FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS / ESCUELA DE TECNOLOGIAS REDES Y TELECOMUNICACIONES

Auditoria de Seguridad Informática y Perimetral en la Empresa Implementos Agropecuarios

Trabajo de titulación presentado en conformidad a los requisitos establecidos para optar por el Título de Tecnólogo en Redes y Telecomunicaciones

Profesor Guía

Ing. Henry Burbano

Autor

Diego Fernando Méndez Noboa

Año

2012

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el/la estudiante, orientando sus conocimientos para un adecuado desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

…….

Henry Burbano

171147608-3

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

"Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes"

.....

Diego Méndez

0603438995

AGRADECIMIEMTO

Quiero agradecer a la Universidad de las Américas por ser la institución que me abrió las puertas hacia el conocimiento, en especial a mi tutor quien fue el guía hacia la conclusión de los objetivos trazados, a la Empresa Implementos Agropecuarios por facilitarme sus instalaciones para la realización del presente proyecto.

DEDICATORIA

El presente trabajo va dedicado a Dios por brindarme la oportunidad de cumplir con mis objetivos bendiciéndome con salud, a mi madre por estar siempre conmigo, así como a mi abuelita y mi padrino por brindarme su apoyo siempre.

RESUMEN

El presente trabajo de investigación, pretende determinar fallas, vulnerabilidades en el caso de haberlas y el estado actual de la red LAN en la Empresa Implementos Agropecuarios para lo cual se ha estructurado un documento con cuatro capítulos con la finalidad de obtener un panorama más amplio del tema a tratar.

Como apertura del documento se presenta de forma general la realización de una investigación previa a la red LAN de la Empresa Implementos Agropecuarios donde se podría determinar posibles problemas que expondrían la seguridad de la información, para de esta forma establecer los parámetros de la auditoria a realizar ,así como la formulación del problema , la realización de objetivos tanto generales como específicos y el alcance la misma.

Una vez determinados los parámetros de la Auditoria se necesitará abordar temas como redes LAN , WAN y seguridades de red los cuales se examinará en diferentes fuentes de consulta como Internet, libros ,revistas, entre otros .Con la información obtenida debidamente tabulada y concisa se realizara el capítulo I llamado marco teórico.

En el capítulo II se presentará el levantamiento de información, en el cual se conseguirá la información sobre equipamiento de la red LAN y WAN de la empresa, así como de la estructura de misma.

Continuando con la estructura del presente documento el capítulo III la auditoria, consiste en pruebas (dentro de los parámetros que la empresa establezca), tanto a nivel físico como a nivel de software con el fin de determinar posibles fallas de seguridad que presenta la red, además este capítulo contiene tablas gráficos de las pruebas realizadas (dependiendo el caso) seguidas por las conclusiones y recomendaciones.

ABSTRACT

The present investigation aims to determine faults, vulnerabilities if any and the current status of the LAN in the Company Agricultural Implements for which a document is structured with four chapters in order to obtain a broader picture of issue to be addressed.

Since opening the document provides a general conducting a preliminary investigation to the LAN Company Agricultural Implements which could identify potential safety problems that expose information, to thereby set the parameters of the audit to make and the formulation of the problem, conducting both general and specific objectives and scope thereof.

Having determined the parameters of the audit will need to address issues such as LAN, WAN and security network which will be discussed in different reference sources like the Internet, books, magazines, among others. With this information properly tabulated and concisely will be held chapter I called theoretical framework.

Chapter II will present the collection of information, which is get information on equipment for the LAN and WAN of the company, as well as the structure itself. Following the structure of this document Chapter III audit is to test (within the parameters established by the company), both physically and in terms of software to identify potential security flaws that shows the network, this chapter also contains tables graphics tests (depending on the case) followed by the conclusions and recommendations.

ÍNDICE

Introducción

En la actualidad las telecomunicaciones y especial el uso redes LAN Y WAN son la principal herramienta de utilización de las empresas para la realización de negocios, por lo que el uso de los estándares de seguridad es la prioridad debido al tipo de información que se maneja, así como la de la rapidez en la transmisión de información .

El manejo adecuado y mantenimiento de la estructura física como: cables, equipos de una red LAN son parte importante ya que un funcionamiento adecuado de los mismos permite un desempeño normal de una red LAN.

Para la realización del presente proyecto, se utilizara métodos de investigación como el analítico-sintético, histórico-lógico, con los cuales se desarrollara temas de forma general en los siguientes:

Redes LAN

“Una red de área local, red local o LAN (del inglés local area network) es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.(http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local)”

Redes WAN

“Una red de área amplia, con frecuencia denominada WAN, acrónimo de la expresión en idioma inglés wideareanetwork, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería RedIRIS, Internet o cualquier red en la cual no estén en un mismo edificio todos

sus miembros (sobre la distancia hay discusión posible). (http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia)”

Seguridad informática

“La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información que se transmite dentro de una red LAN y WAN. Este tipo de información se conoce como información privilegiada o confidencial.

(http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica)”

Políticas de seguridad

El uso de la política de seguridad es un factor importante a través de la implementación de estas se garantiza en parte la correcta administración del cuarto de telecomunicaciones.

ANTECEDENTES

En base a una investigación previa realizada a la red LAN de la empresa Implementos Agropecuarios se detectan varios problemas que exponen la información de la misma y entre los más importantes tenemos:

- No existe un administrador de red dentro de la empresa.
- Falta de documentación de cableado estructurado.
- Poca o ninguna utilización de políticas de seguridad dentro del uso del servidor.

FORMULACIÓN DEL PROBLEMA

La falta de documentación adecuada de la red implementada no permite una correcta administración de la misma, además al no tener un administrador dentro de la planta y al hacerlo de forma remota expone o compromete mucha de la información valiosa para la empresa.

Al no tener políticas de seguridad dentro del servidor se compromete la información y la utilización de la red LAN de la empresa, siendo propensa a daños, pérdida de información, acceso fácil por parte de personas no autorizadas dentro y fuera de la empresa.

OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Determinar fallas, vulnerabilidades y el estado actual de la red LAN en la Empresa Implementos Agropecuarios

OBJETIVOS ESPECÍFICOS

- Recopilar información en libros e Internet que sea útil y conveniente para llevar a cabo la solución del presente problema.
- Analizar toda la información adquirida para determinar el uso adecuado de estándares utilizados en la implementación de la red LAN.
- Verificar la robustez de las seguridades existentes en la red LAN de la empresa Implementos Agropecuarios.
- Establecer el estado actual de la red WAN hasta el punto de servicio del proveedor
- Desarrollar un documento en el cual constará la fundamentación teórica necesaria para el estudio del proyecto, así como las recomendaciones y conclusiones de la auditoría realizada en la empresa Implementos Agropecuarios.

ALCANCE

Después de la auditoría en la red LAN de la Empresa Implementos Agropecuarios se tendrá una idea clara sobre las vulnerabilidades , fallas existentes o no de la red, así como de los estándares de seguridad en redes LAN implementados, políticas de seguridad en la Empresa para lo cual al finalizar se tendrá:

- Resultados obtenidos de la auditoría realizada.
- Documentación en la que constarán conclusiones de la auditoría realizada.
- Recomendaciones para mejorar o corregir los problemas detectados si los hubiera.

ASPECTOS METODOLOGICOS

MÉTODOS:

Histórico lógico

Con el método histórico lógico se podrá analizar la información obtenida en libros revistas o Internet, y así obtener una lógica clara sobre el funcionamiento y evolución de las seguridades en redes.

Analítico sintético

Al utilizar método analítico sintético se podrá tabular la información obtenida a través de la cual podremos llegar a obtener una idea clara de las vulnerabilidades existentes en una red LAN Y WAN.

TÉCNICAS:

Entrevista

Esta técnica permitirá relacionar de una mejor manera el tema propuesto, ya que al haber un contacto directo con los usuarios del servicio de la red se obtendrá información importante para la realización de la auditoria.

CAPITULO I

Marco Teórico

1.1 Red de computadoras

”Una red de computadoras es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información y recursos y ofrecer servicios (http://es.wikipedia.org/wiki/Red_de_computadoras)”.

“La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI (http://es.wikipedia.org/wiki/Red_de_computadoras)”.

1.1.1Clasificación de las redes

1.1.2 Por alcance

- **Red de área local (LAN):** Es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.
- **Red de área local inalámbrica (WLAN):** Es un sistema de comunicación muy utilizado como alternativa a las redes de área local cableadas o como extensión de estas. Utiliza tecnologías de radiofrecuencia que permite mayor movilidad a los usuarios al minimizar las conexiones cableadas.
- **Red de área amplia (WAN):** Es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente.

1.1.3 Por tipo de conexión

Medios guiados

- **El cable coaxial:** Se utiliza para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes.
- **El cable de par trenzado:** Es una forma de conexión en la que dos conductores eléctricos aislados son entrelazados para tener menores interferencias y aumentar la potencia y disminuir la diafonía de los cables adyacentes.

Medios no guiados

- **Red por radio:** Es aquella que emplea la radiofrecuencia como medio de unión de las diversas estaciones de la red.

Por relación funcional

- **Cliente-servidor:** Es una arquitectura que consiste básicamente en un cliente que realiza peticiones a otro programa (el servidor) que le da respuesta.
- **Peer-to-peer:** Es aquella red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí.

1.1.4 Por tecnología

- **Red Point-To-Point:** Este tipo de red requiere, en algunos casos, máquinas intermedias (routers) que establezcan rutas para que puedan transmitirse paquetes de datos.
- **Red Broadcast** se caracteriza por transmitir datos por un sólo canal de comunicación que comparten todas las máquinas de la red. En este caso, el paquete enviado es recibido por todas las máquinas de la red pero únicamente la destinataria puede procesarlo.

1.1.5 Por topología

- **En una red en estrella:** Las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste.

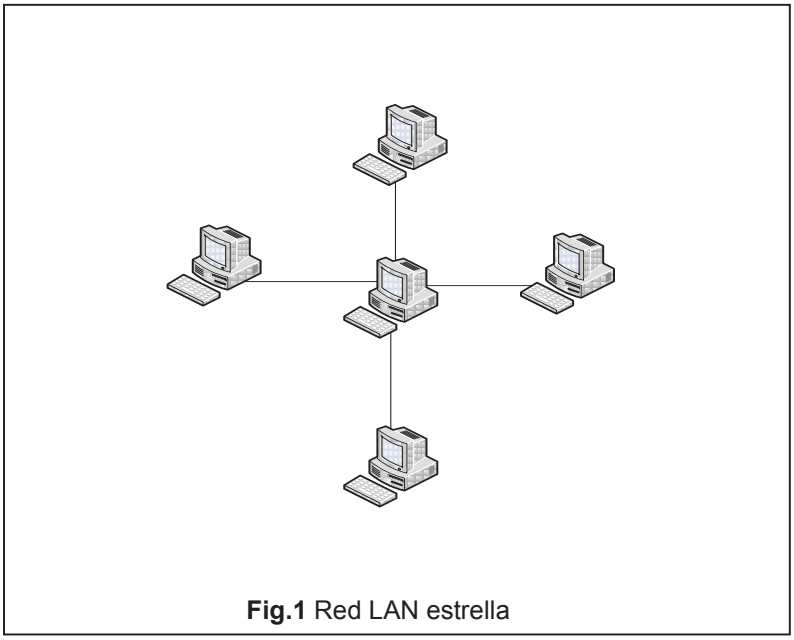


Fig.1 Red LAN estrella

1.2 Cableado Estructurado

“Es el conjunto de elementos pasivos, flexible, genérico e independiente, que sirve para interconectar equipos activos, de diferentes o igual tecnología permitiendo la integración de los diferentes sistemas de control, comunicación y manejo de la información, sean estos de voz, datos, video, así como equipos de conmutación y otros sistemas de administración.

En un sistema de cableado estructurado, cada estación de trabajo se conecta a un punto central, facilitando la interconexión y la administración del sistema, esta disposición permite la comunicación virtualmente con cualquier dispositivo. (http://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf)”

1.2.1“Cable Utp (del inglés:Unshielded Twisted Pair, par trenzado no apantallado) Rj45

RJ-45 (registered jack 45) es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). Es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho pines o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

Fig.2 Cable utp Rj-45

Fuente: http://es.wikipedia.org/wiki/RJ-45

Cable utp por categorías

“Cableado de categoría 1:

Descrito en el estándar EIA/TIA 568B. El cableado de Categoría 1 se utiliza para comunicaciones telefónicas y no es adecuado para la transmisión de datos.

Cableado de categoría 2:

El cableado de Categoría 2 puede transmitir datos a velocidades de hasta 4 Mbps

Cableado de categoría 3:

El cableado de Categoría 3 se utiliza en redes 10BaseT y puede transmitir datos a velocidades de hasta 10 Mbps

Cableado de categoría 4:

El cableado de Categoría 4 se utiliza en redes Token Ring y puede transmitir datos a velocidades de hasta 16 Mbps

Cableado de categoría 5:

El cableado de Categoría 5 puede transmitir datos a velocidades de hasta 100 Mbps o 100 BaseT

Cableado de categoría 6:

Redes de alta velocidad hasta 1Gbps (Equipos).(http://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf)"

El estándar Cat 7:

"Fue creado para permitir 10 Gigabit Ethernet sobre 100 metros de cableado de cobre. El cable contiene, como los estándares anteriores, 4 pares trenzados de cobre.(http://es.wikipedia.org/wiki/Cable_de_Categor%C3%ADa_7)"

1.3 La Voz sobre IP

"(VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares.

1.3.1 Funcionamiento de la voz IP

Los pasos básicos que tienen lugar en una llamada a través de Internet son: conversión de la señal de voz analógica a formato digital y compresión de la señal a protocolo de Internet (IP) para su transmisión. En recepción se realiza el proceso inverso para poder recuperar de nuevo la señal de voz analógica.

Cuando hacemos una llamada telefónica por IP, nuestra voz se digitaliza, se comprime y se envía en paquetes de datos IP.

Estos paquetes se envían a través de Internet a la persona con la que estamos hablando. Cuando alcanzan su destino, son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original. (http://www.ocitel.net/index.php?option=com_content&view=article&id=52:conceptos-de-voip&catid=39:infotelecom&Itemid=65)"

1.3.2 Calidad del servicio

"La calidad de este servicio se está logrando bajo los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda al transmitir menos información.

1.3.3 Ventaja

- Evitar los cargos altos de telefonía (principalmente de larga distancia) que son usuales de las compañías de la Red Pública Telefónica Conmutada.

1.3.4 Desventaja

- "Calidad de la transmisión. Es un poco inferior a la telefónica, ya que los datos viajan en forma de paquetes, es por eso que se pueden tener algunas pérdidas de información y demora en la transmisión. (http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet)"

1.4 Punto de acceso inalámbrico

Fig.3 Acces Point

Fuente: http://www.ordenadores-y-portatiles.com/punto-de-acceso.html

1.4.1 Definición:

“Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming". Por otro lado, una red donde los dispositivos cliente se administran a sí mismos -sin la necesidad de un punto de acceso- se convierten en una red ad-hoc. Los puntos de acceso inalámbricos tienen direcciones IP asignadas, para poder ser configurados.

Son los encargados de crear la red, están siempre a la espera de nuevos clientes a los que dar servicios. El punto de acceso recibe la información, la almacena y la transmite entre la WLAN (Wireless LAN) y la LAN cableada.

Un único punto de acceso puede soportar un pequeño grupo de usuarios y puede funcionar en un rango de al menos treinta metros y hasta varios cientos.

Este o su antena normalmente se colocan en alto pero podría colocarse en cualquier lugar en que se obtenga la cobertura de radio deseada.

El usuario final accede a la red WLAN a través de adaptadores. Estos proporcionan una interfaz entre el sistema de operación de red del cliente (NOS: Network Operating System) y las ondas, mediante una antena inalámbrica. (http://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico)"

1.5 Switch

"Switch traducido significa interruptor. Se trata de un dispositivo inteligente utilizado en redes de área local (LAN - Local Area Network), una red local es aquella que cuenta con una interconexión de computadoras relativamente cercanas por medio de cables.

La función primordial del Switch es unir varias redes entre sí, sin examinar la información lo que le permite trabajar de manera muy veloz, ya que solo evalúa la dirección de destino, aunque actualmente se combinan con la tecnología Router para actuar como filtros y evitar el paso de tramas de datos dañadas. (http://www.informaticamoderna.com/Switch.htm)"

Fig.4 Switch

Fuente: http://www.informaticamoderna.com/Switch.htm

1.5.1 Interconexión de conmutadores y puentes

“Los puentes y conmutadores se conectan unos a los otros pero siempre hay que hacerlo de forma que exista un único camino entre dos puntos de la red. En caso de no seguir esta regla , se forma un bucle o loop en la red, que produce la transmisión infinita de tramas de un segmento al otro. Generalmente estos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

1.5.2 Conexiones en un conmutador Ethernet.

Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de la capa 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos.

En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por lo tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

1.5.3 Bucles de red e inundaciones de tráfico.

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles, que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos.

Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas

inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones. Atendiendo al método de direccionamiento de las tramas utilizadas

1.5.4 Store-and-Forward

Los conmutadores Store-and-Forward guardan cada trama en un búfer antes del intercambio de información hacia el puerto de salida. Mientras la trama está en el búfer, el switch calcula el CRC y mide el tamaño de la misma. Si el CRC falla, o el tamaño es muy pequeño o muy grande (un cuadro Ethernet tiene entre 64 bytes y 1518 bytes) la trama es descartada. Si todo se encuentra en orden es encaminada hacia el puerto de salida.

Este método asegura operaciones sin error y aumenta la confianza de la red. Pero el tiempo utilizado para guardar y chequear cada trama añade un tiempo de demora importante al procesamiento de las mismas. La demora o delay total es proporcional al tamaño de las tramas: cuanto mayor es la trama, más tiempo toma este proceso.

1.5.5 Cut-Through

Los conmutadores cut-through fueron diseñados para reducir esta latencia. Esos switches minimizan el delay leyendo sólo los 6 primeros bytes de datos de la trama, que contiene la dirección de destino MAC, e inmediatamente la encaminan.

El problema de este tipo de switch es que no detecta tramas corruptas causadas por colisiones (conocidos como runts), ni errores de CRC. Cuanto mayor sea el número de colisiones en la red, mayor será el ancho de banda que consume al encaminar tramas corruptas.

Existe un segundo tipo de switch cut-through, los denominados fragment free, fue proyectado para eliminar este problema. El switch siempre lee los primeros 64 bytes de cada trama, asegurando que tenga por lo menos el tamaño mínimo, y

evitando el encaminamiento de runts por la red. (http://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29)”

1.6 Router

1.6.1 Definición

Un router también conocido como encaminador, enrutador, direccionador o ruteador es un dispositivo de hardware usado para la interconexión de redes informáticas que permite asegurar el direccionamiento de paquetes de datos entre ellas o determinar la mejor ruta que deben tomar.

“El router toma decisiones (basado en diversos parámetros) con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego redirige los paquetes hacia el segmento y el puerto de salida adecuados.(http://www.mitecnologico.com/Main/Routers)”

Fig.5 Simbolo de Router

Fuente: http://www.adrformacion.com/cursos/wserver08/leccion1/tutorial6.html

1.6.2 Tipos de routers

“En líneas generales podemos distinguir 2 clases de routers en función del tráfico gestionado:

- Routers de Red Núcleo (Core Routers): se trata de equipamiento de interconexión que constituye la red de datos de los proveedores de Internet o de grandes corporaciones.
- Routers de Salida (Gateway o pasarela): es el equipo con el que se realiza la conexión a Internet o a otra sub-red.

“El módem de ADSL es, generalmente, un router configurados como gateway por el proveedor. Los routers WiFi a todo lo dicho añaden la posibilidad de conexión inalámbrica.(http://www.mitecnologico.com/Main/Routers)”

1.7 Servidores

1.7.1 Definición

Un servidor es una aplicación que se ejecuta dentro de un computador especial o no que provee servicios dentro de una red, a sus clientes (hosts).

1.7.2 Cliente

Son aquellos hosts que utilizan los servicios de una red siempre y cuando tengan los permisos del servidor.

1.7.3 Tipos de servidores

1.7.3.1 Servidor de Correo

Un servidor de Correo es un servicio de red que “Almacenan, envían, reciben, enrutan, y realizan otras operaciones relacionadas con email para los clientes de la red.(http://www.ithinkweb.com.mx/capacita/redes_inf.html)”, principalmente se

usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP.

1.7.3.2 Servidor de correo Exchange

"Es el servidor de correo electrónico de Microsoft ofrece acceso móvil, remoto y de escritorio al correo electrónico con avanzada seguridad y privacidad. (http://es.scribd.com/doc/7456728/Manual-de-Exchange-)"

Exchange Server tiene dos propósitos principales:

1. "Exchange Server soporta POP, IMAP, emails web, así como su propio cliente de correo Microsoft Outlook.
2. Exchange Server permite a los usuarios compartir información, ya sea a travéz de Outlook en sus escritorios o Outlook Web Access a través de un navegador web.(htttp//www.cavsi.com/preguntasrespuestas/que-es-icrosoft-exchange-server/)"

1.7.3.3 Servidor web

Un servidor es un servicio de red que se ejecuta continuamente en un computador, manteniéndose a la espera de peticiones de ejecución que le hará un hosts de la red. "El servidor web se encarga de contestar a estas peticiones de forma adecuada, entregando como resultado una página web o información de todo tipo de acuerdo a los comandos solicitados. (http://www.misrespuestas.com/que-es-un-servidor-web.html)" Un servidor web se le asigna habitualmente el puerto TCP 80.

Fig.6 Servidor Web

Fuente: http://2012computacion.blogspot.com/2012/02/que-es-un-servidor-web.html

1.7.3.4 Servidor Apache HTTP

"El Servidor Apache HTTP es un servidor Web de tecnología Open Source para uso no comercial desarrollado por la Apache Software Foundation (http://www.apache.org). Red Hat Enterprise Linux incluye el Servidor Apache HTTP versión 2.0 así como también una serie de módulos de servidor diseñados para mejorar su funcionalidad.(http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-httpd.html)"

Ventajas

- Código abierto
- Multi-plataforma
- Popular (fácil conseguir ayuda/soporte)

1.7.3.5 Servidor SSH

"SSH (Secure SHell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas

remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo..

Seguridad del SSH

SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos. (http://es.wikipedia.org/wiki/Secure_Shell)"

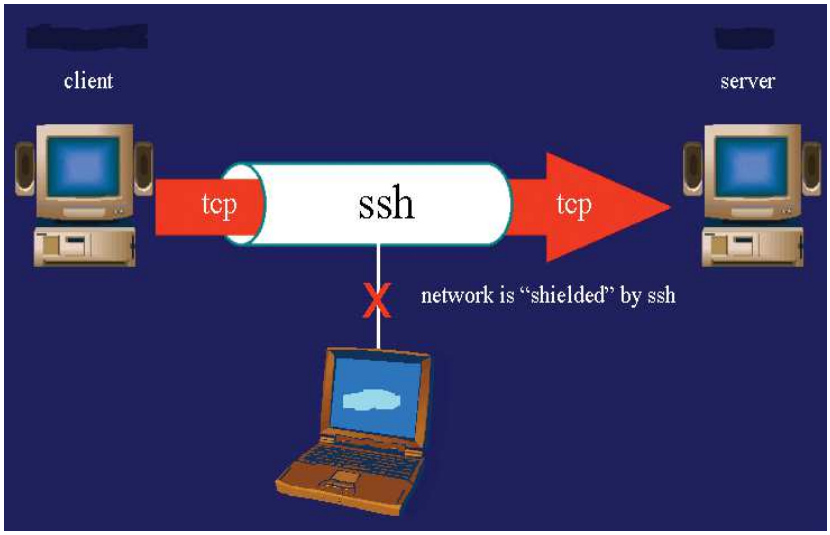


Fig.7 Servidor SSH

Fuente: http://irvingprog.wordpress.com/2010/09/21/conectar-a-servidor-ssh-desde-windows/

1.7.3.6 Servidor Proxy

“Un servidor proxy es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a una sede Web.

El servidor de seguridad del proxy bloquea algunas sedes o páginas Web por diversas razones.

- **Funcionan como servidor de seguridad y como filtro de contenidos.** Son un mecanismo de seguridad implementado por el ISP o los administradores de la red en un entorno de Intranet para desactivar el acceso o filtrar las solicitudes de contenido para ciertas sedes Web consideradas ofensivas o dañinas para la red y los usuarios.

- **Mejoran el rendimiento**

  Guardan en la memoria caché las páginas Web a las que acceden los sistemas de la red durante un cierto tiempo. Cuando un sistema solicita la misma página web, el servidor proxy utiliza la información guardada en la memoria caché en lugar de recuperarla del proveedor de contenidos. De esta forma, se accede con más rapidez a las páginas Web.(http://java.com/es/download/help/proxy_server.xml)”

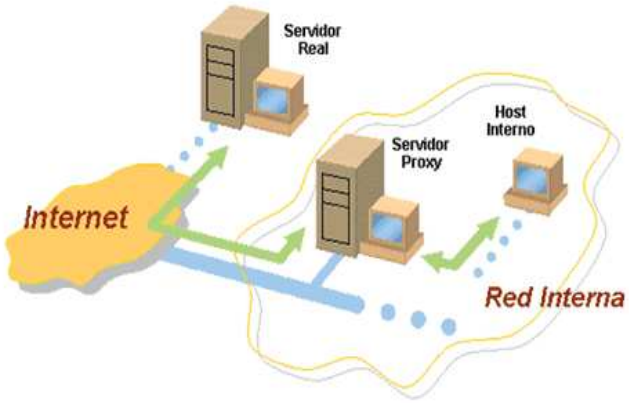


Fig.8 Servidor Proxy

Fuente: http://cinthyapaolacordova.edublogs.org/funcionamiento-basico-de-un-servidor-proxy

1.7.3.7 Servidor DHCP

El protocolo de configuración dinámica de host (DHCP) “es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado.(www.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)”

1.7.3.8 Firewall

Un firewall es un dispositivo (físico o lógico) cuya función es la de permitir o denegar las transmisiones de una red a la otra. Un uso típico es situarlo entre una

red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

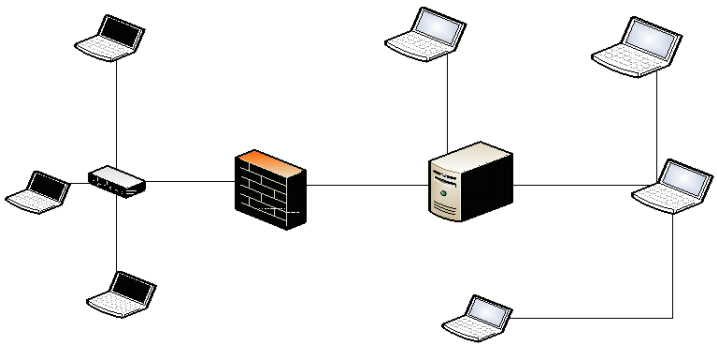


Fig.9 Firewall

1.8 Antivirus

1.8.1 Definición

“En informática los antivirus son programas cuyo objetivo es detectar y/o eliminar software malicioso(Virus).

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, etc.

1.8.2 Métodos de contagio

Existen dos grandes grupos de propagación: los virus cuya instalación el usuario en un momento dado ejecuta o acepta de forma inadvertida, o los gusanos, con los que el programa malicioso actúa replicándose a través de las redes. En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o no previstos. Dichos comportamientos son los que dan la traza del problema y tienen que permitir la recuperación del mismo.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como: «Ejecute este programa y gane un premio».
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software que pueda contener uno o varios programas maliciosos.(http://es.wikipedia.org/wiki/Antivirus)”
- Unidades extraíbles de almacenamiento (USB, CD)

CAPITULO II

Levantamiento de Información

2.1 Distribución de Áreas en la Empresa Implementos Agropecuarios

Primera planta

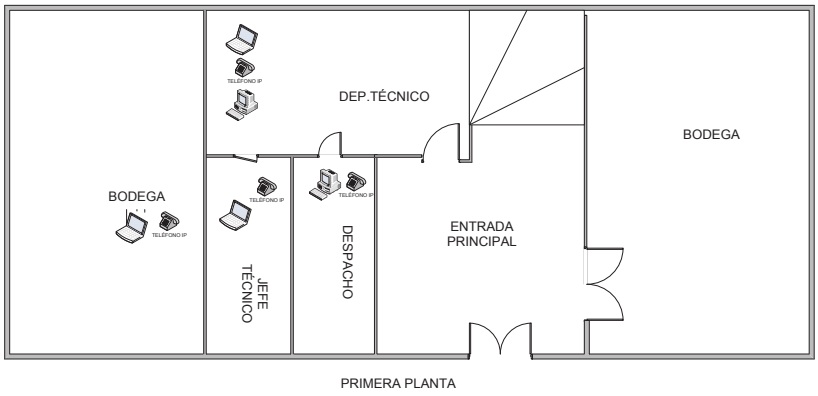


Fig.10 Croquis Primera Planta Empresa Implementos Agropecuarios

Segunda Planta

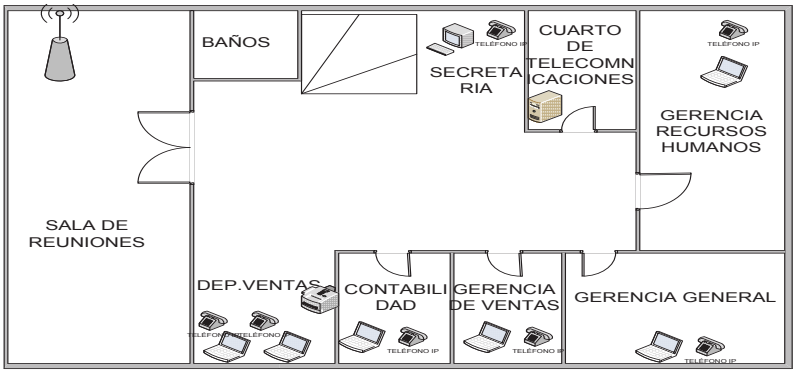


Fig.11 Croquis Segunda Planta Empresa Implementos Agropecuarios

Diagrama o Esquema de red de la empresa.

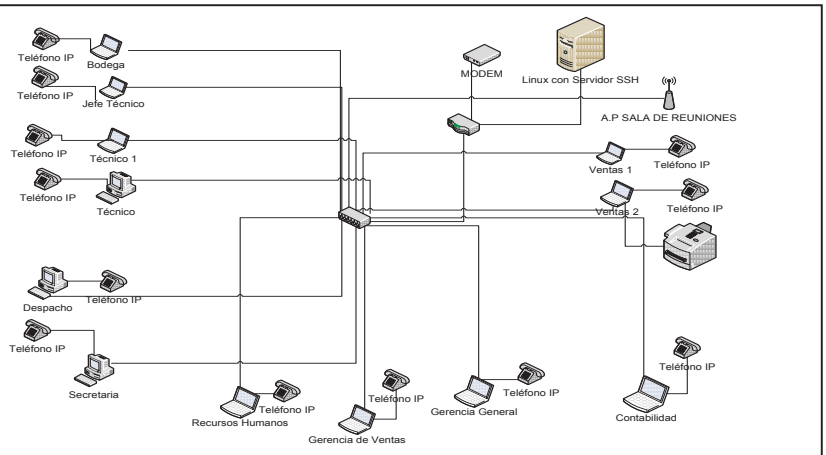


Fig.12 Red Empresa Implementos Agropecuarios

Tabla 1

2.2 Distribución de equipos de la Empresa Implementos Agropecuarios

Distribución de equipos			
Departamentos	# Ptos de red	# Disp.	Equipos
Bodega	1	2	Portátil y Teléfono IP
Contabilidad	1	2	Portátil y Teléfono IP
Despacho	1	2	Pc y Teléfono IP
G. de Recursos Humanos	1	2	Portátil y Teléfono IP
G. de Ventas	1	2	Portátil y Teléfono IP
G. General	1	2	Portátil y Teléfono IP
Recursos Humanos	1	2	Portátil y Teléfono IP
Sala de Reuniones	1	1	Router ,WIFI
Secretaria	1	2	Pc y Teléfono IP
Técnico	4	4	Portátil ,pc, Teléfonos IP
Ventas	3	5	Portátiles ,Teléfonos IP, Impresora
Cuarto de Telecomunicaciones			Servidor ,Modem , Switch, router IP con VoIP, Purificador de aire ,Ups

Descripción de Equipos

2.3.1 DVG-6004S " Router D-Link con VoIP y Gateway

Fig.13 Gateway

Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=894

CARACTERÍSTICAS PRINCIPALES

- Permite usar el equipamiento e infraestructura PBX tradicional existente
- Administra servicios de datos y voz en una misma red
- 4 puertos switch 10/100 integrados.
  (http://www.dlinkla.com/home/productos/producto.jsp?idp=894)"

2.3.2 DES-3028 "FE Switch capa 2 D-Link

Fig.14 Switch

Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=984http

CARACTERÍSTICAS PRINCIPALES

- Switch con 24 puertas FE y 4 puertas GE SFP
- Soporte QoS
- Características avanzadas de administración
- Soporta múltiples estándares y protocolos de administración. (http://www.dlinkla.com/home/productos/producto.jsp?idp=984)"

2.3.3 ADSL2 D-8811 Router D-Link

Fig.15 Router

Fuente: http://www.tp-link.com/mx/products/details/?model=TD-8811

CARACTERÍSTICAS PRINCIPALES

- "Proporciona acceso a Internet a través del servicio ADSL y crea una red cableada de intercambio, todos con un solo producto
- El Firewall integrado lo protege contra ataques de Internet

- Diversas políticas de QoS permiten diversas aplicaciones, para satisfacer las necesidades de las diferentes personas. (http://www.tp-link.com/mx/products/details/?model=TD-8811)”

2.3.4 **FreshAir HEPA** Filtro de aire

Fig.16 Equipo para Filtrar Aire

Fuente: http://ecoquestair.com/shop/living_air/freshair_hepa/

CARACTERÍSTICAS PRINCIPALES

- “Filtro HEPA elimina los contaminantes tan pequeñas, como el polen, caspa de mascotas, el humo, las esporas de moho y el polvo.
- El polvo y gas / Olor Los sensores detectan los niveles de calidad del aire y se indican mediante la pantalla frontal de la unidad.
- Modo automático ajusta automáticamente la velocidad del ventilador para manejar los contaminantes rápidamente. (http://ecoquestair.com/shop/living_air/freshair_hepa/)”

2.3.5 DPH-150SE

INTERNET IP PHONE

"Teléfonos diseñados idealmente para oficina que permiten tomar ventaja de su conexión a internet para hacer llamadas telefónicas de bajo costo.

Fig.17 Teléfono IP

Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=1006

CARACTERÍSTICAS PRINCIPALES

- Comunicación VoIP a través de Internet o red LAN
- 2 Puertos de conexión permite realizar llamadas y navegar al mismo tiempo
- IP asignada mediante , DHCP o estática
- Completo set de características de seguridad, incluyendo Firewall Activo y encriptación WPA2 para proteger su red contra intrusos externos. (http://www.dlinkla.com/home/productos/producto.jsp?idp=1006)"

2.3.6 DIR-300

WIRELESS 11G ROUTER WITH 4-PORT 10/100MBPS SWITCH

"Conectividad inalámbrica para compartir acceso a Internet en el hogar y pequeña oficina

Fig.18 Acces Point

Fuente: http://www.dlinkla.com/home/productos/producto.jsp?idp=1006

CARACTERÍSTICAS PRINCIPALES

- Hasta 54Mbps de velocidad de trasferencia de datos
- Compatible con dispositivos que operen en 802.11b/g
- Switch de 4 puertos para incorporar a red dispositivos cableados
- Soporta encriptación WPA y WPA2.
  (http://www.dlinkla.com/home/productos/producto.jsp?idp=1006)"

2.3.7 Lexmark X464de multifunción

Fig.19 Multifunción

Fuente: www1.lexmark.com/MX/es/catalog/product.jsp?catId=cat1530073&prodId=MX5065

Características:

- “Una opción inteligente y confiable para que impresión dúplex, copia, digitalización y fax de alta velocidad concurran en una sola máquina, a una velocidad que alcanza 40 ppm y con capacidad para digitalizar documentos y enviarlos directamente por correo electrónico o a una unidad flash. (http://www1.lexmark.com/MX/es/catalog/product.jsp?catId=cat1530073&prodId=MX5065)”

Capítulo III

Auditoría

3.1 Informe de Auditoría de Hardware

3.1.1 No existe ventilación adecuada en el cuarto de telecomunicaciones (mediciones de temperaturas en diferentes horarios).

Fig.20 Cuarto de Telecomunicaciones

Fig.21 Temperatura (Mañana)

Fig.22 Temperatura (Tarde)

Fig.23 Temperatura (noche)

Tabla 2

3.1.2 Cuadro de temperatura máxima de equipos.

Equipo	Temperatura máxima de funcionamiento
DVG-6004S (Router)	45°C
DES-3028 (Switch)	40°C
ADSL2 D-8811 (Router)	40°C

Tabla 3

3.1.3 Cuadro de temperatura óptima de trabajo.

Equipo	Temperatura óptima de funcionamiento
DVG-6004S (Router)	22.5°C
DES-3028 (Switch)	20°C
ADSL2 D-8811 (Router)	20°C

Tabla 4

3.1.4 Cuadro de valores de temperatura obtenidos en diferentes horarios del día.

Horario de funcionamiento	Temperatura obtenida
Mañana	27°C
Tarde	34°C
Noche	22°C

Conclusión:

- Los valores de temperatura obtenidos muestran claramente que, en un determinado momento (Tarde) del día llegan a comprometer el correcto funcionamiento de lo equipos porque que este bordea el nivel máximo de tolerancia de los mismos.

Recomendación:

- Utilizar sistemas de sistemas adecuados de enfriamiento dentro del cuarto de telecomunicaciones.

3.1.5 No existe etiquetado adecuado en puntos de red.

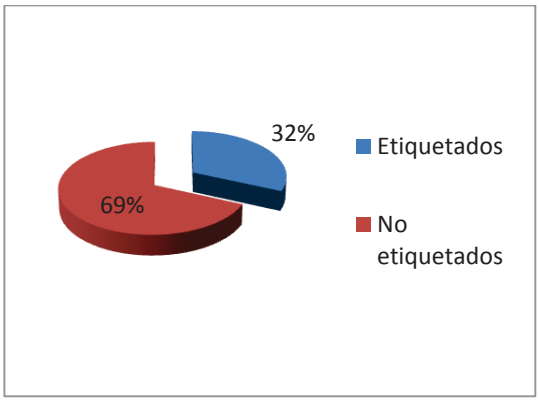
En la Fig. 3.5 se visualiza utilización de cinta adhesiva para identificar un punto de red lo cual no es la forma adecuada de realizar un etiquetado.

Fig.24 Etiquetado Inadecuado

Tabla 5

3.1.6 Tabla y gráfica de etiquetas en puntos de red.

Puntos de red	Porcentaje
Etiquetados	32%
No etiquetados	69%
Total	100%



Nota: Se utiliza el total de puntos de red existentes (16) y se determina el porcentaje de etiquetados(5) , y no etiquetados (11) repectivamente.

Conclusión:

- Con el escaso o incluso inadecuado uso de etiquetas, una labor de mantenimiento dentro de la red se hace extremadamente laboriosa, lo que representaría una respuesta poco efectiva el momento de solucionar un problema.

Recomendación:

- Tomando en cuenta que el 62% de los puntos de red no se encuentran etiquetados, se recomienda volver a etiquetar los mismos ya que no representaría un costo elevado para la empresa, facilitando el mantenimiento de la red o solucionar requerimientos futuros.

3.1.7 Poca utilización de estándares para la construcción de cables

En la Fig. 3.3 se observa que la protección del cable se encuentra fuera del conector lo que indica el poco cuidado al momento de haberlo elaborado.

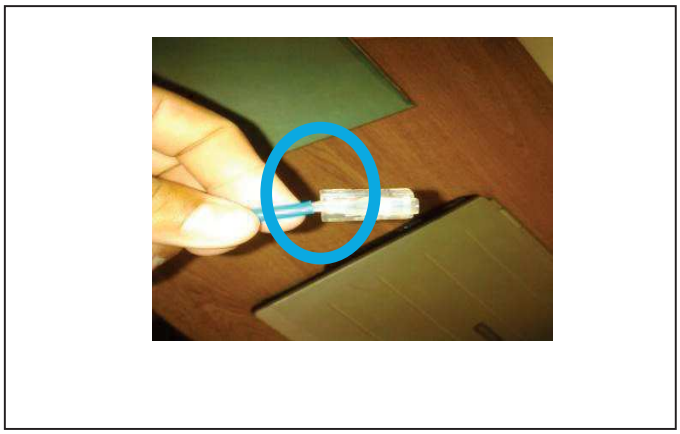
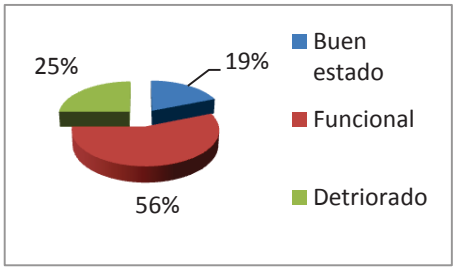


Fig.25 Cable en malas condiciones

Tabla 5

3.1.8 Tabla y gráfica de Cable UTP (patch cord)

Patch cord	Porcentaje
Buen estado	19%
Funcional	56%
Deteriorado	25%
Total	100%



Nota: Se utiliza el total de patch cord utilizados (16) se determina el porcentaje de buen estado (3), funcional (9), y deteriorado (4) repectivamente.

Buen estado: Todo aquel cable que físicamente no tienen mucho deterioro y tienen conectividad (comando ping).

Funcional: Todo cable que físicamente se encuentra deteriorado (fig. 3.3) y tiene conectividad (comando ping).

Deteriorado: Todo cable que no tiene conectividad (comando ping).

Conclusión:

- Un 75% entre buen estado y funcional de los patch cord que se utilizan en la red tienen conectividad, pero no es lo optimo ya que toda la red es vinculante y al utilizar cables no adecuados se puede presentar efectos como retrasmisiones o efectos de antena entre otros dentro de la red de la empresa, provocando incluso perdidas de información.

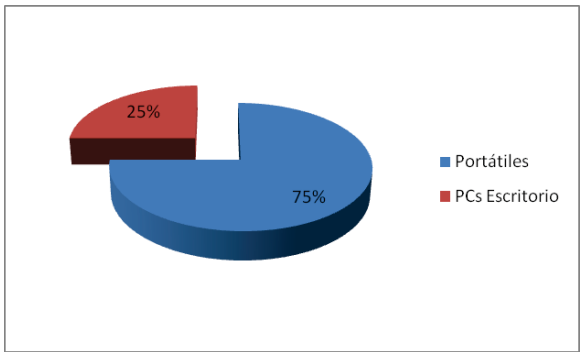
Recomendación:

- Al tener un 25% de los patch cord en completo deterioro recomienda el remplazo de los mismos y contar con patch cord adicionales para futuros inconvenientes.
- Realizar certificación del cableado, ya que la prueba de conectividad realizáda es básica (comando ping).

Tabla 6

3.1.9 Tabla y gráfica de equipos utilizados dentro de la empresa.

Equipos	Porcentaje
Portátiles	75%
PCs Escritorio	25%
Total	100%



Nota: Se utiliza el total de equipos portátiles y de escritorio utilizados (12) por los usuarios y se determina el porcentaje de portátiles (9) , y Pcs de escritorio (3) repectivamente.

Conclusión:

- Al poseer un 75% de equipos portátiles, la empresa como tal tiene movilidad dentro de la misma, adicionalmente los recursos de la red inalámbrica son aprovechados de una forma eficiente.

Recomendación:

- Así como la movilidad es una ventaja de los equipos portátiles, también pueden ser una desventaja, por cuanto pueden ser objetos de robo con mayor facilidad por lo que se recomienda utilizar correas o candados de seguridad para estos equipos.

3.2 Informe de Auditoría de Software

El mantenimiento de software se lo hace de forma remota (no hay administrador de red). Servidores de correo, web son administrados por la empresa Novanet.

3.2.1 Comprobación de asignación dinámica de dirección IP. Con la realización de esta prueba se comprobara: el servicio de asignación dinámica de dirección IP y la máscara de red.

a) Ingresar a recursos de red clic derecho sobre el icono de tarjeta de red.

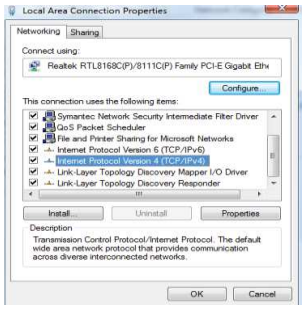


Fig.26 Ventana de propiedades de tarjeta de red

b) Seleccionar la opción protocolo internet IPV4, dar clic sobre propiedades y verificar que la opción obtener dirección IP automáticamente este seleccionada.

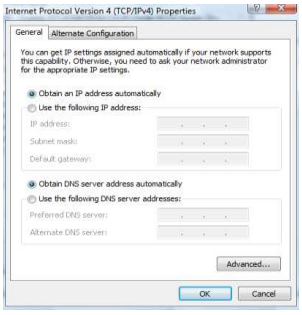


Fig.27 Ventana para asignar dir IP

c) Una vez comprobada que está habilitada la opción de dirección IP automática lo siguiente es determinar cuál es la dirección IP asignada y saber cuál es su máscara, para lo cual se presiona la tecla del logotipo de Windows + R (Abre el cuadro de diálogo Ejecutar)

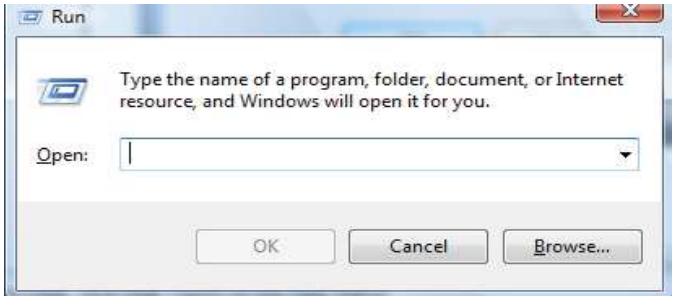


Fig.28 Ventana para ejecutar

d) Tipiar el comando cmd y luego presionar ok con lo cual se abrirá la ventana de comandos (MS-DOS) de Windows dentro de se tipea el comando ipconfig.

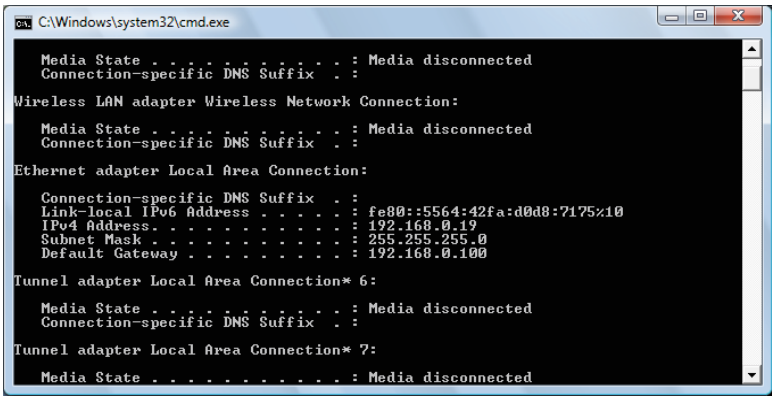


Fig.29 Comprobación de dir IP

Conclusión:

- Al asignarse una dirección IP de forma dinámica es un claro indicador de que el servidor DHCP se encuentra activo así como se pone en evidencia que no se encuentra realizado subneting porque la máscara de red indica 255.255.255.0.

Recomendación:

- Al asignar la dirección IP apenas un equipo se conecta a la red de la empresa permite que este aproveche sus recursos como el Internet lo que genera un consumo del ancho de banda, por lo que se recomienda tener un control de acceso a los puntos de red, así como realizar subnetig por áreas de trabajo de acuerdo al número de equipos que se encuentren.

3.2.2 Comprobación de ancho de banda online.

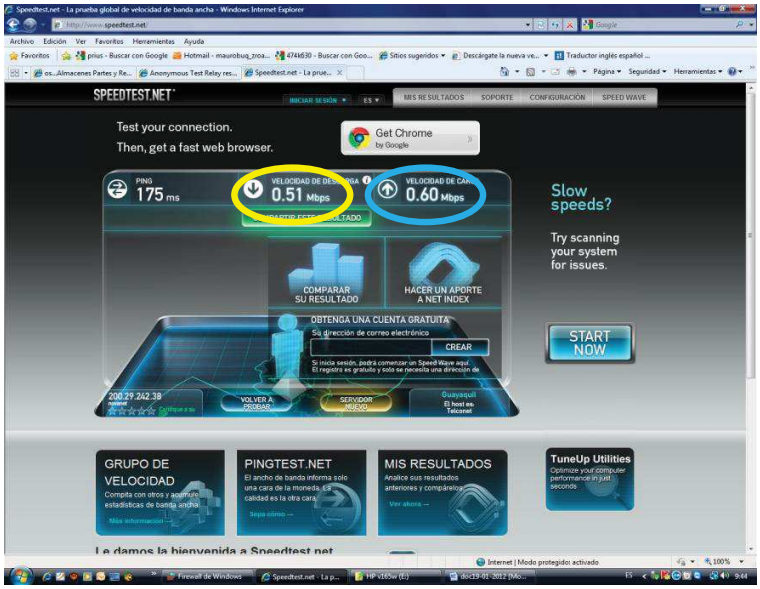


Fig.30 Prueba online ancho de banda

Fuente:http://www.speedtest.net/

Velocidad ofrecida por el Proveedor	Velocidad obtenida en Medidor de velocidad online promedio
Velocidad de carga **0.75Mbps**	Velocidad de carga **0.60Mbps**
Velocidad de descarga 0**.50Mbps**	Velocidad de descarga **0.41 Mbps**

Conclusión:

- Los valores obtenidos al momento de la medición son normales ya que generalmente entre un 10% Y 20% del ancho de banda se consume en el envío de paquetes, tráfico de red,de sincronización.

Recomendación:

- Mantener el servicio contratado.

Tabla 7

3.2.3 Escaneo de puertos online.

Puerto	Nombre	Estado	Información
20	FTP Data	Cerrado	Puerto utilizado en modo activo para el proceso de transferencia de datos FTP.
21	FTP	Cerrado	Servicio para compartir archivos FTP.
22	SSH	Abierto	Secure SHell, utilizado principalmente para conexión por línea de comandos entre otras muchas funciones. Uso casi exclusivo para Linux, en Windows algunas aplicaciones pueden abrirlo.
23	Telnet	Cerrado	Telecomunication NETwork permite controlar un equipo remotamente. Puerto potencialmente peligroso.

25	SMTP	Cerrado	Telecommunication NETwork, usado para envío de correo electrónico. Un puerto muy escaneado para aprovechar vulnerabilidades para el envío de SPAM. Asegúrate de validar usuarios para el envío de correo.
53	DNS	Cerrado	Sistema de nombre de dominio, utilizado para resolver la dirección IP de un dominio.
79	Finger	Cerrado	Informa al cliente datos sobre los usuarios conectados a un determinado servicios del servidor. Puede revelar información no deseada.
80	HTTP	Abierto	Servidor Web. Utilizado para navegación web. Este servicio por si solo ya supone un riesgo, suele ser escaneado y se las ingenian para encontrar nuevas entradas por el.
110	POP3	Cerrado	Una de las formas de acceder a los correos de tu cuenta de correo electrónico personal.
119	NNTP	Cerrado	Servidor de noticias.
135	NetBIOS	Cerrado	Remote Procedure Calls. Usado para compartir tus archivos en red, usar unicamente en red local y no hacia Internet, ya que cualquiera podría acceder al contenido que compartas de tu ordenador. Es habitual encontrarlo abierto en Windows.
139	NetBIOS	Cerrado	Usado para compartir servicios compartidos de impresoras y/o archivos. Potencialmente peligroso si se encuentra abierto ya que se puede

			acceder a un gran contenido del equipo.
143	IMAP	Cerrado	Otra forma de acceder a los correos electrónicos de tu cuenta de correo electrónico personal. Mas moderna que el POP3 y con una funcionalidad similar.
443	HTTPS	Cerrado	Usado para navegación Web en modo seguro. Se usa junto con un certificado de seguridad. Los comercios electrónicos por ejemplo aseguran sus ventas gracias a este servicio.
443	AOL Instant Messenger	Cerrado	Popular cliente de mensajería instantánea.
563	POP3 SSL	Cerrado	Conexión POP3 pero con cifrado SSL. Una forma más segura de acceder a los correos electrónicos de tu cuenta personal ya que el intercambio de datos se realiza cifrado por medio de Secure Socket Layer (SSL).
993	IMAP4 SSL	Cerrado	Una forma más segura de acceder a los correos de tu cuenta personal por medio cifrado Secure Socket Layer (SSL), cifrando los datos de la comunicación.

995	POP3 SSL	Cerrado	Conexión POP3 pero con cifrado SSL. Una forma más segura de acceder a los correos electrónicos de tu cuenta personal ya que el intercambio de datos se realiza cifrado por medio de Secure Socket Layer (SSL).
1080	Proxy	Cerrado	Servicio de proxy. Garantiza a los clientes del servicio mas seguridad en las conexiones en Internet, ya que tu IP no aparece en las conexiones, apareciendo la IP del servidor proxy.
1723	PPTP	Cerrado	Virtual private network (VPN). Puerto usado para conectar equipos por medio de Red Privada Virtual.
3306	MySQL	Abierto	Base de datos MySQL. La base de datos usada de forma mas frecuente como complemento a las páginas web dinámicas.
8080	Proxy Web	Cerrado	Una forma de navegar más privada por Internet, ya que el servidor oculta tu IP al navegar por Internet.

Nota: Con esta herramienta online se comprobará el estado actual de los puertos habilitados (abiertos) o inhabilitados (cerrados) y así poder determinar posibles vulnerabilidades. http://www.puertosabiertos.com/es/escaner-de-puertos.htm).

Conclusión:

- De acuerdo al escaneo realizado se determina que la red se encuentra insegura ya que podría ser víctima de ataques como: intercepción pasiva de paquetes, alteración, reproducción de comandos, y denegación de servicio. porque el puerto 3306 (MYSQL) se encuentra abierto.

Recomendación:

- Se recomienda cerrar el puerto 3306 (MYSQL) ya que este puerto se encuentra activo y en caso de utilizarlo crear listas de acceso ACL para tener un mayor control de quien accede a este servicio de red.

3.2.4 Obtención de Dirección IP del servidor de dominio web, online.

Esta herramienta online permite obtener la dirección IP del servidor web de la empresa basados en la dirección web de la misma la cual es www.ics.com.ec

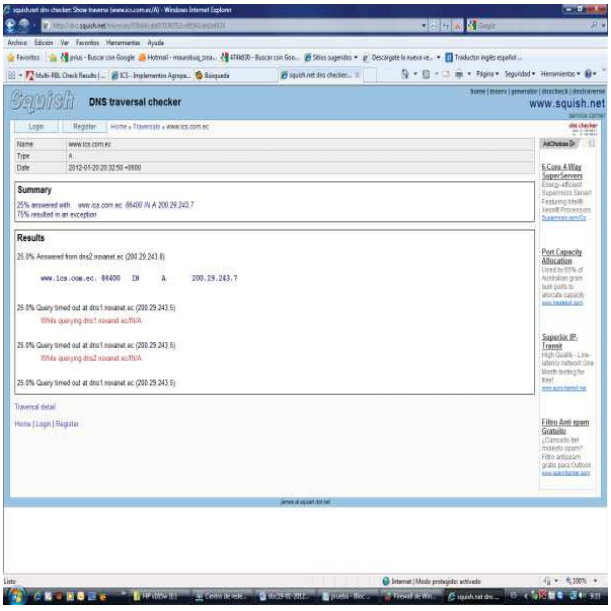


Fig.31 Obtencion de dirección IP del servidor

Fuente: http://dns.squish.net/

3.2.5 Prueba para determinar que servidor de correo externo posee la empresa Implementos Agropecuarios.

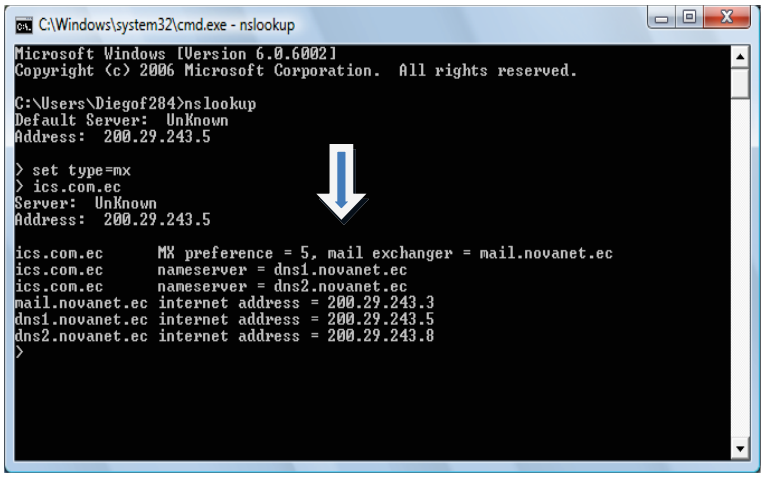


Fig.32 Comprobación de tipo de servidor de correo

Conclusión:

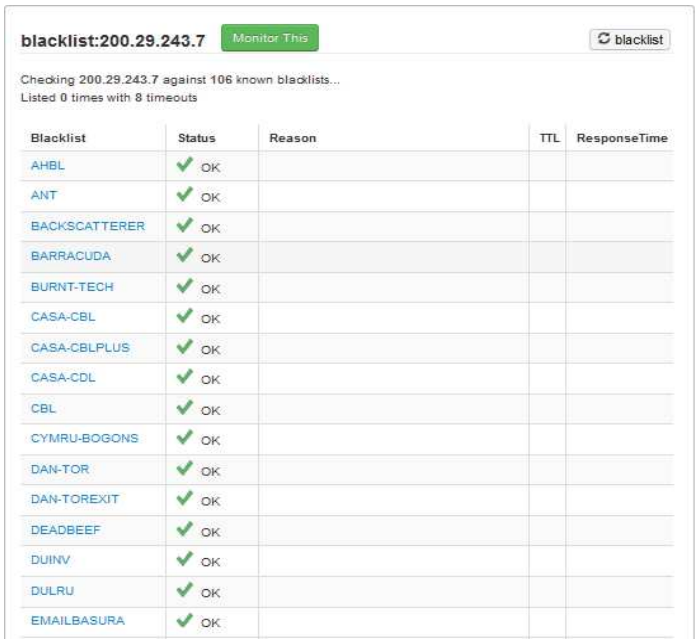
- Se realiza una prueba exitosa ya que el comando nslookup permitió determinar el tipo de servidor de correo que la empresa posee.

Recomendación:

- Se recomienda utilizar el comando nslookup para determinar el tipo de servidor de correo que se posee.

3.2.6 Comprobación online de la pertenencia o no de la IP de la Empresa Implementos Agropecuarios en listas negras. 200.29.243.7 ,en el sitio www.mxtoolbox.com.

"Una lista negra (o black list) es una lista donde se registran las direcciones IPs que generan spam de forma voluntaria o involuntaria. (http://www.dnsqueries.com/es/mi_ip_esta_en_lista_negra.php)"



blacklist:200.29.243.7 Monitor This blacklist

Checking 200.29.243.7 against 106 known blacklists...
Listed 0 times with 8 timeouts

Blacklist	Status	Reason	TTL	ResponseTime
AHBL	OK			
ANT	OK			
BACKSCATTERER	OK			
BARRACUDA	OK			
BURNT-TECH	OK			
CASA-CBL	OK			
CASA-CBLPLUS	OK			
CASA-CDL	OK			
CBL	OK			
CYMRU-BOGONS	OK			
DAN-TOR	OK			
DAN-TOREXIT	OK			
DEADBEEF	OK			
DUINV	OK			
DULRU	OK			
EMAILBASURA	OK			

Fig.33 Comprobacion de pertenecía o no a listas negras

Fuente: www.mxtoolbox.com.

Conclusión:

- Al finalizar la prueba online se observa que la IP de la empresa no se encuentra dentro de las listas negras, lo cual demuestra una buena administración de la misma

Recomendación

- Seguir manteniendo las políticas actuales de administración.

3.2.7 Prueba de open relay servidor de correo, en el sitio www.mailradar.com/openrelay**.**Con esta herramienta virtual se puede determinar la vulnerabilidad del servidor de correo de la empresa. “Se denomina ataque por Open Relay al mecanismo de usar el MTA (Mail Transport Agent, Agente de Transporte de Correo) como puente para correos. (http://es.wikipedia.org/wiki/Open_Relay)”

Fig.34 Comprobación de vulnerabilidad del servidor de correo

Fuente: www.mailradar.com/openrelay

Conclusión:

- Al finalizar la prueba online de open relay del servidor de correo de la empresa, se obtiene resultados favorables ya que pasa el test sin ningún inconveniente.

Recomendación:

- Seguir manteniendo las políticas actuales de administración del servidor de correo.

3.2.8 Comprobación wireless SSID (Service Set IDentifier).

A través de esta prueba se determina la visibilidad o no del identificador de red.

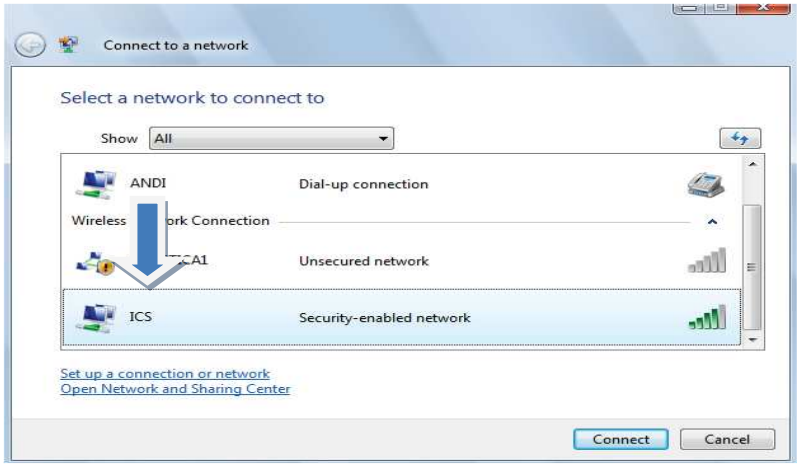


Fig.35 Ventana de redes WIFI visibles

Conclusión:

- El SSID se encuentra visible lo que representa un potencial problema de seguridad, ya que al tener acceso se podría intentar ingresar a la red interna de la empresa ocasionando un posible ataque o utilización de recursos como el Internet.

Recomendación:

- Ocultar el SSID esto es posibles hacerlo dentro de las opciones que tiene el equipo de la empresa encargado de brindar el servicio de WIFI.

3.2.9 Comprobación de petición de clave para conexión WIFI

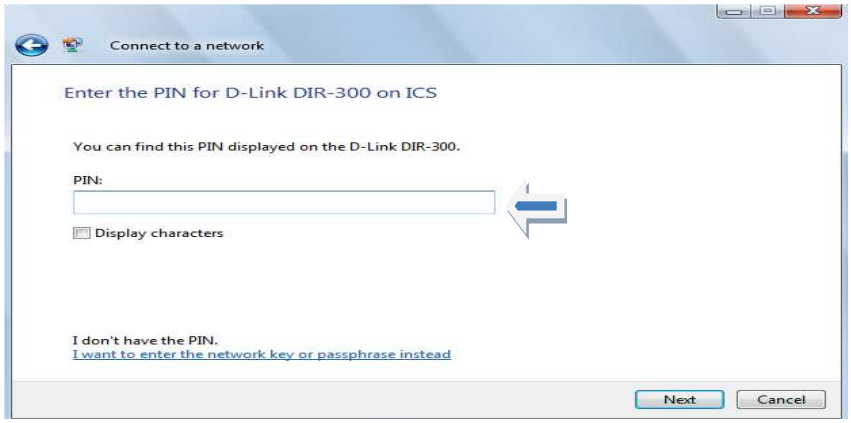


Fig.36 Ventana de petición de clave de acceso a red WIFI

Conclusión:

- La petición de clave para el ingreso en la red inalámbrica de la empresa indica que no cualquiera puede ingresar en la misma y hacer uso de los recursos de red.

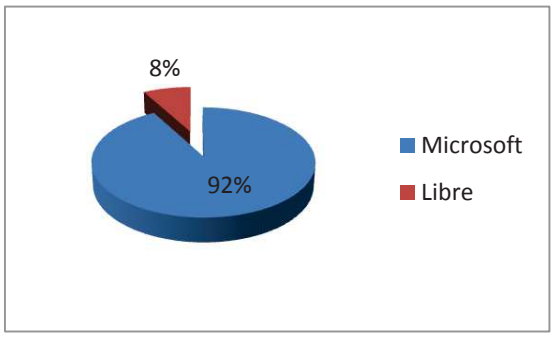
Recomendación:

- Seguir manteniendo las políticas actuales, cambiar con frecuencia la clave utilizando números y caractéres especiales.

Tabla 8

3.2.10 Tabla y gráfica de sistema operativo utilizado.

Sistema Operativo	Porcentaje
Microsoft	92%
Libre	8%
Total	100%

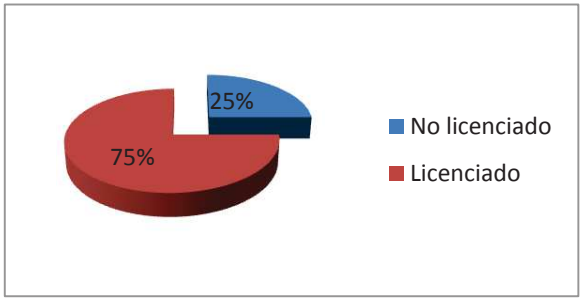


Nota: Se utiliza el total de sistema operativo utilizado (13) y se determina el porcentaje de sistema operativo Microsoft (12) , y el sistema operativo Libre (1) repectivamente.

Tabla 9

3.2.11 Análisis de licenciamiento del sistema operativo Microsoft.

Sistema Operativo	Porcentaje
No licenciado	25%
Licenciado	75%
Total	100%



Nota: Se utiliza el total de sistema operativo Mircrosoft utilizado (12) y se determina el porcentaje de sistema operativo Microsoft con licencia (9) , y el sistema operativo Microsoft sin licencia (3) repectivamente.

Conclusión:

- Al ser Microsoft un 92% del sistema operativo que se utiliza en la empresa y de este valor un 75% se encuentra licencenciado demuestra que hay el interés por parte de la misma en mantener software legal.

Recomendación:

- Tan solo al faltar un 25% de software de Microsoft por licenciarse se recomienda hacerlo y así evitar sanciones o inconvenientes futuros.

3.2.12 Comprobación del nivel de seguridad de contraseñas.

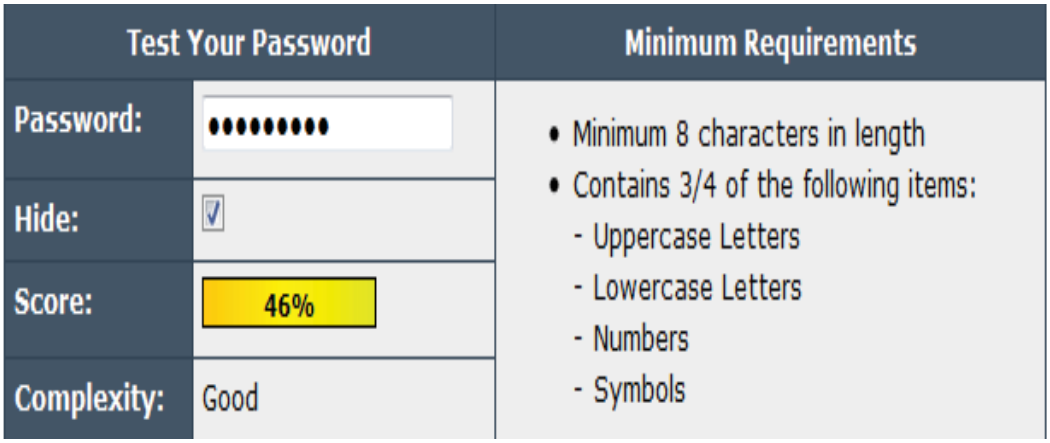


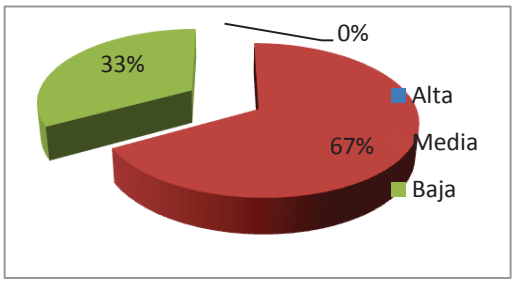
Fig.37 Comprobación del nivel de seguridad de contraseñas

Fuente: www.passwordmeter.com

Tabla 10

3.2.13 Tabla y gráfica de seguridad de contraseñas.

Seguridad de contraseñas	Porcentaje
Alta	0%
Media	67%
Baja	33%
Total	100%



Nota: Se utiliza el total de contraseñas utilizadas (12) por los usuarios y se determina el porcentaje de seguridad alta (0) ,media(8) y baja (4) repectivamente.

Conclusión

- De acuerdo al análisis realizado existe un 33% de contraseñas inseguras lo cual significa que es un punto débil y de mucho cuidado ya que sería fácil vulnerarlos en ingresar a la red de la empresa.

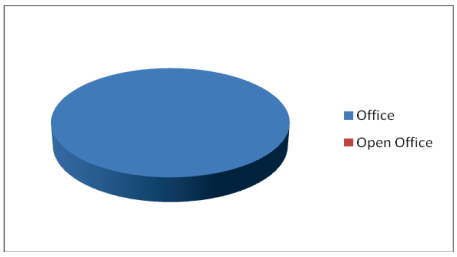
Recomendación

- Se sugiere la utilización de contraseñas más seguras utilizando un número mayor de caracteres y entre estos utilizar números letras y caracteres especiales.
- Establecer políticas de contraseñas.

Tabla 11

3.2.14 Tabla de software de ofimática.

Software	Porcentaje
Office	100%
Open Office	0%
Total	100%

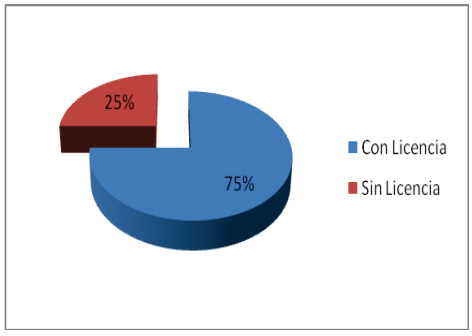


Nota: Se utiliza el total de software ofimático utilizado (12) y se determina el porcentaje correspondiente a Office (12) , y Open Office (0) repectivamente.

Tabla 12

3.2.15 Tabla de software de ofimática con licencia.

Software de Ofimática	Porcentaje
Con Licencia	75%
Sin Licencia	25%
Total	100%



Nota: Se utiliza el total de software ofimático Office utilizado (12) y se determina el porcentaje de sistema ofimático Office con licencia (9) , y el sistema ofimático Office sin licencia (3) repectivamente.

Conclusión:

- El 75% de lo equipos se encuentra con software de ofimática licenciado lo que indica que mantienen una política buena de software.

Recomendación:

- En caso de no poder adquirir licencias para el 25% restante de equipos se recomienda utilizar software libre como el Open Office.

3.2.16 Comprobación de respuesta de antivirus Kaspersky "La prueba EICAR (nombre oficial: EICAR Standard Anti-Virus Test File) es una prueba para probar la respuesta de los programas antivirus en el equipo. La razón detrás de esto es permitir a las personas, empresas y programadores de antivirus, probar su software sin tener que utilizar un verdadero virus informático que pudiera causar daño real al no responder el antivirus correctamente. (http://es.wikipedia.org/wiki/EICAR)"

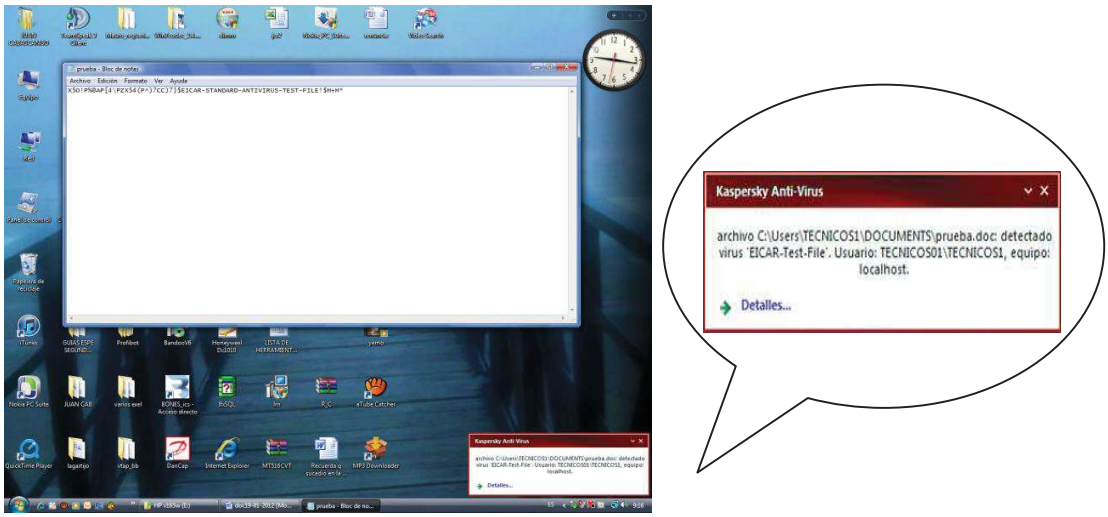
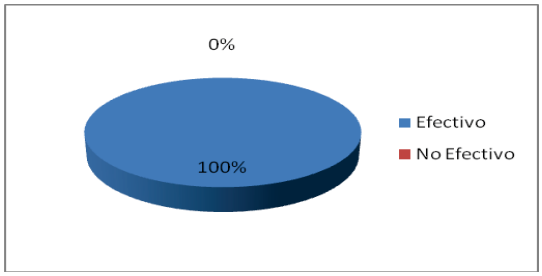


Fig.38 Comprobación de antivirus

Tabla 13

3.2.17 Tabla y gráfica de prueba de antivirus Kaspersky. (EICAR)

Prueba	Porcentaje
Efectivo	100%
No Efectivo	0%
Total	100%



Conclusión:

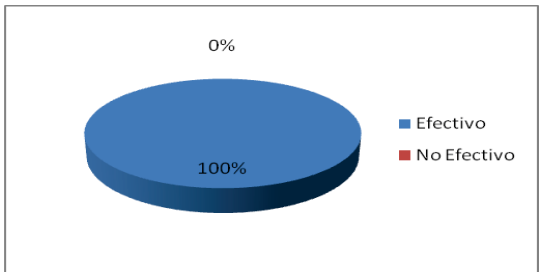
- La respuesta obtenida con la simulación de un posible ataque o amenaza ha sido 100% efectiva (protección del equipo) por parte del antivirus.

Recomendación:

- Seguir manteniendo las políticas actuales como son actualizaciones automáticas de antivirus.

3.2.18 Análisis de licenciamiento del Antivirus.

Software Licenciado	Porcentaje
Licenciado	100%
No licenciado	0%
Total	100%



Conclusión:

- Al poseer 100% de software licenciado indica un buen manejo de protección de quipos a nivel de software.

Recomendación:

- Actualizar de forma periódica el antivirus utilizado.

3.2.18 Comprobación de acceso al internet.

La prueba consiste en verificar acceso a redes sociales, paginas pornográficas y aplicaciones P2P como el ares.

Fig.39 Comprobación de acceso a internet

Fuente: www.facebook.com

Conclusión

- No existe restricciones en el acceso a redes sociales (Facebook, twitter. entre otras) así como páginas pornográficas, o aplicaciones P2P lo cual puede significar que parte del tiempo de trabajo sea mal empleado en la revisión de las mismas.

Recomendación:

- Implementar políticas de acceso a Internet ya que los recursos de red no están siendo aprovechadas de una manera adecuada.

REFERENCIAS

http://2012computacion.blogspot.com/2012/02/que-es-un-servidor-web.html
http://cinthyapaolacordova.edublogs.org/funcionamiento-basico-de-un-servidor-proxy/
http://ecoquestair.com/shop/living_air/freshair_hepa/
http://es.scribd.com/doc/7456728/Manual-de-Exchange-
http://es.wikipedia.org/wiki/Antivirus
http://es.wikipedia.org/wiki/Cable_de_Categor%C3%ADa_7
http://es.wikipedia.org/wiki/Conmutador_%28dispositivo_de_red%29
http://es.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
http://es.wikipedia.org/wiki/EICAR
http://es.wikipedia.org/wiki/Open_Relay
http://es.wikipedia.org/wiki/Punto_de_acceso_inal%C3%A1mbrico
http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_amplia
http://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local
http://es.wikipedia.org/wiki/Red_de_computadoras, 2012
http://es.wikipedia.org/wiki/RJ-45
http://es.wikipedia.org/wiki/Secure_Shell
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet
http://irvingprog.wordpress.com/2010/09/21/conectar-a-servidor-ssh-desde-windows/
http://java.com/es/download/help/proxy_server.xml
http://mxtoolbox.com/SuperTool.aspx?action=blacklist%3a200.29.243.7
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/ch-httpd.html
http://www.adrformacion.com/cursos/wserver08/leccion1/tutorial6.html
http://www.cavsi.com/preguntasrespuestas/que-es-microsoft-exchange-server/
http://www.dlinkla.com/home/productos/producto.jsp?idp=1006

http://www.dlinkla.com/home/productos/producto.jsp?idp=1006
http://www.dlinkla.com/home/productos/producto.jsp?idp=894
http://www.dlinkla.com/home/productos/producto.jsp?idp=984
http://www.dnsqueries.com/es/mi_ip_esta_en_lista_negra.php
http://www.informaticamoderna.com/Switch.htm
http://www.ithinkweb.com.mx/capacita/redes_inf.html
http://www.mailradar.com/openrelay/
http://www.misrespuestas.com/que-es-un-servidor-web.html
http://www.mitecnologico.com/Main/Routers
http://www.mitecnologico.com/Main/Routers
http://www.ocitel.net/index.php?option=com_content&view=article&id=52:conceptos-de-voip&catid=39:infotelecom&Itemid=65
http://www.ordenadores-y-portatiles.com/punto-de-acceso.html
http://www.passwordmeter.com/
http://www.tp-link.com/mx/products/details/?model=TD-8811
http://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf
http://www.uazuay.edu.ec/estudios/electronica/proyectos/cableado_estructurado.pdf

ANEXOS

“El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el Departamento de Defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa de dicho departamento. (http://es.wikipedia.org/wiki/Familia_de_protocolos_de_Internet)”

El cliente

“El cliente establece y origina las llamadas realizadas de voz, esta información se codifica, se empaqueta y se transmite a través del micrófono (entrada de información) del usuario, de la misma forma la información se decodifica y reproduce a través de los altavoces o audífonos (salida de la información).(http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet)”

“Un Cliente puede ser un usuario de Skype o un usuario de alguna empresa que venda sus servicios de telefonía sobre IP a través de equipos como (Adaptadores de teléfonos analógicos) o teléfonos IP o Softphones que es un software que permite realizar llamadas a través de una computadora conectada a Internet.

Los servidores

Los servidores se encargan de manejar operaciones de base de datos, realizado en un tiempo real como en uno fuera de él. Entre estas operaciones se tienen la contabilidad, la recolección, el enrutamiento, la administración y control del servicio, el registro de los usuarios, etc.

Usualmente en los servidores se instala software denominados Switches o IP-PBX (Conmutadores IP), ejemplos de switches pueden ser "Voipswitch", "Mera", "Nextone" entre otros, un IP-PBX es Asterisk uno de los más usados y de código abierto.

Los gateways

Los gateways brindan un puente de comunicación entre todos los usuarios, su función principal es la de proveer interfaces con la telefonía tradicional adecuada, la cual funcionara como una plataforma para los usuarios (clientes) virtuales.

Los Gateways se utilizan para "Terminar" la llamada, es decir el cliente Origina la llamada y el Gateway Termina la llamada, eso es cuando un cliente llama a un teléfono fijo o celular, debe existir la parte que hace posible que esa llamada que viene por Internet logre conectarse con un cliente de una empresa telefónica fija o celular.(http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet)”

Comprobación de redundancia cíclica(CRC)

“La comprobación de redundancia cíclica (CRC) es un código de detección de errores usado frecuentemente en redes digitales y en dispositivos de almacenamiento para detectar cambios accidentales en los datos.(http://es.wikipedia.org/wiki/Comprobaci%C3%B3n_de_redundancia_c%C3%ADclica)”

Estándar VoIP (SIP)

(Session Initiation Protocol) "Protocolo de Inicio de Sesión" por sus siglas en inglés es un protocolo reciente que es en la actualidad el mayormente utilizado.

VoIP no es un servicio, es una tecnología

“En muchos países del mundo, IP ha generado múltiples discordias, entre lo territorial y lo legal sobre esta tecnología, está claro y debe quedar en claro que la tecnología de VoIP no es un servicio como tal, sino una tecnología que usa el Protocolo de Internet (IP) a través de la cual se comprimen y descomprimen de manera altamente eficiente paquetes de datos o datagramas, para permitir la comunicación de dos o más clientes a través de una red como la red de Internet. Con esta tecnología pueden prestarse servicios de Telefonía o Videoconferencia, entre otros.(http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet)”

Arquitectura de red

Propio Estándar define tres elementos fundamentales en su estructura:

- Terminales: son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.
- Gatekeepers: son el centro de toda la organización VoIP, y son el sustituto para las actuales centrales, normalmente implementan por software, en caso de existir, todas las comunicaciones que pasen por él.
- Gateways: se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario. (http://es.wikipedia.org/wiki/Voz_sobre_Protocolo_de_Internet)"

Diferencia entre la Telefonía IP de la telefonía normal

"En una llamada telefónica normal, la central telefónica establece una conexión permanente entre ambos interlocutores, conexión que se utiliza para llevar las señales de voz.

En una llamada telefónica por IP, los paquetes de datos, que contienen la señal de voz digitalizada y comprimida, se envían a través de Internet a la dirección IP del destinatario. Cada paquete puede utilizar un camino para llegar, están compartiendo un medio, una red de datos. Cuando llegan a su destino son ordenados y convertidos de nuevo en señal de voz.(http://www.ocitel.net/index.php?option=com_content&view=article&id=52:conceptos-de-voip&catid=39:infotelecom&Itemid=65)"

Glosario

ADSL:“(sigla del inglés Asymmetric Digital Subscriber Line) es un tipo de tecnología de línea DSL. Consiste en una transmisión analógica de datos digitales apoyada en el par simétrico de cobre que lleva la línea telefónica convencional o línea de abonado, siempre y cuando la longitud de línea no supere los 5,5 km medidos desde la Central Telefónica, o no haya otros servicios por el mismo cable que puedan interferir.(http://es.wikipedia.org/wiki/L%C3%ADnea_de_abonado_digital_asim%C3%A9trica)”

ANSI:**“**El Instituto Nacional Estadounidense de Estándares (ANSI, por sus siglas en inglés: American National Standards Institute) es una organización sin ánimo de lucro que supervisa el desarrollo de estándares para productos, servicios, procesos y sistemas en los Estados Unido.(http://es.wikipedia.org/wiki/Instituto_Nacional_Estadounidense_de_Est%C3%A1ndares)”

Auditor:“Una persona o empresa encargada de realizar un análisis independiente, sobre el funcionamiento de una organización, para luego emitir su opinión.(www.deguate.com/infocentros/gerencia/glosario/a.htm)”

Dirección IP:“Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP.(http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP)”

EIA:“(Electronic Industries Association) Asociación vinculada al ámbito de la electrónica. Es miembro de ANSI. Sus estándares se encuadran dentro del nivel 1 del modelo de referencia OSI.(www.segu-info.com/glosario/?id=53)”

Estándares:“Consiste en el establecimiento de normas a las que debe ajustarse la información geográfica, los procesos de intercambio de ésta y la interoperación

de los sistemas que deben manejarla.(www.idera.gov.ar/web/idera/conceptos-acerca-de-las-ide)”

IEEE:“Instituto de Ingenieros Eléctricos y Electrónicos (USA). Su Comité de Estándares para las Tecnologías Educativas trabaja con el objetivo de desarrollar estándares técnicos, prácticas recomendadas y guías para la implementación informática de sistemas de formación y educación.(www.educ.cl/index.php)”

Protocolo:“Es un conjunto de reglas usadas por computadoras para comunicarse unas con otras a través de una red por medio de intercambio de mensajes.(http://es.wikipedia.org/wiki/Protocolo_%28inform%C3%A1tica%29)”

TIA: Asociacion de Industrias de Telecomunicaciones