CAPITULO II

TRABAJO DE CAMPO

2 ELEMENTOS NECESARIOS PARA LA CONFIGURACIÓN Y FUNCIONAMIENTO DE LAS REDES INALAMBRICAS.

Hasta ahora sabemos dos cosas: nos gusta la tecnología Wi-Fi y sabemos que hay una norma (la 802.11) que la regula ¿Pero como funciona? Primero entendamos como funciona la tecnología inalámbrica. La norma 802.11 esta basada en la misma tecnología que hace funcionar nuestros teléfonos celulares. Toda la red inalámbrica se encuentra dividida en celdas. Cada una de estas celdas (llamadas según la norma 802.11 Basic Servicie Set ó BSS) esta controlada por una base ó Access Point. En el caso en que el radio de la celda no sea lo suficientemente grande como para abastecer el área que se requiere, es posible agregar más celdas.

La norma IEEE 802.11 fue diseñada para sustituir a la capa física y MAC de la norma 802.3 (Ethernet), así, la única diferencia entre ambas es la manera en la que los dispositivos acceden a la red, por lo que ambas normas son perfectamente compatibles.

En el caso de las redes locales inalámbricas, está clara la cada vez mayor imposición del sistema normalizado por IEEE con el nombre 802.11g , norma conocida como Wi-Fi o Wireless Fidelity, aprobada en 1.990 y basada en el modelo OSI (Open System Interconnection), la primera norma 802.11 utilizaba infrarrojos como medio de transmisión para pasar hoy en día al uso de radiofrecuencia en la banda de 2.4 Ghz, con este sistema podemos establecer redes a velocidades que pueden alcanzar desde los 11 Mbps hasta los 54 Mbps estándares en los equipos actuales, aunque es posible alcanzar mayores velocidades. El estándar IEEE 802.11g alcanza

velocidades más altas y es compatible con los equipos 802.11b ya existentes. El 802.11g opera en la misma banda de frecuencia de 2,4 GHz y con los mismos tipos de modulación DSSS que el 802.11b a velocidades de hasta 11 Mbps, mientras que a velocidades superiores utiliza tipos de modulación OFDM más eficientes.

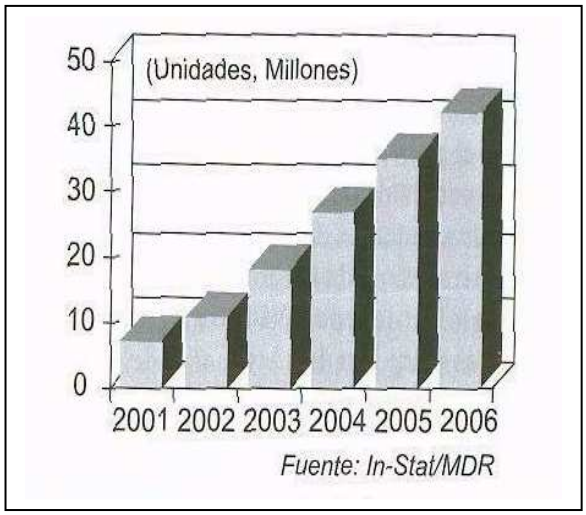
Esta compatibilidad con versiones anteriores protege la inversión de los clientes en varios aspectos. Una tarjeta de interfaz de red IEEE 802.11g, por ejemplo, puede funcionar con un punto de acceso 802.11b y viceversa, a velocidades de hasta 11 Mbps. Para lograr velocidades más altas, de hasta 54 Mbps, tanto el punto de acceso como la tarjeta de red deben ser compatibles con el estándar 802.11g. El borrador del estándar también especifica tipos de modulación opcionales (como OFDM/CCK) diseñados para mejorar la eficiencia en una instalación íntegramente 802.11g. En instalaciones grandes, la ventaja de tener aproximadamente los mismos alcances de transmisión efectivos es que la estructura WLAN 802.11b ya existente se puede mejorar fácilmente para lograr velocidades más altas sin necesidad de instalar puntos de acceso adicionales en muchos lugares nuevos a la hora de cubrir una zona determinada.

2.1. Estándares de calidad para el aseguramiento de la calidad en el flujo de información bajo estándares internacionales.

La amplia cobertura de zonas de las redes 802.11 es uno de los principales motivos para tener presente una constante preocupación e interés por la seguridad. Un atacante puede ubicarse en un lugar en que nadie espere encontrarlo y mantenerse suficientemente lejos del área física de la red. Otro motivo es el extenso uso de las propias redes 802.11: Se estima que en este año el numero de dispositivos de hardware con capacidades 802.11sobrepasarà las cuarenta millones de unidades, sobre todo a medida que el apareció de estas unidades vaya rebajándose. Después de que los productos 802.11g llegaran al mercado, el precio de muchas tarjetas de cliente 802.11b bajo hasta el nivel de precios de las tarjetas de red Ethernet 100BaseT.

Las redes 802.11 son omnipresentes, fáciles de encontrar y, como comprobará en esta explicación, a menudo no requieren ningún esfuerzo para conectarse con ellas. Incluso aunque estén protegidas mediante WEP (que siga siendo una de las contramedidas de seguridad mas habituales en las redes 802.11), las debilidades del protocolo WEP han sido muy explicadas y son conocidas por prácticamente cualquier persona con un mínimo interés en las redes inalámbricas.

GRAFICO 2.1: CRECIMIENTO DEL MERCADO DE DISPOSITIVOS INALAMBRICOS 802.11.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



"Por el contrario, otras redes inalámbricas de paquetes conmutados no son ni de lejos tan habituales, no tienen vulnerabilidades muy conocidas y anunciadas y para su explicación suele necesitarse hardware propietario muy caro y de disponibilidad reducida. Al mismo tiempo, los crackers de redes 802.11 suelen gestionar sus propias redes inalámbricas y utilizar sus equipos tanto para sus actividades ilícitas como para el trabajo en red domestica y en su comunidad".[1]

[1] Vladimirov Andrew A., Seguridad de redes Inalámbricas, EDICIONES AMAYA MULTIMEDIA, Madrid, 2005. Pág. 34-42

Los ataques contra teléfonos GSM y GPRS tienen que ver principalmente con la clonación de uni9dades, lo que se sale del ámbito de hacking inalámbrico. En cuanto a las redes de área personal (PAN, personal área network, la situación con respecto al hacking es mucho mas interesante de explorar desde el punto de vista de la consultaría de seguridad de redes.

Los ataques contra redes personales de infrarrojos son una forma de ataque muy oportunista que se basa en encontrarse en el lugar apropiado en el momento correcto (un cracker tendrá que encontrarse cerca del dispositivo atacado y dentro de un sector de 30 grados a partir de su puerto de infrarrojos).

Ya que la potencia de la radiación infrarroja esta limitada a solo 2 mW, es de esperar que la señal no llegue más allá de los 2 metros. Una excepción a estos limites de 30 grados y 2mW se da en el caso en el que se despliega un punto de acceso infrarrojo (por ejemplo, Compex iRE201) en una oficina o sala de conferencias. En esta situación, todo lo que necesita hacer un cracker para analizar el tráfico y conectarse con la PAN inalámbrica es conectarse en la misma habitación que el punto de acceso. No existe seguridad en la capa 2 (la de enlace) en las redes personales IrDA (Asociación de datos por infrarrojos) y, a menos que se implanten sistemas de autentificación o cifrado en las capas superiores, la red de infrarrojos queda abierta para cualquiera que desee aprovecharse de ella. Los clientes de Windows 2000 y XP se asocian automáticamente con otras máquinas IrDA y la pila del proyecto Linux-IrDA, proporciona una opción de descubrimiento de máquinas IrDA remotas (irattach -s) al igual que irdadump, que es una herramienta similar a tcpdump. Se ha podido utilizar irdaping para bloquear máquinas Windows 2000 que no tuvieran instalados los parches necesarios antes del Service Pack 3. Si desea volcar la información de los paquetes IrDA de la capa 2 de Windows 2000, la interfaz de depuración de infrarrojos de IrCOMM2k (una versión de la pila de Linux-IrDA), realizara un buen trabajo. Sin embargo, no importa como de inseguras sean las redes de

infrarrojos, su uso tan reducido y sus límites en cuanto al alcance físico implican rastrear datos transmitidos mediante la luz jamás serán tan populares como buscar datos transmitidos en las ondas de radiofrecuencia (RF).

Por ese motivo, el warnibbling (buscar paquetes en redes de corto alcance) o la búsqueda de redes Bluetooth se volverá mucho mas popular que buscar conexiones de infrarrojos y podrá llegar a competir en popularidad con el wardriving (buscar redes de largo alcance) en algún momento. Ya hay disponibles herramientas para el descubrimiento de redes Bluetooth como red @Stake y una interfaz de usuario gráfica (GUI) apropiada para esta herramienta () como Bluesniff, de Ssmo. Group) que se puede conseguir y utilizar problemas.

Existen tres factores limitadores de la extensión del hacking de Bluetooth. El primero de ellos es el uso tan limitado aún de esta técnica aunque es probable que esta tendencia cambie en unos pocos años. Otros mediante este protocolo. Sin embargo, los dispositivos Bluetooth de capacidades y puntos de acceso pueden cubrir un área de metros de radio o aun más si utilizan antenas de alta ganancia. Este sirve para ataques remotos. El tercer factor limitado constituyen los mecanismos de seguridad que protegen las redes personales Bluetooth. Hasta el momento no hay ningún ataque conocido que pueda saltarse el cifrado de flujo E0 que se usa para cifrar los datos en las redes personales Bluetooth. Sin embargo, al tiempo que podrá determinar si este sistema propietario de cifrado soportara el principio de Kerckhoff y si la famosa revolución no autorizará repetirse.

Las redes 802.11 ampliamente abiertas que nos rodean

Como ya se ha comentado, en la mayoría de los casos un atacante no tiene que hacer nada en particular para conseguir lo que quiere. Se cree que la mayoría de las redes inalámbricas sin protección eran puntos de acceso de

usuario domestico, redes de comunidades inalámbricas o de puntos de acceso publico, vuelve a estar equivocado. De hecho algunas corporaciones son importantes empresas del mundo de la tecnología de la información (IT) o consultoras relacionadas con el mismo, lo que resulta particularmente lamentable. Ni siquiera nos atrevemos a pensar en el número de las redes 802.11 localizadas que habían implantado medidas de seguridad apropiadas más allá de los estándares del protocolo WEP y el filtrado de direcciones MAC (fáciles de atacar).

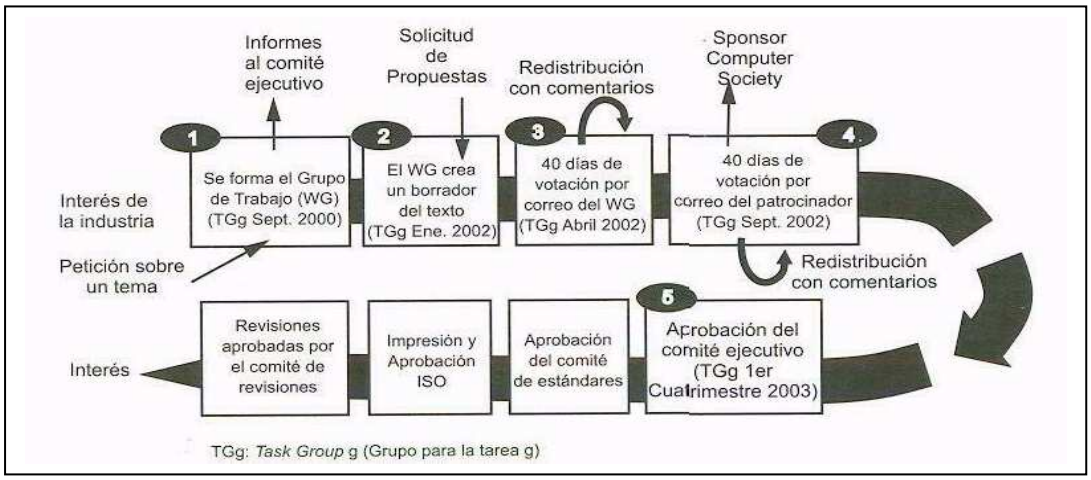
El futuro de la seguridad 802.11

Los estándares 802.11 aliviaran esta situación de por vida, solo el tiempo le dará la razón. Muchos fabricantes comenzaron a lanzar equipos 802.11 g al mercado, a pesar de que el estándar 802.11 no estaba completo. Una gran cantidad de estos productos previos al estándar 802.11 g se comunicaban como superseguros gracias al nuevo estándar. En realidad el estándar 802.11 g, en esencia se trata de la implementación del método de modulación de la capa física de 802.11 a mediante múltiplexación de división ortogonal de frecuencia (OFDM) para una banda ISM media (la banda no regulaba para uso industrial) con el objeto de proporcionar velocidad al estándar 802.11a (el máximo definido por el estándar es de 84 Mb/s), consiguiendo de este modo tanto una alta velocidad de conexión y compatibilidad con el estandar802.11 b o incluso con el espectro disperso de secuencia directa (DSSS) del estándar 802.11 original. Por ello, los intentos del mercado por enlazar el estándar 802.11 g con la seguridad.

Por otra parte, el estándar 802.11 i, es el nuevo estándar de seguridad inalámbrica destinado a sustituir al WEP y a proporcionar una seguridad inalámbrica mucho mas robusta, de acuerdo con sus desarrolladores. Se suponía que 802.11 i se haría publico junto con 802.11 g, pero no vivimos en un mundo perfecto. La versión 1 de la certificación WPA (Wireless

Protected Access) de la Alliance implementa muchas de las características de desarrollo actual 802.11i, pero no todos los productos 802.11g actualmente en el mercado poseen certificación WPA, por el momento existen muchas redes 802.11 que siguen funcionando con versiones antiguas y inseguras del protocolo y hemos visto redes 802.11 g sin ningún tipo de cifrado de datos habilitado claramente debido a administradores poco consistentes de la seguridad.

GRAFICO 2.5: PROCESO DE DESARROLLO DEL PROTOCOLO 802.11 i.
FUENTE: HACKING WIRELESS, ANDREW A VLADIMIROV.



2.2. Metodologías a ser aplicadas para la implementación de las redes inalámbricas.

La seguridad es un aspecto que cobra especial relevancia cuando hablamos 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 institución, bastaría con que estuviese en un lugar próximo donde le llegase la señal. Es más, en el caso de un ataque pasivo, donde sólo se escucha la información, ni siquiera se dejan huellas que posibiliten una identificación posterior.

El canal de las redes inalámbricas, al contrario que en las redes cableadas privadas, debe considerarse inseguro. Cualquiera podría estar escuchando la información transmitida. Y no sólo eso, sino que también se pueden inyectar nuevos paquetes o modificar los ya existentes (ataques activos). Las mismas precauciones que tenemos para enviar datos a través de Internet deben tenerse también para las redes inalámbricas.

Conscientes de este problema, el IEEE publicó un mecanismo opcional de seguridad, denominado WEP, en la norma de redes inalámbricas 802.11. Para solucionar sus deficiencias, el IEEE comenzó el desarrollo de un nuevo mecanismo de seguridad llamado WPA que permitiera dotar de suficiente seguridad a las redes WLAN. También se decidieron utilizar otro tipo de tecnologías como son las VPNs para asegurar los extremos de la comunicación (por ejemplo, mediante IPSec). La idea de proteger los datos de usuarios remotos conectados desde Internet a la red corporativa se extendió, en algunos entornos, a las redes WLAN. Pero la tecnología VPN es quizás demasiado costosa en recursos para su implementación en redes WLAN.

Seguridad WEP

WEP (*Wired Equivalent Privacy*, Privacidad Equivalente al Cable) 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: Se puede habilitar o deshabilitar WEP y especificar una clave de encriptación. Wired Equivalent Privacy (WEP) proporciona transmisión de datos "segura". La encriptación puede ser ajustada a 128 bits, 64 bits o deshabilitada. La configuración de 128 bits da el mayor nivel de seguridad. También hay que recordar que todas las estaciones que necesiten comunicarse deben usar la misma clave para generar la llave de encriptación. Actualmente hay más niveles de WEP: 152, 256 y hasta 512 bits, cuanto más alto es este dato, la comunicación es más segura, a costa de perder rendimiento en la red. También decir que este protocolo no es 100% seguro, que hay software dedicado a violar este cifrado.

Seguridad WPA

WPA (*Wi-Fi Protected Access*, acceso protegido Wi-Fi) es la respuesta de la asociación de empresas Wi-Fi a la seguridad que demandan los usuarios y que WEP no puede proporcionar.

El IEEE tiene casi terminados los trabajos de un nuevo estándar para reemplazar a WEP, que se publicó en la norma IEEE 802.11i a mediados de 2004. Debido a la tardanza (WEP es de 1999 y las principales vulnerabilidades de seguridad se encontraron en 2001), Wi-Fi decidió, en colaboración con el IEEE, tomar aquellas partes del futuro estándar que ya estaba suficientemente madura y publicar así WPA. WPA es, por tanto, un subconjunto de lo que será IEEE 802.11i. WPA (2003) se está ofreciendo en los dispositivos actuales.

WPA soluciona todas las debilidades conocidas de WEP y se considera suficientemente seguro. Puede ocurrir incluso que usuarios que utilizan WPA no vean necesidad de cambiar a IEEE 802.11i cuando esté disponible. Además WPA puede admitir diferentes sistemas de control de acceso incluyendo la validación de usuario-contraseña, certificado digital u otro sistema o simplemente utilizar una contraseña compartida para identificarse.

2.3. Logros e insuficiencias observadas en el sistema de las redes cableadas.

En la actualidad las Redes de Área local (LAN), se encuentran implementadas en toda institución o empresa, pero lo que siempre nos preguntamos o queremos conocer es cual es la ventaja de tener una red cableada o una red inalámbrica, aquí se presenta un estudio minucioso de ventajas y desventajas:

DISEÑO:

Para poder realizar la conexión, conectamos nuestro AP al Switch o Hub mediante un cable de red, y mediante este access point se conectará nuestro equipo inalámbrico. Las computadoras de la red tienen las siguientes características:

RED CABLEADA

PRINCIPAL

- Sistema Operativo Windows 2000 Advanced Server
- Procesador P4 1.8 GHz
- 256 MB de memoria
- Servidor DNS
- Dirección IP: 192.15.1.2
- Gateway: 192.15.1.1 (Dirección IP del Access Point)

EQUIPO 1

- Sistema Operativo Windows XP Profesional
- Procesador P4 2.4 GHz
- 512 MB de memoria

- Dirección IP: 192.15.1.10

EQUIPO 2

- Sistema Operativo Windows 2000 Profesional
- Procesador Pentium 133 MHz
- 64 MB de memoria
- Dirección IP: 192.15.1.11

HUB

- La velocidad de transmisión es de 10 Mbps

EQUIPO INALÁMBRICO

EQUIPO 2

- Sistema Operativo Windows 98 Segunda Edición
- Procesador Pili 1.1 GHz
- 256 MB de memoria
- Dirección IP: 192.15.1.7
- Gateway: 192.15.1.1 (Dirección IP del Access Point)

ACCESS POINT

- Dirección IP: 192.15.1.1

Hay que tomar en cuenta que las antenas de la tarjeta de red inalámbrica como de la del Access point, tienen un alcance de 100 metros indoors (dentro de un edificio) hasta 400 metros outdoors (fuera de un edificio)

Para obtener los resultados de la red, realizaremos un monitoreo de la misma, tanto en su ambiente cableado como de ambiente inalámbrico, mediante un software de monitoreo llamado "WathsUp".

Primeramente buscamos la red existente mediante la propiedad "Net Tools" dentro "WathsUp", obteniendo como resultado la conexión.

Como vemos, se ha detectado las tres computadoras de la red cableada, la computadora con la tarjeta inalámbrica y además el Acces Point describiendo las características de cada una.

PRINCIPAL:

El historial de los tiempos de respuesta que ha tenido el equipo PRINCIPAL durante un período de tiempo, como vemos se ha mantenido estable durante el análisis.

Status O, significa que la computadora se encuentra en estado normal, activo y respondiendo, observamos que no tiene conteos de bajada, y que los servicios que brinda se encuentran activos (DNS, HTTP, SMTP).

VELOCIDAD.-

Para realizar esta determinación tenemos que tomar en cuenta que se utilizó un HUB para conectar la red, el mismo que transmite a una velocidad máxima de 10Mbps.

RED INALÁMBRICA:

La tarjeta utilizada en la conexión alcanza, en teoría, una velocidad de transmisión de hasta 22mbps, al igual que el punto de acceso.

En la práctica alcanzó una velocidad de hasta 9 mbps, tomando en cuenta que el HUB utilizado solo transmite a 10 mbps, podríamos decir que tanto la tarjeta como el AP utilizaron su potencial en la transmisión.

RED CABLEADA:

Dentro de la red cableada, se pudo observar que en los datos se transmitieron a una velocidad un poco mayor que en la red inalámbrica, alcanzando los 10 mbps en todas las tarjetas de la red.

Cabe recalcar que, cuando se realizaron transferencias de archivos, no hubo mayor diferencia entre ambas redes.

COSTOS.-

RED INALÁMBRICA:

La inversión para implementar una red inalámbrica de 4 equipos se muestra en el Cuadro 2.1:

Cuadro 2.1. Costos de una Red inalámbrica

FUENTE: El Investigador

DETALLE	V/UNIT.	V/TOTAL
3 Tarjetas de red inalámbrica PCI:	USD. 18.00	USD. 54.00
1 Access Point :	USD. 82.27	USD. 82.27
TOTAL :		USD. 136.27

Hay que indicar que estos costos se refieren a costos en el mercado Ecuatoriano, pues en nuestro país, se trata de una nueva tecnología y que se encuentra en pleno auge comercial por lo que sus precios son considerados altos con respecto a otos países.

RED CABLEADA:

La inversión en la red cableada se detalla en el cuadro 2.2:

Cuadro 2.2. Costos de una red Cableada

FUENTE: El Investigador

DETALLE	V/UNIT.	V/TOTAL
1 Switch	USD 80.00	USD 80.00
50 metros de cable UTP	USD 0.50	USD 25.00
8 conectores RJ45	USD 0.60	USD 4.80
3 tarjetas de red PCI	USD 15.00	USD 45.00
TOTAL		USD 154.80

Podemos notar claramente que hay una diferencia de USD 19, por lo que sería más conveniente realizar una implementación de una red inalámbrica casera, incluso por su movilidad y versatilidad.
Siempre y cuando se tenga en cuenta que en un futuro no se va a realizar varios cambios en la instalación, pues serían costos adicionales al cableado.

Lo que se puede deducir de este resultado, es que una red cableada tiene un costo mas alto por el costo del alambre, es mejor implementar una red cableada por su anchote banda pero hay que tomar en cuenta que no vaya a ver un cambio de infraestructura del edificio en donde se implantó la red, pues de no ser así sería conveniente utilizar una red inalámbrica.

Como se sabe, las redes LAN son redes que permiten conectar números moderados de computadoras, máximo 30 máquinas, a distancias cortas de hasta 200 metros, tomando en consideración este particular, estudiaremos la factibilidad de cual red sería mejor utilizar para una institución.

En una institución que trabaje con por lo menos 80 estaciones de trabajo divididas en 8 departamentos, el realizar un cableado costana, según cotizaciones consultadas las cuales toman un valor de $ 25.00 por estación,

tendríamos un valor total mínimo de $ 2000.00. Cabe indicar que la estimación del valor es con una configuración y cableado sencillo.

Para el mismo caso, utilizando tecnología inalámbrica y tomando en consideración los precios anteriormente mencionados tendríamos un costo de $1898.16.

Vemos nuevamente que el costo inicial de la tecnología cableada es mayor que si se utilizara tecnología inalámbrica.

Pero que pasaría si la empresa decide hacer cambios de remodelación total de sus oficinas, tendría que hacer un nuevo cableado pagando nuevamente el mismo valor o quizás un valor mayor al inicial de $ 2000.00, con lo que se tendría una cifra demasiado superior a la tecnología inalámbrica.

Cuadro 2.3. Diferencias entre Red inalámbrica y red Cableada
FUENTE: El Investigador

	LAN	**WLAN**
VELOCIDAD	100 mbps	42 mbps
ANCHO DE BANDA (según NetMedic)	15 mbps	15 mpbs
COSTOS: • **Red Casera** • **Red Corporativa (80 máq.)** • **Mantenimiento**	 $ 154.80 $ 2000.00 Depende de los cambios realizados	 $ 136.27 $ 1898.16 No se realizan mayores cambios

Cabe recalcar que la velocidad de la red se determina en su conjunto, en cambio el ancho de banda de determina en la transferencia de archivos.

2.4. Análisis de los resultados obtenidos de las fuentes de información primaria.

Conforme la tecnología avanza los precios de los dispositivos electrónicos van disminuyendo, siendo está una ventaja muy considerable si de ir con la tecnología se trata.

El presente proyecto teóricamente demuestra que implementar una red inalámbrica de bajo costo es factible siempre y cuando exista la disponibilidad para adaptarse a la nueva tecnología.

Las ventajas como se pudieron observar son múltiples en comparación con las redes cableadas ya que en el caso de las inalámbricas el espacio de trabajo es mucho mayor y no tenemos que estar restringidos a la distancia que pueda cubrir el cable, por otro lado los costos son un tanto altos en lo que tiene que ver al concentrador o Access Point o Hub que fue el objeto del estudio ya que los dos trabajan en la capa 1 del modelo de referencia OSI, está es la principal razón por la que se utilizo un Hub en lugar de un Switch y la utilización de un Access Point por un Switch Inalámbrico.

Los costos al momento de elegir la mejor tecnología variaron mínimamente ya que una red cableada y una inalámbrica en dispositivos casi ha emparejado en valores pero en utilidad se concluyo que la inalámbrica es mejor.