

2.2.3.2.3 Privacidad de datos

Asegura que los datos no son leídos durante la comunicación de una computadora con otra. En este caso no sólo se autentica cada mensaje sino que también se encripta, a este tipo de mensajes se les denomina mensajes privados.

2.2.4 Tabla comparativa de los métodos de autentificación

La siguiente tabla muestra la comparación de algunos de los métodos de autentificación más usados.

Tabla IV. Comparativa de métodos de autentificación

	EAP-LEAP	EAP-TLS	EAP-TTLS	EAP-PEAP
Soporte de RADIUS	Cisco, FreeRadius (LINUX), Funk, Interlink, Meetinghouse, Radiator	Cisco, FreeRadius (LINUX), Funk, Interlink, Meetinghouse, Radiator, Microsoft	Funk, Interlink, Meetinghouse, Radiator	Cisco, Funk, Interlink, Meetinghouse, Microsoft, Radiator
Soporte en Cliente	Cisco, Funk, Meetinghouse	Cisco, Funk, Meetinghouse, Microsoft, Open1X	Alfa-Ariss, Funk, Meetinghouse, Open1X	Funk, Meetinghouse, Microsoft
Sistemas Operativos Embebidos	Ninguno	Windows XP/2000/2003	Ninguno	Windows XP/2000/2003
Plataformas soportadas con Software de Terceros	Win32	MacOS X, BSD, Linux, Win32	MacOS X, BSD, Linux, Win32	Win32
Autenticación de Servidor	*Password Hash*	Clave pública (certificado)	Clave pública (certificado))	Clave pública (certificado)
Autenticación de Cliente	*Password Hash*	Clave pública (certificado o tarjeta inteligente)	CHAP, PAP, MS-CHAP(v2), EAP	Cualquier EAP, como EAP-MS-CHAP(v2) o clave pública
Claves dinámicas	Si	Si	Si	Si

Fuente: **Soluciones de seguridad en redes inalámbricas**. http://portal.astic.es/NR/rdonlyres/3429B178-FC84-4A1C-BF99-05FDE7AED4D7/0/mono04.pdf. (01/12/2004)

3 MÉTODO DE REDES PRIVADAS VIRTUALES

3.1 ¿Qué es una VPN?

Una red privada virtual (*Virtual Private Network* / VPN) proporciona, mediante procesos para encapsular y cifrar, una red de datos privada sobre infraestructuras de telecomunicaciones públicas, como *Internet*.

Las VPNs logran la seguridad de una red privada al permitir que se realice un túnel seguro, a través de una red pública de tal forma que permita a los participantes del túnel disfrutar de la misma seguridad y funciones que sólo están disponibles en las redes privadas.

Una vez establecido un túnel seguro, los datos pueden ser transmitidos con confianza y seguridad entre los dispositivos de red. Para configurar una red inalámbrica utilizando las VPNs, debe comenzarse por asumir que la red inalámbrica es insegura.

Esto quiere decir que la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red, mediante el uso de una lista de acceso adecuada en un router o agrupando todos los puertos de acceso inalámbrico en una red de área local virtual (*Virtual Local Area Network* / VLAN) si se emplea *switching*.

Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. Deberá permitirse acceso completo al cliente, sólo cuando éste ha sido debidamente autorizado y autenticado.

3.2 Requerimientos de una VPN

Al implementar una solución de red privada virtual, se desea facilitar un acceso controlado a los recursos y a la información.

La solución debe permitir la libertad para que los clientes remotos autorizados se conecten fácilmente a los recursos corporativos dentro de una red, y también deberá permitir que las oficinas remotas se conecten entre sí para compartir recursos e información.

Finalmente, debe garantizar la privacidad y la integridad de los datos que viajan en *Internet* u otra red pública.

Las mismas cuestiones aplican en el caso de datos sensibles que viajan a través de una red corporativa.

Por lo tanto, una solución de VPN debe proporcionar lo siguiente:

- **Autenticación:** La solución deberá verificar la identidad y restringir el acceso de la VPN. Además, deberá proporcionar registros contables y de auditoria.

- **Administración de dirección:** La solución deberá asignar una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan así.

- **Cifrado de datos:** Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados en la red.

- **Cifrado de Claves Simétricas (una clave):** Este tipo de cifrado utiliza una clave única que poseen tanto el remitente como el destinatario. La clave es utilizada tanto para el cifrado como para el descifrado, también es llamada clave de sesión.

- **Cifrado de Claves Públicas (dos claves):** En el cifrado de claves públicas se usan dos claves: una pública y otra privada, que están relacionadas matemáticamente.

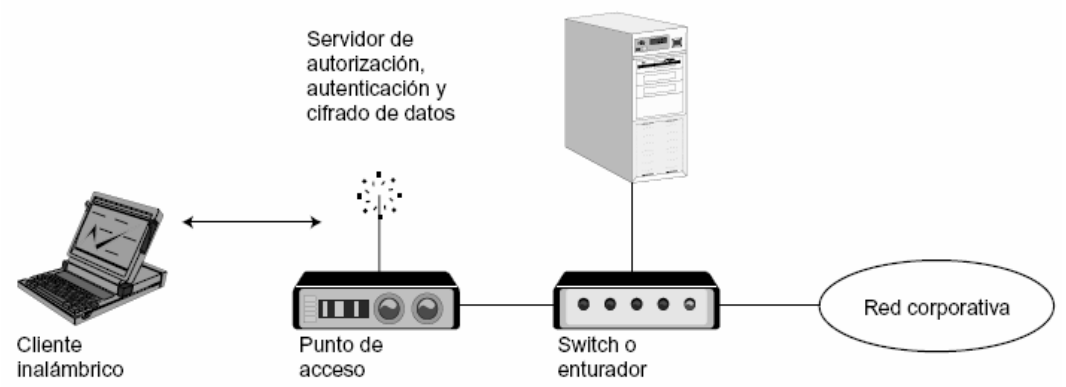
- **Administración de llaves:** La solución deberá generar y renovar las llaves de cifrado para el cliente y para el servidor.

- **Soporte múltiple de protocolos:** La solución deberá poder manejar protocolos comunes utilizados en las redes públicas. Estos incluyen Protocolo de *Internet* (IP), Central de paquete de *Internet* (IPX), etc.

3.3 Estructura de una VPN para acceso inalámbrico seguro

La siguiente figura muestra la topología sugerida para obtener una VPN segura en el acceso inalámbrico.

Figura 17. Estructura de una VPN para acceso inalámbrico seguro



Fuente: **Seguridad en redes inalámbricas 802.11.** www.icesi.edu.co/es/publicaciones/publicaciones/contenidos/sistemas_telematica/3/jamdrid-seguridad_redes_inalambricas.pdf. (20/04/2004)

3.4 Protocolos utilizados en una VPN

3.4.1 *Point-to-Point Tunneling Protocol* / PPTP

El PPTP fue desarrollado por ingenieros de *Ascend Communications, U.S. Robotics*, *3Com Corporation*, *Microsoft*, y *ECI Telematics* para proveer entre usuarios de acceso remoto y servidores de red una red privada virtual.

Como protocolo de túnel, PPTP encapsula *datagramas* de cualquier protocolo de red en *datagramas* IP, que luego son tratados como cualquier otro paquete IP.

La gran ventaja del encapsulamiento de *datagramas* es que cualquier protocolo puede ser ruteado a través de una red IP, como *Internet*.

PPTP fue diseñado para permitir a los usuarios conectarse a un servidor RAS desde cualquier punto en *Internet* para tener la misma autenticación, encriptación y los mismos accesos de LAN como si discaran directamente al servidor.

En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de *Interne*t utilizando PPTP.

El paquete PPTP está compuesto por un *header* (cabecera) de envío, un *header* IP, un *header GREv2* y el paquete de carga.

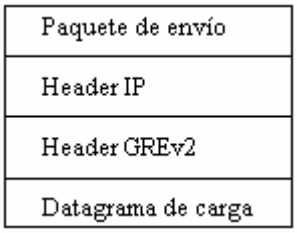
El *header* de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea *Ethernet*, *frame relay*, PPP.

El *header* IP contiene información relativa al paquete IP, como por ejemplo, direcciones de origen y destino, longitud del *datagrama* enviado, etc.

El *header GREv2* contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor.

Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el *datagrama* es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros.

Figura 18. Capas del encapsulamiento PPTP



Fuente: **Virtual Private Networks (VPN).**
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml. (30/05/2004)

3.4.2 IP *Security* o IPSec

IPSec trata de remediar algunos errores de IP, tales como protección de los datos transferidos y garantía de que el emisor del paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son *Authentication Protocol* (AH) y *Encapsulated Security Payload* (ESP).

- Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

- Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

- Por autenticidad se entiende por la validación de remitente de los datos.

- Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

Authentication Protocol (AH) provee autenticación, integridad y protección a repeticiones pero no así confidencialidad.

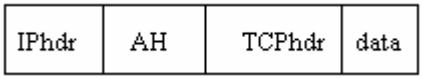
La diferencia más importante con ESP es que AH protege partes del *heade*r IP, como las direcciones de origen y destino.

Encapsulated Security Payload (ESP) provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al *header*.

El modo de transporte es utilizado por el *host* que genera los paquetes. En este modo, los *headers* de seguridad son antepuestos a los de la capa de transporte, antes de que el *heade*r IP sea incorporado al paquete.

En otras palabras, AH cubre el *header* TCP y algunos campos IP, mientras que ESP cubre la encriptación del *header* TCP y los datos, pero no incluye ningún campo del *header* IP.

Figura 19. Paquete AH en modo transporte



Fuente: **Virtual Private Networks (VPN).**
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml. (30/05/2004)

El modo de túnel es usado cuando el *header* IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión segura es un *gateway*.

En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el *header* IP entre los extremos, agregando al paquete un *header* IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del *gateway*.

Figura 20. Paquete AH en modo túnel

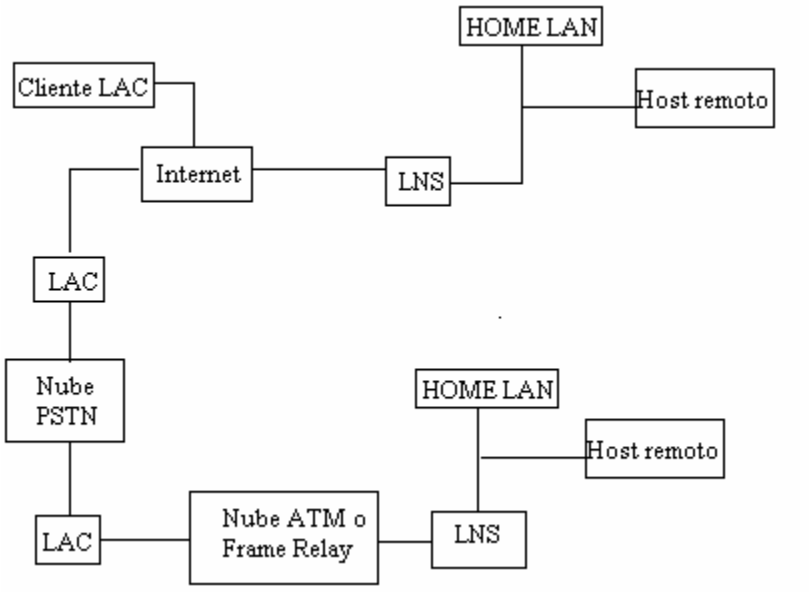
Fuente: **Virtual Private Networks (VPN).**
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml. (30/05/2004)

3.4.3 *Layer to Tunneling Protocol* / L2TP

L2TP facilita el entunelamiento de paquetes PPP a través de una red de manera tal que sea lo más transparente posible a los usuarios de ambos extremos del túnel y para las aplicaciones que éstos ejecuten.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local.

Figura 21. Escenario típico L2TP



Fuente: **Virtual Private Networks (VPN).**
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml. (30/05/2004)

Un L2TP *Access Concentrator* (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS.

Un LAC se sitúa entre un LNS y un sistema remoto, y manda paquetes entre ambos.

Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP *Network Server* (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC.

El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, es una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a *Internet*.

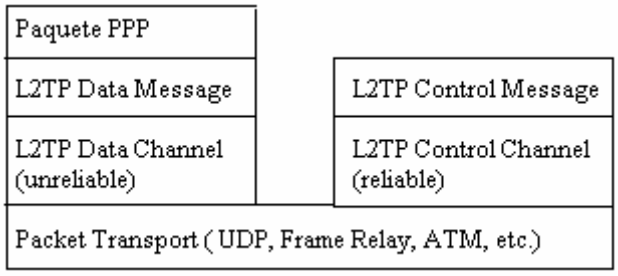
El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el *Home LAN's Management Domain*.

L2TP utiliza dos tipos de mensajes:

- **Mensajes de control:** Los mensajes de control son usados para el establecimiento, el mantenimiento y el borrado de los túneles y las llamadas. Utilizan un canal de control confiable dentro de L2TP para garantizar el envío.

- **Mensajes de datos:** Los mensajes de datos encapsulan los marcos PPP y son enviados a través del túnel.

Figura 22. Relación entre los marcos PPP y los mensajes de control



Fuente: **Virtual Private Networks (VPN).**
http://www.monografias.com/trabajos12/monvpn/monvpn.shtml. (30/05/2004)

3.5 Resultados obtenidos al utilizar VPN

- Mayor seguridad de que los usuarios que accedan a la red estén debidamente autenticados.

- Además de ser una alternativa interesante cuando ya se tiene una red inalámbrica, y no se posee hardware inalámbrico que soporte el protocolo 802.1x.

- VPN es uno de los mejores mecanismos de seguridad.

- Las VPN ofrecen un nivel más de seguridad basado en la creación de un túnel seguro entre el usuario y la red.

- Las *Virtual Private Networks* (VPN) son una alternativa a la conexión WAN mediante líneas telefónicas y al servicio RAS, bajando los costos de éstos y brindando los mismos servicios, mediante el uso de la autenticación, encriptación y el uso de túneles para las conexiones.

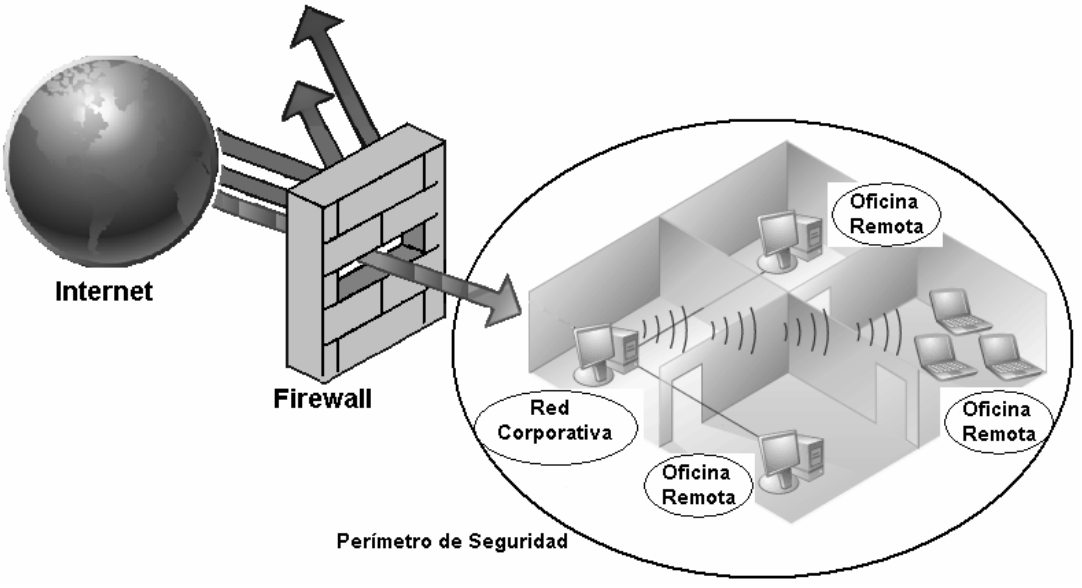
4 *FIREWALLS* Y FILTRADO DE DIRECCIONES MAC

4.1 ¿Qué es un *firewall*?

Un *firewall (*cortafuegos) en *Internet* es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada e *Internet*. El *firewall* determina los servicios de red que pueden ser accesados dentro de ésta por los que están fuera, es decir, quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un *firewall* sea efectivo, todo tráfico de información a través de *Internet* deberá pasar a través del mismo donde podrá ser inspeccionada la información. El *firewall* podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración.

Figura 23. Implementación de un *firewall*



El *firewall* es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información.

Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de *dial-in* y *dial-out*, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento.

Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad.

Un *firewall* de *Internet* sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

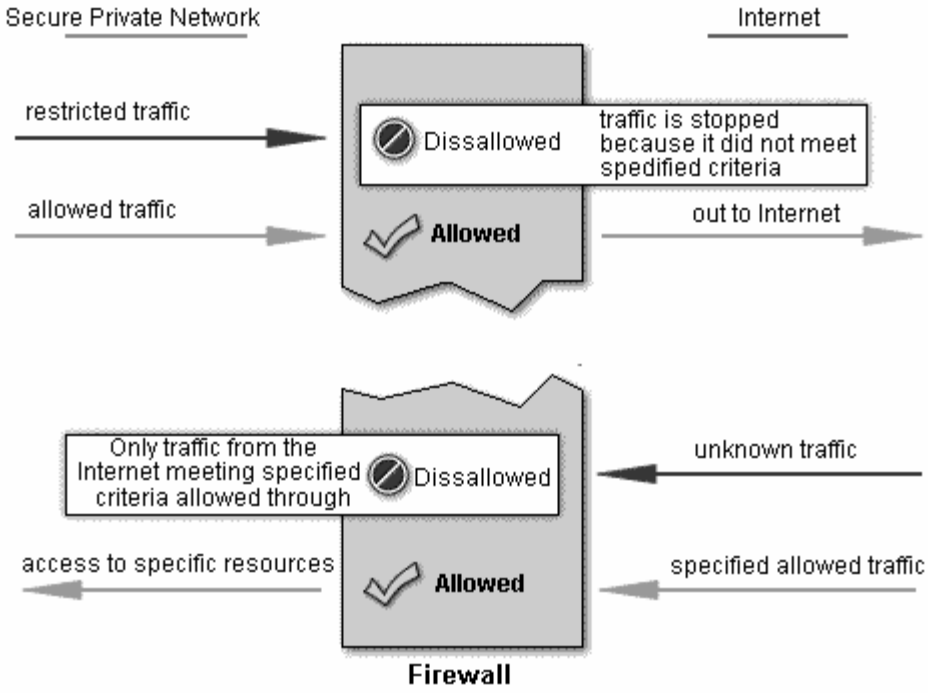
4.2 ¿Cómo funciona un *firewall*?

Básicamente un *firewall* examina el tráfico en la red, tanto entrante como saliente y lo examina en base a ciertos criterios, para determinar si lo deja pasar o lo descarta.

Si detectan algo anormal pueden tener procedimientos a seguir o poner en aviso al administrador.

Actualmente existen dos metodologías que utiliza el *firewall* para negar el acceso, un *firewall* puede permitir todo el tráfico a menos que resuelva ciertos criterios, o puede negar todo el tráfico a menos que resuelva ciertos criterios

Figura 24. Metodologías de negación de acceso de un *firewall*



Fuente: ***Firewalls* - Grupo de Seguridad del CEM**.
http://webdia.cem.itesm.mx/ac/rogomez/seguridad/Firewalls.ppt. (29/04/2000)

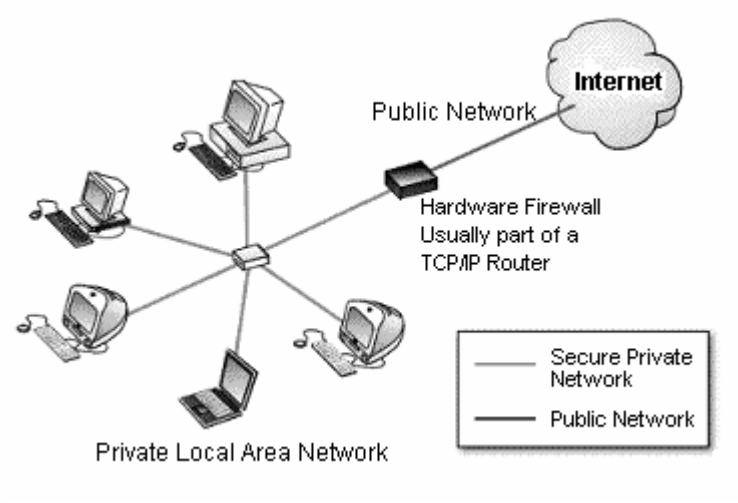
4.3 Tipos de *firewalls*

Existen dos grandes divisiones en cuanto a los tipos de *firewalls* existentes, y ellos son *firewalls* de *hardware* y *firewalls* de *software*.

4.3.1 *Firewalls* de *Hardware*

En este caso el *firewall* es un dispositivo de *hardware*, usualmente es un *router*.

Figura 25. Escenario de un *firewall* de *hardware*

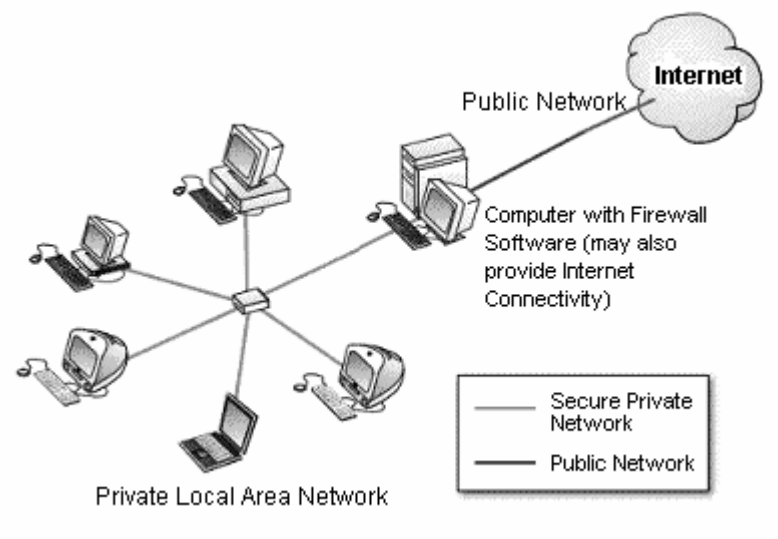


Fuente: ***Firewalls* - Grupo de Seguridad del CEM**.
http://webdia.cem.itesm.mx/ac/rogomez/seguridad/Firewalls.ppt. (29/04/2000)

4.3.2 *Firewalls* de *Software*

En el caso de los firewalls de software son programas que se encuentran corriendo en una computadora.

Figura 26. Escenario de un *firewall* de *software*



Fuente: ***Firewalls* - Grupo de Seguridad del CEM**.
http://webdia.cem.itesm.mx/ac/rogomez/seguridad/Firewalls.ppt. (29/04/2000)

4.4 Beneficios de un *firewall* en *Internet*

Con el paso de algunos años, *Internet* ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona.

Por este medio se organizan las compañías conectadas a *Internet*, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios.

Un *firewall* es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT por sus siglas en inglés) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISP por sus siglas en inglés).

Un *firewall* de *Internet* es el punto perfecto para auditar o registrar el uso de *Internet*.

Esto permite al administrador de red justificar el gasto que implica la conexión a *Internet*, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios de información a consumidores, el *firewall* de *Internet* es ideal para desplegar servidores WWW y FTP.

La preocupación principal del administrador de red, son los múltiples accesos a *Internet*, que se pueden registrar con un *firewall* en cada punto de acceso que posea la organización hacia *Internet*.

Estos puntos de acceso significan puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

4.5 Limitaciones de un *firewall*

Un *firewall* no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación.

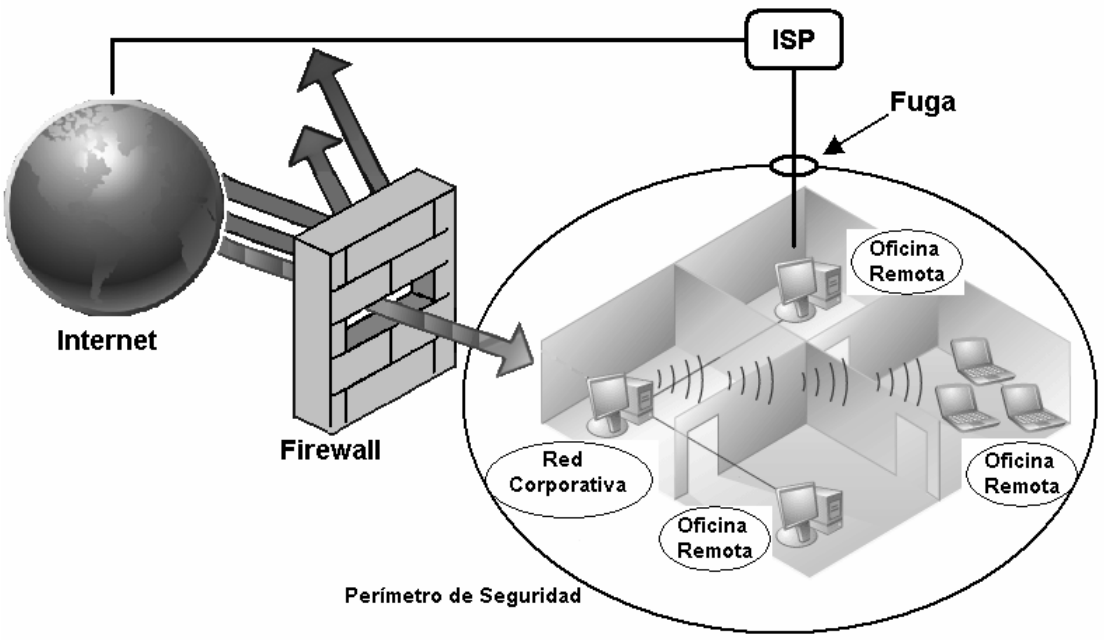
Por ejemplo, si existe una conexión *dial-out* sin restricciones que permita entrar a la red protegida, el usuario puede hacer una conexión SLIP o PPP a *Internet*.

Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un *Firewall Proxy Server* (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por *firewall* construido cuidadosamente, creando una puerta de ataque.

Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.

Figura 27. Limitaciones de un *firewall*



4.6 Filtrado de direcciones MAC

4.6.1 ¿Qué es el filtrado de direcciones por MAC?

Al aparecer las tecnologías inalámbricas han abierto un futuro muy prometedor, pero como en la comunicación inalámbrica no existen cables por los cuales viaje la información esta viaja a través de ondas de radio, la seguridad, privacidad e integridad de los datos genera nuevos y grandes retos.

El filtrado de direcciones por MAC es una técnica que se utiliza para brindar seguridad a nivel direcciones MAC en una red de computadoras inalámbricas.

4.6.2 Funcionamiento del filtrado de direcciones MAC

Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica.

Dicha tabla contiene las direcciones MAC (*Media Access Control*) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

Este método tiene como ventaja su sencillez, por lo cual se puede usar para redes caseras o pequeñas.

Sin embargo, posee muchas desventajas que lo hacen impráctico para uso en redes medianas o grandes, como las siguientes:

- No escala bien, porque cada vez que se desee autorizar o dar de baja un equipo, es necesario editar las tablas de direcciones de todos los puntos de acceso. Después de cierto número de equipos o de puntos de acceso, la situación se torna inmanejable.

- El formato de una dirección MAC no es amigable (normalmente se escriben como 6 *bytes* en hexadecimal), lo que puede llevar a cometer errores en la manipulación de las listas.

- Las direcciones MAC viajan sin cifrar por el aire. Un atacante podría capturar direcciones MAC de tarjetas matriculadas en la red empleando un *sniffer*, y luego asignarle una de estas direcciones capturadas a la tarjeta de su computador. De este modo, el atacante puede hacerse pasar por un cliente válido.

- En caso de robo de un equipo inalámbrico, el ladrón dispondrá de un dispositivo que la red reconoce como válido. En caso de que el elemento robado sea un punto de acceso el problema es más serio, porque el punto de acceso contiene toda la tabla de direcciones válidas en su memoria de configuración.

Debe notarse además, que este método no garantiza la confidencialidad de la información transmitida, ya que no prevé ningún mecanismo de cifrado.

5 REDES INALÁMBRICAS EN GUATEMALA

5.1 Impacto de las redes inalámbricas en Guatemala

El impacto potencial puede ser medido de acuerdo al orden de la utilización de esta tecnología en las empresas guatemaltecas.

En principio la utilización de redes inalámbricas ameritaba utilizar el término de “tecnología de lujo” para una empresa, pero luego este tipo de tecnología trajo en si la solución a las empresas en las cuales las actividades de negocios practicadas por dichas empresas involucran gran movimiento.

Siendo la movilidad una de las características principales de las redes inalámbricas, no tardo mucho tiempo en que empresas que tuvieran problemas con trabajar con redes alambradas adoptaran este tipo de tecnología.

Otro factor importante de gran impacto sobre la implementación de redes inalámbricas son los costos asociados que conllevan. Dado que muchos de los ingenieros o administradores de red se enfocan, por lo regular, en el costo de *hardware* que implicará determinada solución (que indudablemente es importante para sus respectivas empresas), sin embargo no se percatan o le restan importancia a otros aspectos determinantes en una buena solución, tanto en el presente como en los próximos años.

Ciertamente, la incursión de las *Wireless* LAN en Guatemala ha sido lenta y con cierta reserva, debido a los problemas legales que la organización reguladora de frecuencias (SIT) pudiera plantear a cierto usuario que de alguna manera genere interferencias en otro sistema. Sin embargo, un buen diseño de implementación puede evitar dichos problemas. Dentro del área geográfica, propiedad del usuario, pueden instalarse los equipos inalámbricos y tomar ciertas políticas de seguridad para que no implique riesgos de transmisión y recepción en otros sistemas de RF aledaños o viceversa.

Tomando en cuenta las características y beneficios de las redes inalámbricas, poco a poco las WLANs han ido ganando terreno dentro de algunos sectores productivos de Guatemala.

Específicamente las *Wireless* LAN han sido recibidas como soluciones de red en universidades, hoteles, restaurantes y en algunos sectores industriales del país como los ingenios, licoreras, fincas agrícolas, etc.

Casos aún más concretos son los restaurantes como Pollo Campero, La Playa, Nais, que utilizan tecnología inalámbrica como una herramienta de mercadeo para satisfacer las necesidades de sus clientes al poderse conectar con sus PDA's y Laptops. Convirtiendo esta tecnología en una ventaja competitiva sostenible ante sus potenciales competidores que carecen de dicho servicio.

Adicionalmente, las redes inalámbricas tienen un amplio campo en soluciones para edificios antiguos, salas de reuniones, eventos temporales, etc. Es allí donde se cree que hay y habrá una gran acogida por parte de empresas del país.

5.2 Topología sugerida

5.2.1 Posiciones geográficas

La posición geográfica para la instalación de una red inalámbrica y su correcto uso son muy importantes, ya que pueden poner en riesgo toda la instalación.

Por los terrenos montañosos con que cuenta Guatemala, los siguientes factores suelen afectar y por lo tanto deben ser considerados:

- Características topográficas de la zona, como las montañas.
- La curvatura de la tierra dependiendo de la ubicación.
- Edificios, árboles, zonas con nubosidad, etc.

Figura 28. Obstáculos en una red inalámbrica

Fuente: ***Fundamentals of Wireless LANs v1.1***. www.cisco.com. (06/10/2004)

Por lo que se recomienda instalar la red un área libre de obstáculos para su correcto funcionamiento.

5.2.2 Problemas con la transmisión de la señal

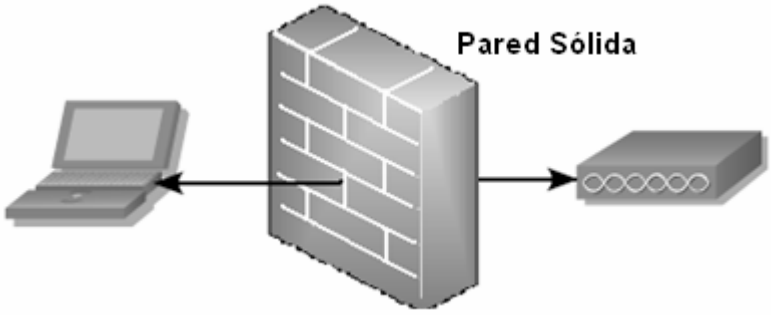
Muchos de los problemas con la trasmisión de la señal suelen ocurrir por las condiciones en las cuales se encuentra instalada la red, y por que no se han leído correctamente todas las especificaciones de los dispositivos utilizados.

En el medio Guatemalteco una de las causas por las cuales la señal no es transmitida como se esperaba, es por el hecho de que la mayoría de construcciones se hacen con materiales sólidos (ladrillos, block, etc.).

Causas por las cuales la señal no es trasmitida correctamente:

- Estanterías de metal.
- Paredes construidas con materiales sólidos.
- Espacios particionados en cubículos.

Figura 29. Obstáculos en la transmisión de la señal



Fuente: ***Fundamentals of Wireless LANs v1.1***. www.cisco.com. (06/10/2004)

5.3 Niveles de seguridad a ser considerados

Mientras que en las redes cableadas es más complicado conectarse de forma ilegítima ya que habría que conectarse físicamente mediante un cable, en las redes inalámbricas donde la comunicación se realiza mediante ondas de radio, esta tarea es más sencilla. Es por ello que hay que prestar aún mayor atención a los aspectos de seguridad de la red.

Los paquetes de información en las redes inalámbricas viajan en forma de ondas de radio (por medio de radio frecuencia).

Las ondas de radio pueden viajar más allá de las paredes y filtrarse en habitaciones/casas/oficinas contiguas o llegar hasta la calle si no se ubica el punto de acceso en el lugar indicado.

De igual forma esto depende mucho del tipo de dispositivos que se utilicen ya que algunos tienen mayor alcance que otros dependiendo de las marcas y precios, es por ello que se recomienda en todo momento estar al tanto de las especificaciones técnicas de los dispositivos a utilizar en la red inalámbrica.

Uno de los principales problemas en que la señal viaje de forma descontrolada es decir a lugares a los cuales no debería de llegar, es que se estaría dando total acceso a la señal, esto podría ser utilizado por un pirata informático o persona no autorizada para estar monitoreando todo el tráfico de la red y de esta forma tener acceso a carpetas compartidas y sobre todo obtener contraseñas o información de conversaciones confidenciales.

El hecho de la infiltración no autorizada en redes inalámbricas domesticas ya es un gran problema porque alguien puede estar robando señal o monitoreando todo lo que se hace en la computadora o red afectada. Este problema se agranda de forma abrumadora en redes corporativas ya que el tipo de información que se maneja es de alta importancia.

Para garantizar una red inalámbrica más segura hay ciertas combinaciones de medidas de seguridad que pueden ser utilizadas.

Estas combinaciones no son una receta ya que para unos tipos de empresas pueden aplicar todas las combinaciones posibles y para otras empresas pueden ser demasiadas o demasiados los costos incurridos en la aplicación de dichas combinaciones de seguridad.

- Situar el Punto de Acceso en el lugar adecuado.

- Cambiar la contraseña que trae el Punto de Acceso por defecto.

- Utilizar un método de encriptación WEP/WPA/WPA2, es muy importante que a la hora de seleccionar el método de encriptación sea el que tenga el mayor numero de bits de encriptación.

- Cambiar el SSID por defecto, ya que regularmente el SSID suelen ser palabras muy sencillas y conocidas.

- Utilizar VPN, ya que es uno de los mejores mecanismos de seguridad.

- Impulsar la utilización de los servidores RADIUS existentes.

- Activar el filtrado de direcciones MAC, con esto se estará asegurando que solo los dispositivos con direcciones MAC especificadas se podrán conectar a la red inalámbrica.

- Establecer un numero máximo de dispositivos que pueden conectarse a la red inalámbrica, esto dependerá si el tipo de Punto de Acceso o dispositivo utilizado lo permite.

- Desactivar el DHCP, esto evitara que alguien que no tenga conocimiento de los datos necesarios (dirección IP necesaria, *Gateway*, DNS) para integrarse a la red pueda hacerlo.

- En caso de que no se vaya a utilizar la red inalámbrica por un cierto tiempo por diferentes motivos (vacaciones, fines de semana, etc.) lo mas recomendado es apagar todos los dispositivos utilizados en la red inalámbrica.

- Dar mantenimiento a todas las claves utilizadas en los diferentes métodos de seguridad.

Como se menciono anteriormente, estas estrategias para proteger redes inalámbricas son solo una guía ya que en todos los casos algunas pueden aplicar y otras no.

Es el deber de cada administrador de la red, establecer que políticas son las más aconsejables para cada red en especial.

5.4 Análisis de costos versus beneficios

A continuación se describirá un caso hipotético en el cual se tratará de demostrar que la implementación de una red inalámbrica es mas barata que una implementación alambrica. De igual forma se pretende mostrar el impacto que causaría dicha implementación.

5.4.1 Descripción del caso hipotético

Considérese un centro comercial de 3 niveles. En los primeros 2 niveles del edificio, estarán alojados varios tipos de tiendas y sectores: venta de ropa, venta de accesorios deportivos, venta de abarrotes o mini supermercados, todas las tiendas y sectores antes mencionados necesitan conexión a Internet, sin embargo en los primeros 2 niveles existen salas temporales y tiendas móviles.

En el tercer nivel se encuentra el área de restaurantes y en este nivel se necesita acceso a Internet para todos los clientes que lleven sus computadoras portátiles ya que seria el primer centro comercial en brindar este tipo de servicio a sus clientes y de esta forma influiría en una ventaja competitiva sostenible contra sus competidores cercanos.

5.4.2 Soluciones propuestas

Las soluciones que se analizaran para resolver el antes descrito, son realizar tendidos de cable UTP o implementar WLANs. Para efectos de este caso hipotético solo se tomaran en cuenta los costos asociados al cableado en el caso de la solución con cable UTP y en el caso inalámbrico se tomaran los costos asociados a brindar el mismo servicio.

5.4.2.1 Cableado UTP

En esta solución básicamente consiste en contratar los servicios de una empresa que realice el cableado estructurado horizontal.

Es importante hacer la salvedad que en este caso solo se toman los costos de cableado simple, los costos no incluyen canaletas o mejoras a la infraestructura de red que ya exista.

Tabla V. Costos de propuesta UTP

Descripción	Cantidad	Precio Unitario	Precio Total
Cable UTP categoría 5 (rollo 1000 pies)	3	100	300
Patch cord Newlink de 7’	32	6.4	204.8
Patch cord Newlink de 3’	32	4.4	140.8
Rack industrial	1	500	500
Router Cisco 805	1	800	800
Switch Cisco WS-C2950G-24EI	3	1000	3000

Costo propuesta UTP = $ 4945.6

5.4.2.2 Conexión por medio de WLANs

Esta solución considera instalar dos puntos de acceso Cisco Airones 350. Los puntos de acceso tienen un área de cobertura de 150 mts, suficiente como para brindar servicio de Internet a todo el edificio.

Tabla VI. Costos de propuesta WLAN

Descripción	Cantidad	Precio Unitario	Precio Total
Access Point Airones Cisco	2	400	800
Adaptador inalámbrico PCMCIA 352	32	100	3200
Router Cisco 805	1	800	800

Costo propuesta WLAN = $ 4800

5.4.3 Por qué escoger la solución WLAN?

Hay muchas razones por las cuales para este problema específicamente es preferible una opción de WLANs a una LAN alambrada, como las que se mencionan a continuación:

- **Costo de la propuesta:** este es un factor muy importante que define en gran parte la implementación o no, de un proyecto. Para este en particular se pueden comparar los costos de implementación para ambas propuestas.

Tabla VII. Comparación de costos (propuestas)

Propuesta	Inversión total
Cableado estructurado	$ 4945.6
Wireless LAN	$ 4800

En la tabla anterior se observa que la diferencia en costos de implementación no es muy grande, pero la verdadera razón de escoger la solución inalámbrica radica en una de las características de las redes inalámbricas la movilidad.

- **Flexibilidad en el servicio:** Cada evento que se lleve a cabo en alguna parte del edificio será distinto con respecto a otros que anteriormente han sido montados, ya que para cada evento los ambientes o decoración en las salas móviles serán completamente variables. Las WLANs permiten colocar los equipos en servicio sin necesidad de un gran esfuerzo técnico y además contribuye en la estética. Caso contrario a las LAN alambradas, que para conseguir más puntos de red de los instalados, se tendría que conectar hubs en cascada y realizar tendidos de cable UTP hacia los equipos finales.

- **Tiempo de puesta en marcha:** Aproximadamente el cableado estructurado estará completamente instalado y certificado en 15 días máximo. Por el contrario, implementar WLANs tomará un máximo de 2 días, tiempo necesario para instalar y configurar los equipos, así como para realizar pruebas de propagación de la señal RF (Radio Frecuencia) y conseguir el servicio óptimo. El tiempo de instalación de una red inalámbrica de 10 nodos es considerablemente menor que el de otras tecnologías como lo demuestra la siguiente tabla.

Tabla VIII. Tiempo de instalación de red

	Token Ring	Ethernet	WLAN
Colocación de ducterias y cableado	1 semana	1 semana	0
Configuración y Pruebas de red	1 – 2 días	1 día	6 horas
Colocación de computadoras	7 – 8 horas	7 – 8 horas	15 minutos

5.5 Tipos de empresas que utilizan WLANs

Del mismo modo que las redes alambradas, las WLAN pueden ser utilizadas en cualquier tipo de empresa o entidad corporativa e industria.

Algunos ejemplos de empresas o entidades corporativas e industrias que pueden utilizar las redes inalámbricas se muestran a continuación:

Tabla IX. Posibles empresas a utilizar WLANs

Empresa o entidad corporativa
Centros proveedores de acceso a la *Web* como los café *Internet*
Campus Universitarios (por ejemplo la USAC) o laboratorios
Hospitales y centros de salud para la atención a los pacientes en salas móviles
Supermercados, Almacenes y/o Bodegas
Bancos (Oficinas, agencias de atención al cliente, cajeros automáticos, etc.)

Tabla X. Posibles industrias a utilizar WLANs

Industria
Cafetalera
Agrícola
Azucarera
Textil
Etc.

5.6 Tecnología WLAN como solución de red en empresas Guatemaltecas

En Guatemala existen muchas empresas que continuamente realizan cambios en la infraestructura en la red interna de datos; a su vez, existen otras compañías que de forma frecuente cambian el diseño de las instalaciones

donde radican o simplemente se realizan remodelaciones parciales o totales del sitio (oficinas de exposiciones, tiendas de ventas, etc.).

Por ejemplo, con el fin de maximizar el espacio de trabajo en algunas situaciones se colocan paredes de tabla-yeso para formar varias oficinas más pequeñas, o se colocan cubículos para puestos de trabajo, etc.

Si en esos lugares ya existe una red LAN cableada (utilización de cable UTP o coaxial), sin lugar a duda estos cambios generarán gastos por reordenamiento o cableado de los nuevos puntos de acceso a la red.

Gastos como: limpieza de los puntos de red actuales, compra de nuevo cable y accesorios para montar los puntos, mano de obra, etc. En estos casos, en los cuales surgen molestias tanto para la compañía como para los clientes que visitan el sitio, las *Wireless* LAN han recibido una aceptación muy grande.

5.6.1 Interconexión de LANs convencionales a una WLAN

Básicamente la solución consiste en proporcionar el equipo inalámbrico necesario (APs, tarjetas de red inalámbricas, *notebooks*, PDAs, etc.) según sea el caso, para que usuarios sin importar el lugar donde se encuentren, permanezcan siendo parte de la red y accesando a los recursos disponibles en la misma.

Este tipo de solución se ha brindado por diferentes factores:

- Uno, en aquellas situaciones en las cuales llevar cableado físico hacia los usuarios es sumamente dificultoso y representa un alto desembolso económico par la empresa.

- Dos, cuando la ubicación de las estaciones de trabajo sean zonas de alto riesgo.

- Tres, en ambientes en los cuales no pueden tenderse cables físicos.

- Cuatro, en lugares, como hoteles, donde se requiere brindar un servicio de la más alta calidad y que implique confort, comodidad y satisfacción para los usuarios.

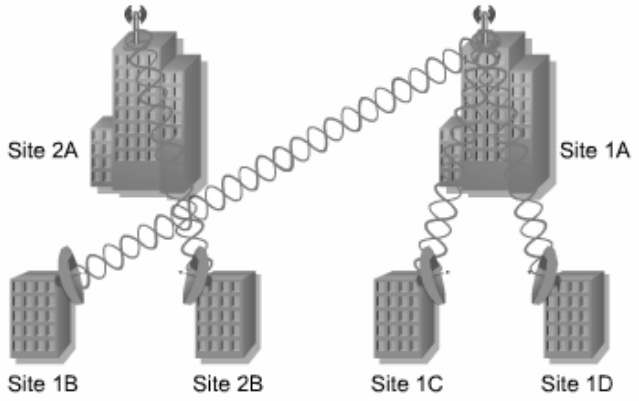
5.6.2 WLAN como solución a edificios dispersos

Solución que ha sido adoptada por aquellas empresas cuya necesidad básica sea el interconectar varios sitios (edificios, bodegas, almacenes, etc.) separados por distancias relativamente cortas.

Esta solución no incurre en gastos tales como: tendidos de cable coaxial o fibra óptica, o bien el arrendamiento de enlaces dedicados o la compra de equipos extras tales como *switches*, *bridges*, *routers*, etc.

Obviamente deben adquirirse los equipos apropiados (que en este caso APs o *Wireless Bridges*) para conectar los distintos sitios que así se requiera.

Figura 30. Situación de edificios dispersos



Fuente: ***Fundamentals of Wireless LANs v1.1***. www.cisco.com. (06/10/2004)

A manera de ejemplo de este tipo de situaciones, se cita el caso de algunas universidades del país como lo son la Universidad San Carlos de Guatemala, Universidad Galileo, Universidad Francisco Marroquín, donde se han trabajado propuestas de enlazar la mayoría de edificios que conforman el campus universitario.

Dicho enlace es para formar parte de la Intranet de la institución, logrando con ello beneficios tanto para el personal docente y administrativo así como para los estudiantes, como seria: revisión de calendario de cursos, pago de cursos en línea, fechas de inscripción y otros mas. Incluso, estudiantes con *notebooks*, un adaptador de red inalámbrico y una cuenta de usuario, podrían acceder a la red estando en un parque que este dentro del área cubierta por los APs.

Un ejemplo claro de este tipo de servicio es la implementación de Internet inalámbrico por parte de SAE-SAP.

Actualmente SAE-SAP tiene instalada una red inalámbrica, de tal forma que ubicándose cerca de las instalaciones de SAE-SAP un estudiante equipado de una computadora, tarjeta de red inalámbrica o dispositivo inalámbrico y la información necesaria para la configuración de la misma, puede conectarse fácilmente a Internet de forma inalámbrica.

5.7 Proyección de las WLAN en Guatemala

5.7.1 Proyección en América Latina

En los sectores privado y público de América Latina existe un importante interés y actividad en el campo de las tecnologías inalámbricas.

En estos momentos el sector privado usa estas tecnologías para dar acceso a diferentes servicios. Se están creando modelos de negocios ventajosos para las áreas urbanas y suburbanas, así como también para áreas desatendidas y comunidades rurales que nunca antes habían tenido acceso.

En algunos casos, las grandes compañías de telecomunicaciones están aliándose con pequeñas empresas de aparatos y servicios para ofrecer acceso a las áreas que no cuentan con estos servicios.

Además, las alianzas público-privadas, que en ciertos casos han sido fomentadas por instituciones internacionales para el desarrollo, están dando

mayor apoyo al uso de las tecnologías inalámbricas y ayudando a crear modelos sostenibles de negocios para el suministro de acceso inalámbrico.

Los gobiernos de la región están implementando cada vez más proyectos de desarrollo basados en tecnologías inalámbricas, promoviendo además la competencia por medio de una política de liberalización de las bandas.

5.7.1.1 Perspectivas para el sector privado

Según un informe del *Business News America*, se esperaba que las compañías de telecomunicaciones latinoamericanas gastasen más de US$3,000 millones en 2004 para ampliar los servicios de banda ancha.

Una observación más detallada de algunas inversiones recientes revela una mayor comprensión de la importancia de las tecnologías inalámbricas por parte de los sectores público y privado.

Algunos expertos del sector industrial sostienen que, dada la insuficiente capacidad de la línea fija, las tecnologías inalámbricas fijas podrían jugar un importante papel en el establecimiento de la banda ancha en la región.

Pese a que las grandes compañías de telecomunicaciones han tenido una función importante en la adopción de tecnologías inalámbricas en la región, no están impidiendo el accionar de operadores más pequeños, ya que, en algunos casos, consideran que el suministro de servicios rurales es una fuente alternativa de ganancias y no una amenaza.

Como consecuencia, están surgiendo muchos operadores pequeños en toda la región. El mercado mexicano es un ejemplo del interés en las tecnologías inalámbricas por parte de operadores grandes y pequeños del sector privado.

5.7.1.2 Perspectivas para el sector público

Dadas las crecientes ventajas económicas y la gran publicidad que acompaña a las tecnologías inalámbricas, los gobiernos de América Latina están apoyando en forma explícita estas tecnologías en su agenda para el desarrollo y los bancos multilaterales de desarrollo también les brindan asistencia para que puedan continuar con sus esfuerzos en esta área.

Por ejemplo, USAID ha destinado US$10 millones para la Iniciativa Última Milla, la cual proporcionará TIC a las zonas rurales y pobres de los países en vías desarrollo (incluyendo los países latinoamericanos y caribeños).

Para USAID son de particular interés las tecnologías *Wi-Man* (*Wireless Metropolitan Area Networking*), que ofrecen conexiones de banda ancha punto a multipunto. Además USAID está interesada en fomentar cambios en la regulación para asegurar el éxito de las iniciativas basadas en tecnologías innovadoras en los países que reciben su ayuda.

En algunos casos, USAID ha logrado obtener libertades para poder realizar proyectos de acceso inalámbrico en comunidades rurales.

El interés del Banco Mundial en promover el uso de tecnologías inalámbricas es evidente ya que, en 2004, esta institución organizó un seminario sobre el tema titulado “Tecnologías inalámbricas para el desarrollo: nuevas soluciones de conectividad para la inclusión digital”.

Muchos gobiernos dependen de la tecnología inalámbrica para brindar servicios sociales, tales como la educación, salud y comunicación y otros, en áreas remotas. El objetivo es que estos servicios lleguen a ser auto sostenibles en un periodo de entre cinco y diez años con la llegada del comercio electrónico.

Los gobiernos de Argentina, Colombia, Ecuador y Perú han aunado esfuerzos con EION Inc., compañía canadiense de tecnologías inalámbricas, para llevar a cabo estas actividades.

Dicha compañía suministra aparatos inalámbricos, servicios y asistencia técnica para proyectos piloto que son implementados por los gobiernos. Si bien este modelo no es apropiado para todos los contextos, ha dado buenos resultados en áreas donde no hay infraestructuras alámbricas, por ejemplo en los Andes o en otras zonas donde la topografía causa problemas de conectividad.

Como parte de la solución, EION propone un modelo ”auto contenido” con una conexión VSAT que ofrece un *uplink* ininterrumpido que puede ser accionado por medio de tecnologías inalámbricas para conectar varias comunidades cercanas.

La disponibilidad en el mercado de los aparatos *WiMax*, que son relativamente baratos, y su exitosa aplicación en los países andinos, demuestran que este modelo podría ser aplicado en forma más amplia. EION todavía no ha tenido grandes problemas con la política de bandas o el régimen de licencias.

5.7.1.3 Avances basados en el mercado

Los mercados rurales de banda ancha son prometedores, la OCDE (2004) pone en evidencia que está surgiendo un cambio de políticas que es el resultado de un cambio de punto de vista sobre los mercados rurales.

Anteriormente se suponía que las áreas rurales no atraen a nuevos competidores, no tienen suficiente demanda, requieren costos demasiado altos, tienen una calidad de servicio inferior, o que necesitan recibir subsidios.

Estos supuestos son incorrectos porque no tienen en cuenta los nuevos modos de ofrecer los servicios, incluidas las tecnologías inalámbricas.

De hecho, la aplicación de la tecnología inalámbrica en las áreas rurales podría dar como resultado un mayor crecimiento en todo el sector de las TIC.

La OCDE indica porcentajes cada vez más altos para el servicio de acceso de banda ancha en las áreas rurales como un ejemplo de la latente demanda rural.

Las acciones de Baja *Wireless*, ULTRAVISION, MVS *Communications* y Telmex en México muestran que existe un fuerte y creciente interés del sector privado en servir las áreas rurales. Además las tecnologías inalámbricas prometen ampliar rápidamente el acceso a las áreas rurales en ambas direcciones.

A medida que las redes inalámbricas aumentan en alcance y escala, aumentará el valor los mercados rurales y el sector privado estará más interesado en ellos.

5.7.2 Proyección en Guatemala

Anteriormente se han mencionado algunos beneficios generales que conlleva la implementación de una WLAN: movilidad, facilidad de instalación, reducción de costos de operación y mantenimiento de la red, flexibilidad y escalabilidad. Adicionalmente a estos, existen otros beneficios sensibles que proyectan las WLAN en Guatemala.

Una WLAN es compatible con plataformas de servidores y PC normalizadas, protocolos de red principalmente (TCP/IP) y sistemas operativos mas importantes del lado de Microsoft (Windows XP, Windows 2003 Server, etc.) del lado Linux (*SUSE* 10, *Mandrake* 10, *Red Hat Advance Server*, etc.), estas compatibilidades con las tecnologías ya existentes hacen que la migración hacia una red inalámbrica no sea un cambio que necesite dar un giro de 360 grados con relación a lo que ya se viene utilizando con anterioridad.

Sin embargo, el beneficio más impactante que ofrece esta tecnología de red, es que no existe la necesidad de tener una conexión física en un punto de red, para estar conectado a la misma y hacer uso de los recursos compartidos.

Teniendo en cuenta todos los beneficios que una red inalámbrica brinda la pregunta que surge es ¿Por qué todas las empresas no implementan una red inalámbrica? La respuesta a esta pregunta esta basada en las necesidades propias que cada una de las empresas tenga, por ejemplo las redes alambradas son más rápidas que las redes inalámbricas, sin embargo, es muy importante establecer hasta que punto una empresa está dispuesta a sacrificar la velocidad.

De igual forma las redes inalámbricas se enfocan en sus características principales, las cuales la hacen distinguirse de las demás tecnologías. Por ejemplo, se espera que todas aquellas empresas que tengan las siguientes características debieran de considerar una solución inalámbrica:

- Requiere velocidades de LAN Ethernet normales
- Movilidad de los usuarios
- Ambientes que son remodelados continuamente
- Crecimiento rápido
- Dificultades significativas para instalar LANs alambradas

- Necesidad de conexiones entre dos o más LANs en un área metropolitana

- Requiera oficinas temporales

Las tecnologías inalámbricas tienen un papel fundamental en todas partes, pero especialmente en los países en vías de desarrollo y en aquellos con economías en transición.

Con gran velocidad y sin enormes inversiones, las redes inalámbricas pueden facilitar el acceso al conocimiento y a la información, por ejemplo haciendo uso de un espectro de radio sin licencia para dar un acceso barato y rápido a *Internet*.

Sin duda, es justamente en los lugares donde no existe infraestructura donde las tecnologías inalámbricas y más específicamente las redes pueden ser especialmente eficaces, ya que se ayudará a que los países den grandes pasos en lo que se refiere a infraestructuras y tecnología de la telecomunicación y se dará más poder a su propia gente.

Para todos, empresas y particulares, están bastante claras las bondades de la tecnología inalámbrica, sin embargo el despegue de ésta tecnología dentro de Guatemala dependerá del precio de los dispositivos y de las distintas funcionalidades o aplicaciones que se le encuentren en las industrias actuales.

Como era de esperarse una de las mayores innovaciones tecnológicas en los últimos 25 años *Internet* (según Instituto de Tecnología de Massachussets), no se podía quedar al margen del uso de las tecnologías inalámbricas, de tal forma que el uso de Internet siga extendiéndose de nuevas formas.

La tecnología inalámbrica puede llevar *Internet* a los “desiertos cibernéticos”, donde hay pocas oportunidades de tener un cierto tipo de cableado. Estos desiertos cibernéticos son las zonas rurales, a las cuales llevar un cable de fibra óptica hasta el lugar donde es requerido es muy difícil y demanda mucha inversión lo cual incurrirá en precios más altos para el consumidor final.

Las compañías que prestan servicio de *Internet*, han visto en la comunicación inalámbrica un nuevo mercado que se abre. Un mercado que puede ser aprovechado al máximo y algo muy importante para las compañías es el hecho de que este negocio es muy rentable.

CONCLUSIONES

1. Con la tecnología inalámbrica se abre todo un mundo de posibilidades de conexión sin la utilización de cableado clásico, proporcionando una flexibilidad y comodidad sin precedentes en la conectividad entre ordenadores. Esta tecnología tiene como mayor inconveniente la principal de sus ventajas, el acceso al medio compartido de cualquiera con el material y los métodos adecuados, proporcionando un elevado riesgo de seguridad que se tendrá que tener presente.

2. La seguridad en las redes inalámbricas es un aspecto crítico que no se puede descuidar. Debido a que las transmisiones viajan por un medio no seguro, se requieren mecanismos que aseguren la confidencialidad de los datos así como su integridad y autenticidad.

3. Entre las tecnologías para brindar seguridad en redes inalámbricas mostradas en este trabajo se encuentra una de las mas famosas aunque no la más segura, el sistema WEP, incluido en la norma IEEE 802.11 para proporcionar seguridad, tiene distintas debilidades que lo hacen no seguro, por lo que deben buscarse alternativas y/o mezclas con otras tecnologías de seguridad.

4. Como se menciono en este trabajo, es relativamente fácil el crear una red híbrida –*Ethernet* cableada e inalámbrica, porque se sigue teniendo las ventajas de la velocidad que brinda la parte cableada y con la innovación de expandir las posibilidades con la parte inalámbrica.

5. Las amenazas son algo que no se puede controlar porque son externas, lo único que se puede controlar es el área vulnerable, área donde se encuentran los dispositivos de hardware de la empresa. Es por ello que se tiene que encarar el tema de la seguridad inalámbrica de manera integral y, sobre todo, comprender que la seguridad inalámbrica es un proceso no un producto.

6. La elección de la(s) tecnología(s) para brindar seguridad en redes inalámbricas, debe tomarse en base a factores claramente establecidos desde el inicio de la implementación del proyecto, por ejemplo: los recursos con los que se cuenta, la complejidad o tamaño del proyecto, el equipo y/o sistemas existentes, ya que, si no se establecen, adecuadamente, existe un alto riesgo de no llevar a cabo el proyecto con éxito.

RECOMENDACIONES

1. En cualquier implementación de seguridad inalámbrica el objetivo principal debe ser la utilización de una política de seguridad homogénea y sin fisuras, el cual trate todos los aspectos que conlleven riesgo, sin mermar la rapidez y que sepa aprovechar las ventajas de las redes inalámbricas.

2. En la actualidad, muchos productos de redes integran conmutación, servicios de acceso, autenticación de cortafuegos y características VPN, incorporan alguna funcionalidad específica WLAN y reivindican su superioridad sobre otras aplicaciones. Es muy importante evaluar la viabilidad y escalabilidad a largo plazo. Calcular el coste de instalación y puesta en marcha y el rendimiento de la inversión que estos productos ofrecen.

3. Es muy importante contar con una proyección de crecimiento del proyecto, para poder realizar una buena elección en la(s) tecnología(s) de seguridad y, sobre todo, del equipo que se debe adquirir.

4. Al momento de elegir la(s) tecnología(s) de seguridad y del equipo necesario para implementarlas, evaluar la escalabilidad que las éstas poseen.

5. Sin duda las herramientas como *firewalls*, antivirus, detectores de intrusos, cifrado, herramientas de alerta temprana, son herramientas muy útiles y talvez indispensables, pero lo que realmente importa es como se administre todo eso para que junto con las políticas y procedimientos se logre un entorno seguro.

BIBLIOGRAFÍA

1. Alvarado Gonzáles, René Estuardo. Descripción de los servicios, arquitectura y tendencias del protocolo WAP para le desarrollo de aplicaciones para redes inalámbricas. Tesis Ing. en Ciencias y Sistemas. Guatemala, Universidad de San Carlos de Guatemala, Facultad de Ingeniería, 2003. 214 pp.

2. Saz López, Carlos David. Redes inalámbricas para sistemas de seguridad. Tesis Ing. en Ciencias y Sistemas. Guatemala, Universidad de San Carlos de Guatemala, Facultad de Ingeniería, 2000. 103 pp.

3. Hjelm, Johan. **Designing wireless information services.** 1ª ed. New York: Wiley Computer Pub, 2000. 413 pp.

Referencias electrónicas

4. **Arquitectura de la red.** http://www.unavarra.es/organiza/etsiit/cas/estudiantes/pfc/redaccna/Tecnologias%20de%20Acceso/WLAN/Arquitectura%20red/arquitectura_WLAN.htm. (30/09/2005)

5. **Como hacer una red wifi segura.** http://blyx.com/hotwo-wpa+eap-tls+freeradius.pdf. (06/07/2005)

6. **Conceptos básicos de seguridad en redes *wireless*.** http://www.virusprot.com/Whitepap1.html. (01/11/2002)

7. **Conceptos de seguridad en redes inalámbricas 802.11.** http://www.gui.uva.es/~laertes/nuke/index.php?option=com_content&task=view&id=39&Itemid=41. (29/10/2004)

8. ***Configuring Wired Equivalent Privacy* (WEP).** www.cisco.com. (22/01/2005)

9. **El estándar IEEE 802.11 *Wireless* LAN.** http://greco.dit.upm.es/~david/TAR/trabajos2002/08-802.11-Francisco-Lopez-Ortiz-res.pdf. (28/12/2003)

10. **Estándares y mecanismos de seguridad.** http://www.enterate.unam.mx/Articulos/2004/agosto/redes.htm. (15/08/2004)

11. ***Ethernet* inalámbrica.** http://www.intel.com/es/home/trends/wireless/info/ethernet.htm. (10/11/2003)

12. ***Exploring Kerberos, the protocol for distributed security in Windows* 2000.** http://www.microsoft.com/msj/0899/kerberos/kerberos.htm. (10/08/1999)

13. ***Extensible Authentication Protocol* y PPP.** www.infor.uva.es/~jvegas/docencia/ar/seminarios/EAP.pdf. (28/10/2003)

14. ***Firewalls* y Seguridad en *Internet*.** www.coral-systems.com/documents/Tutorial Firewall.pdf. (18/04/2005)

15. ***Fundamentals of Wireless* LANs v1.1.** www.cisco.com. (06/10/2004)

16. **Glosario de Informática e *Internet*.** http://glosario.panamacom.com. (10/01/2006)

17. **IEEE 802 LAN/MAN *Standards Committee*.** http://www.ieee802.org. (13/07/2006)

18. **Integración de servicios en redes de nueva generación y evolución de la red.** www.tekvizion.com. (30/10/2003)

19. **Métodos de autentificación y encriptación en redes 802.11.** http://www.gui.uva.es/~laertes/nuke/index.php?option=com_content&task=view&id=18&Itemid=41. (25/10/2004)

20. **Protocolo de seguridad Wep.** http://www.monografias.com/trabajos18/protocolo-wep/protocolo-wep.shtml. (30/09/2005)

21. **Protocolos de seguridad en redes inalámbricas.** http://www.saulo.net/pub/inv/SegWiFi-art.htm. (07/06/2004)

22. **Qué hace *Kerberos*.** http://www.monografias.com/trabajos7/kerbe/kerbe.shtml. (10/05/2005)

23. **RADIUS.** http://es.wikipedia.org/wiki/RADIUS. (12/06/2006)

24. **Redes inalámbricas que hacen más.** http://www.pcwla.com/pcwla2.nsf/0/28384AE34EB3915880256CBD005987ED. (30/09/2005)

25. **Redes inalámbricas WLAN.** http://www.enterate.unam.mx/Articulos/2004/Abril/redes.htm. (01/04/2004)

26. **Redes inalámbricas.** http://www.multingles.net/docs/alezito/alezito_inalamb.htm. (16/01/2005)

27. **Redes inalámbricas. Wi-fi, el futuro de la comunicación.** http://www.mailxmail.com/curso/informatica/wifi/capitulo15.htm. (29/10/2003)

28. **Seguridad al descubierto.** www.watchguard.com. (10/11/2002)

29. **Seguridad de la Red de Área Local Inalámbrica (WLAN).** http://www.pc-news.com/detalle.asp?sid=&id=4&Ida=1291. (30/09/2005)

30. **Seguridad elemental para conexiones *Wireless*.** http://www.microsoft.com/latam/technet/articulos/articulos_seguridad/marzo/seguridad-wireless.asp. (01/03/2005)

31. **Seguridad en LAN inalámbricas con PEAP y contraseñas.** http://www.microsoft.com/latam/technet/seguridad/guidance/lan/peap_int.mspx. (04/03/2004)

32. **Seguridad en redes inalámbricas con Windows 2000.** www.dotnetmania.com/dnm010.pdf. (10/12/2004)

33. **Soluciones de seguridad en redes inalámbricas.** http://portal.astic.es/NR/rdonlyres/3429B178-FC84-4A1C-BF99-05FDE7AED4D7/0/mono04.pdf. (01/12/2004)

34. **Un estudio cuestiona WPA, el nuevo estándar de seguridad para WiFi.** http://www.hispasec.com/unaaldia/1843. (11/11/2003)

35. **Uso más seguro de redes inalámbricas públicas.** http://www.microsoft.com/latam/seguridad/hogar/wirelessnetwork.mspx. (29/09/2004)

36. ***Virtual Private Networks* (VPN).** http://www.monografias.com/trabajos12/monvpn/monvpn.shtml. (30/09/2005)

37. **Wi-Fi *Protected Access*.** http://es.wikipedia.org/wiki/WPA. (29/06/2006)

38. **Wi-Fi**. http://www.monografias.com/trabajos14/wi-fi/wi-fi.shtml. (30/09/2005)