FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

ESCUELA DE TECNOLOGÍAS REDES Y TELECOMUNICACIONES

AUDITORÍA DE SEGURIDAD INFORMÁTICA INTERNA Y PERIMETRAL DE LA EMPRESA MARKETWATCH EN EL ÁREA DE OPERACIONES

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

Carlos Alberto Vergara Vargas

2012

DECLARACIÓN DEL PROFESOR GUÍA

"Declaro haber dirigido este trabajo a través de reuniones periódicas con el 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."

.....

Ing. 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”

……..

Carlos Vergara

171827747-6

AGRADECIMIENTOS

La presente Tesina es un esfuerzo en el cual, directa o indirectamente, participaron varias personas, leyendo, opinando, corrigiendo, teniéndome paciencia, dando ánimo, acompañando en los momentos de crisis y en los momentos de felicidad.

DEDICATORIA

A mis padres, porque creyeron en mí y me sacaron adelante, dándome ejemplos dignos de superación y entrega, porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles y porque el orgullo que sienten por mí, fue lo que me hizo ir hasta el final.

RESUMEN

La presente tesina tiene por objeto realizar una auditoría de seguridad informática en la empresa Marketwatch, la cual ayudará a la detección de errores y dar a conocer cuáles son las falencias que tiene la misma y de esta manera dar soluciones oportunas para que sean implementadas en caso de ser requeridas.

En esta auditoría se plantea realizar pruebas, tanto en la parte de software y hardware, para que de esta manera, llegar a obtener un informe final en el cual se va a dar a conocer cuáles son las vulnerabilidades que se encontró en la presente auditoría y dar las respectivas soluciones y recomendaciones.

ABSTRACT

The present work is to conduct an audit of computer security in the company Marketwatch, which help detect errors and make known what are the weaknesses that have the same and thus provide appropriate solutions to be implemented in case being required.

This audit raises testing, both the software and hardware, so that in this way, reaching get a final report which will make known what are the vulnerabilities that are found in this audit and to the respective solutions and recommendations.

ÍNDICE

INTRODUCCIÓN

La presente tesina, está enfocada a la realización de una auditoria de sistemas de la seguridad interna y perimetral de la empresa Marketwatch en el Área de Operaciones, para que de esta manera se pueda ver cuáles son sus falencias en cuanto a seguridad de la red en general, tanto en la parte de software y hardware.

Para realizar este trabajo de investigación, se recurrió primeramente a realizar el levantamiento de información de manera minuciosa en el área a investigar (Operaciones), la cual cuenta con 3 estaciones de trabajo, en la cuales se va a proceder a realizar evaluaciones a cada una de las máquinas y ver si es que las mismas están acorde con las políticas de seguridad que debe tener una empresa para no sufrir posibles ataques informáticos, ya sean externos o internos.

Además se analizarán si los equipos con los que cuenta la empresa son los que realmente necesita acorde al tamaño de la misma, o también recomendar si a futuro se puede implementar algún equipo o tecnología.

Por último se va a elaborar un informe final, en el cual va a constar en detalle la auditoría realizada al área de operaciones de la empresa Marketwatch con todas observaciones que se encontró en el transcurso de esta investigación y de esta manera poder llegar a dar las respectivas soluciones y dependiendo del caso una que otra recomendación para el óptimo desempeño de la red en cuanto a su seguridad interna.

Cabe destacar que este trabajo tiene por objeto la obtención del título profesional de Tecnólogo en Redes y Telecomunicaciones.

CAPÍTULO I: MARCO TEÓRICO

1.1 ANTECEDENTES

- La empresa Marketwatch dedicada a realizar estudios de mercado se encuentra ubicada en la ciudad de Quito y en la cual se va a proceder a realizar una auditoría específicamente en el área de operaciones.

- Cuenta en su nómina con 14 empleados.

- Dentro de su infraestructura física cuenta con 19 estaciones de trabajo.

- Tiene de una red de cableado estructurado mediante el cual se tiene acceso a Internet tanto alámbrico como inalámbrico.

- Tiene un servidor con Windows Server 2008 y sus estaciones de trabajo cuentan con Windows Xp y Windows 7.

- Cableado interno categoría 5e.

- Conexión inalámbrica mediante router.

En la figura 1.1 se puede observar el rack con los diferentes equipos de telecomunicaciones como son: switch, router, central telefónica con que cuenta la empresa.

Fig 1.1 Rack

Equipo	Modelo	Descripción
Switch Dlink	DES 1024	Fast Ethernet 10/100 Base-TX
Router Dlink	DIR 300	802.11 b/g
Router Cisco	1700	Configuración VPN
Central Telefónica Panasonic	KX-Tes824	Análoga

Fig 1.2 Tabla equipos del rack

En la figura 1.3 muestra una toma eléctrica regulada, además de los puntos de voz y datos.

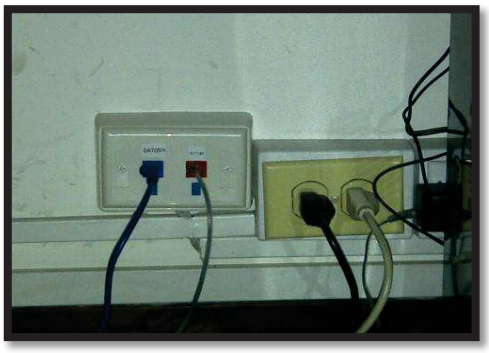


Fig 1.3 Puntos Voz – Datos y toma eléctrica

El la figura 1.4 se puede observar el servidor de la empresa

Fig 1.4 Servidor

En cuanto a la infraestructura física, posee equipos como router, switch y una central telefónica así como un servidor que administra las funciones de red de la empresa, figura 1.1, así como puntos de voz – datos como se aprecia en la figura 1.3 y el servidor en la figura 1.4.

1.1.1 FORMULACIÓN DEL PROBLEMA

- La empresa no tiene información referente a la infraestructura de la red.
- Se desconoce el nivel de seguridad en la red inalámbrica.

1.1.2 OBJETIVO GENERAL

- Detectar vulnerabilidades en el área de operaciones, evaluando su estructura de red y de software para generar un documento que sirva de referencia para las respectivas correcciones de los problemas que puedan presentarse.

1.1.3 OBJETIVOS ESPECÍFICOS

- Evaluar la situación actual de hardware.
- Evaluar la situación actual de software.
- Evaluar la situación actual en relación a la seguridad.
- Elaborar un documento con un resumen de la auditoría y evaluación de resultados obtenidos.

1.1.4 ALCANCE

- Revisar la infraestructura de red de la empresa Marketwatch para ver si está o no acorde a las necesidades de la misma.
- Verificar políticas de seguridad implementadas en las estaciones de trabajo.
- Chequear que todos los puntos de red estén etiquetados correctamente para tener mayor facilidad para detectar problemas.
- Se va a evaluar exclusivamente al área de operaciones de la empresa Marketwatch que cuenta con 3 estaciones de trabajo, la auditoría será de software y hardware.
- Elaborar documento final con las respectivas conclusiones y recomendaciones para que la empresa pueda tomar decisiones en base al informe de la auditoría.

1.1.5 JUSTIFICACIÓN DEL PROYECTO

- Se realizará la auditoría para encontrar y evaluar si existen vulnerabilidades que pueda tener la empresa Marketwatch en su organización interna y de esta manera sugerir la aplicación de acciones correctivas.

- Esta auditoría ayudará a implementar políticas, y elaborar documentación de toda la infraestructura de red para la empresa.

1.2 CONCEPTOS GENERALES DE AUDITORÍA

1.2.1 AUDITAR

“Conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un sistema informático con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente de acuerdo con las normas informáticas y generales existentes en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente”.

http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

Como se sabe en cualquier empresa, siempre los sistemas informáticos son la parte más delicada y susceptible a daños dentro de la infraestructura de una empresa, ya que se pueden convertir en un blanco fácil de hackers si no se tiene las debidas seguridades, por lo que estos sistemas, tienen que siempre estar sometidos a un riguroso control por parte de las personas encargadas de su del mismo.

1.2.2 PAPEL DEL AUDITOR

El papel del auditor está encaminado hacia la búsqueda de problemas o vulnerabilidades que se puedan encontrar en el sistema informático y la infraestructura de una empresa y al mismo tiempo dar las respectivas soluciones y recomendaciones para solucionar los inconvenientes encontrados.

1.2.3 AUDITORÍA INTERNA Y AUDITORÍA EXTERNA

Existen dos grupos generales de auditorías, la interna y la externa, y de cada una de estas existen subgrupos según las necesidades que requiera una empresa.

AUDITORÍA INTERNA

"Existe por expresa decisión de la empresa, es decir que también se puede optar por su disolución en cualquier momento.

AUDITORÍA EXTERNA

Es realizada por personas afines a la empresa se presupone una mayor objetividad que en la auditoría interna debido Al mayor distanciamiento entre auditor y auditado.

La auditoria informática tanto interna como externa debe ser una actividad exenta de cualquier contenido o matiz político ajena a la propia estrategia y política general de la empresa".

http://vbarreto.ve.tripod.com/keys/audi/audi01.html

Como se mencionó anteriormente los dos tipos de auditoría tanto interna como externa, para la empresa Marketwatch se realizó una auditoría interna tanto de la parte de sistemas, así como la de red y a continuación se detalla en que consiste cada una de estas dos auditorías.

1.2.4 AUDITORÍA INFORMÁTICA DE SISTEMAS

“Se ocupa de analizar la actividad que se conoce como técnica de sistemas, en todos sus factores. La importancia creciente de las telecomunicaciones o propicia de que las comunicaciones, líneas y redes de las instalaciones informáticas se auditen por separado, aunque formen parte del entorno general del sistema.

1.2.5 AUDITORÍA INFORMÁTICA DE COMUNICACIÓN Y REDES

Este tipo de auditoría deberá inquirir o actuar sobre los índices de utilización de las líneas contratadas con información sobre tiempos de uso y de no uso, deberá conocer la topología de la red de comunicaciones, ya sea la actual o la desactualizada. Deberá conocer cuantas líneas existen, como son, donde están instaladas, y sobre ellas hacer una suposición de inoperatividad informática. Todas estas actividades deben estar coordinadas y dependientes de una sola organización”.

http://vbarreto.ve.tripod.com/keys/audi/audi01.html

Es para este efecto que se realizan las auditorías dentro de las cuales hay un sin fin de procesos que se deben seguir entre los cuales se destaca algunas metodologías, pero para este trabajo se utilizará la metodología de CRMR.

1.2.6 METODOLOGÍA CRMR

CRMR (Computer Resource Management Review) que traduciendo significa Evaluación de la gestión de recursos informáticos. Esta metodología ayuda a evaluar la eficiencia y rendimiento de los recursos con los que cuenta un sistema informático.

Cabe señalar que realizar una auditoría con la metodología CRMR, no tiene el mismo grado de complejidad de lo que tiene una auditoría global, pero la ventaja de utilizar este tipo de metodología es que se va a encontrar soluciones mucho más rápidas a los inconvenientes que se presenten en el transcurso de la misma.

1.2.7 OBJETIVO CRMR

La metodología CRMR tiene como objetivo principal evaluar el grado de vulnerabilidad o ineficiencia de los procedimientos y métodos de gestión que se aplica para la administración del sistema informático. Las recomendaciones que se emitan del resultado de aplicar esta metodología, tendrán como único fin, dar a conocer las recomendaciones necesarias para su posterior aplicación en cuanto a la mejora del sistema e infraestructura.

1.2.8 ALCANCE CRMR

Se debe fijar los límites que abarcará el CRMR, antes de empezar la auditoría.

Se establecen tres clases:

Reducido: El resultado consiste en señalar las áreas sobre las cuales se va a intervenir y ver su futuro potencial para la obtención inmediata de beneficios.

Medio: La metodología CRMR establece las respectivas conclusiones y recomendaciones como se las realiza en una auditoría común.

Alto: Aquí se incluye planes detallados de acción, incluyendo técnicas para la implementación de las recomendaciones, así como las conclusiones finales.

Para el caso de la auditoría que se lleva a cabo en la empresa Marketwatch se va a utilizar la metodología de clase medio.

1.2.9 INFORMACIÓN NECESARIA PARA LA REALIZACIÓN DEL CRMR

Los usuarios son los que facilitarán la información que el auditor necesite para realizar la auditoría y su posterior informe final.

A continuación de muestra una lista completa de los datos necesarios para obtener el CRMR:

- Informes de anomalías de los sistemas.
- Procedimientos estándar de actualización.
- Monitoreo de los Sistemas.
- Informes del rendimiento de los Sistemas.
- Gestión de Espacio en disco.
- Utilización de CPU, canales y discos.

Esta información debe abarcar todo el entorno del CRMR para realizar un seguimiento de las recomendaciones finales.

1.3 CONCEPTOS DE TELECOMUNICACIONES

1.3.1 ¿QUÉ ES UNA RED?

Se conoce como red a un conjunto de computadores o dispositivos conectados por cables entre sí permitiendo compartir información y recursos.

Las redes varían en tamaño; pueden ser de área local para pequeños negocios o de área extendida a nivel de ciudades o países.

1.3.2 TIPOS DE REDES

Existen diferentes tipos de redes privadas y se diferencian según:

Su tamaño, velocidad de transferencia de datos y cobertura.

Las redes privadas se caracterizan porque pertenecen a una misma organización.

Entre las principales categorías que existen tenemos las siguientes redes:

- LAN (Red de área local).
- MAN (Red de área metropolitana).
- WAN (Red de área extendida).

LAN

> "LAN significa Red de área local. Es un conjunto de equipos que pertenecen a la misma organización y están conectados dentro de un

área geográfica pequeña mediante una red, generalmente con la misma tecnología (la más utilizada es Ethernet)".
http://es.kioskea.net/contents/initiation/types.php

MAN

"MAN (Red de área metropolitana) conecta diversas LAN cercanas geográficamente (en un área de alrededor de cincuenta kilómetros) entre sí a alta velocidad. Por lo tanto, una MAN permite que dos nodos remotos se comuniquen como si fueran parte de la misma red de área local además de tener conexiones de alta velocidad (Fibra Óptica)". http://es.kioskea.net/contents/initiation/types.php3

WAN

"WAN (Red de área extendida) conecta múltiples LAN entre sí a través de grandes distancias geográficas.

Las WAN funcionan con routers, que pueden "elegir" la ruta más apropiada para que los datos lleguen a un nodo de la red.

La WAN más conocida es Internet". http://es.kioskea.net/contents/initiation/types.php3

1.3.3 TOPOLOGÍAS DE RED

En la actualidad existen varias topologías de red, dependiendo de la necesidad de cada cliente, se clasifican de acuerdo a su tamaño y distribución lógica.

Entre las más conocidas están las siguientes:

Redes Anillo.- Como su nombre lo indica esta red tiene la forma de un anillo en la que cada estación está conectada una a continuación de otra, contando cada estación con un receptor y transmisor.

Hay que puntualizar que si algún nodo de la red falla, se pierde la comunicación en toda la red.

Redes Estrella.- Este tipo de red se caracteriza, porque la conexión se hace a través de un distribuidor central que se comunica con las estaciones.

Redes Malla.- Es una red en la que todos los nodos están conectados entre sí, de esta manera si queremos enviar algún mensaje, y en el caso de que algún nodo falle tenemos diferentes caminos para poder llegar al nodo deseado.

1.3.4 CABLEADO ESTRUCTURADO

Cuando se habla de cableado estructurado se refiere a la infraestructura o medio por el cual viajan los paquetes de información generados por equipos como teléfonos, computadores, cámaras de video etc.

A veces se oye hablar sobre los típicos problemas que se pueden suscitar en una empresa como que la red no funciona, o que está lenta, esto se debe en la mayoría de los casos, a que el tiempo de vida útil de la red ya terminó o por una mala instalación del cableado.

Por eso los expertos consideran que la vida útil de un cable común (UTP) es de aproximadamente 5 años.

Cuando se realiza cableado estructurado se debe certificar el trabajo con los diferentes estándares de calidad, seguridad y rendimiento para que de esta manera no invertir recursos en mantenimiento por un trabajo que no se hizo con las debidas normas y estándares.

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

ETIQUETADO

"La norma EIA/TIA-606 especifica que cada terminación de hardware debe tener alguna etiqueta que lo identifique de manera exclusiva.

Se recomienda la utilización de etiquetas que incluyan un identificador de sala y un identificador de conector, así se sabe todo sobre el cable, dónde empieza y dónde acaba". http://www.mailxmail.com/curso-redes-area-local/etiquetado-cables-cableado-estructurado

Por ejemplo el etiquetado esta dado por el piso, área de trabajo y número de estación **P1-RH-3.**

1.3.5 ROUTERS Y SWITCHS

Routers: Son dispositivos que trabajan a nivel de capa 3 (Capa de Red) del modelo OSI, mediante la utilización de direcciones IPs asignadas a cada máquina dentro de un rango pre establecido ya sea estáticamente o dinámicamente.

De esta manera las máquinas pueden acceder al router y comunicarse entre distintos equipos. Cabe señalar que estas direcciones deben ser lógicas.

Switchs: Son dispositivos que trabajan a nivel de capa 2 (Capa Enlace) y en otros casos según la necesidad de la empresa, capa 3 del modelo OSI, a diferencia del router, el switch trabaja a nivel de MAC que es la dirección física de la tarjeta de red.

Esta dirección MAC es única y viene dada en código hexadecimal y es el medio por el cual se realiza la transmisión de datos entre ordenadores, los switchs no trabajan con direcciones IPs si no direcciones MAC.

1.3.6 SEGURIDAD EN REDES

CONTRASEÑAS

> “Una contraseña es una cadena de caracteres que se puede usar para iniciar sesión en un equipo y obtener acceso a archivos, programas y otros recursos. Las contraseñas ayudan a garantizar que no se pueda obtener acceso a un equipo si no se tiene la autorización para hacerlo.

> Para ayudar a mantener protegida la información en el equipo, no debe comunicar su contraseña a nadie, ni anotarla en un lugar donde otros puedan verla". http://windows.microsoft.com/es-MX/windows-vista/What-is-a-password

Dado que las contraseñas se las provee a usuarios se debe tener un sistema de autenticación.

Es por esto que se debe tener una contraseña segura que contenga una combinación de números, letras, caracteres, espacios para que sea difícil descifrarla.

ANTIVIRUS

Es un programa que detecta posibles amenazas como virus, troyanos, gusanos, spyware entre otros, que pueden causar daño al ordenador si este se llegara a infectar, pudiendo perder información valiosa o una baja en el rendimiento del sistema.

¿QUÉ TIPOS DE CONFLICTOS PUEDEN OCURRIR CUANDO SE TIENEN INSTALADOS DOS ANTIVIRUS?

Entre los principales problemas que se pueden tener al instalar 2 antivirus en el computador, es que se va a hacer lenta la PC, además de que uno de los antivirus va a detectar como amenazas a archivos que para el otro no los son.

SEGURIDAD PERIMETRAL

"La seguridad perimetral es uno de los métodos posibles de defensa de una red, basado en el establecimiento de recursos de seguros en el perímetro externo de la red.

Esto nos permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros". www.gabriel-arellano.com.ar/file_download/14

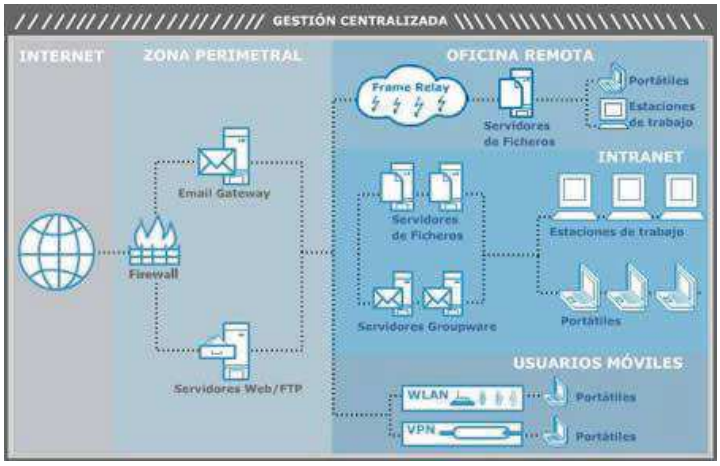


Fig 1.4 Esquema Seguridad Perimetral

http://seguridad-informacion.blogspot.com/2007/12/seguridad-perimetral-gestin-unificada.html

¿QUÉ ES UN FIREWALL?

"Un Firewall es un sistema que bloquea o permite el acceso de conexiones TCP/IP, creando políticas de seguridad para proteger una red confiable de una potencialmente maliciosa.

Puede consistir en distintos dispositivos, tendientes a los siguientes objetivos:

1. Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.

2. Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido".

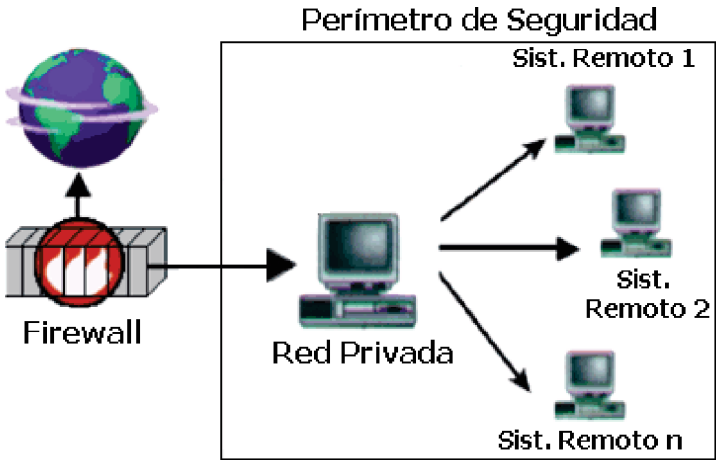


Fig 1.5 Funcionamiento Firewall

http://www.segu-info.com.ar/firewall/firewall.htm

Como puede observarse, el Muro Cortafuegos, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de

seguridad adicionales como la encriptación del tráfico de la red. Se entiende que si dos Firewalls están conectados, ambos deben hablar el mismo método de encriptación-des encriptación para entablar la comunicación". http://www.segu-info.com.ar/firewall/firewall.htm

HARDWARE

"Los componentes y dispositivos del Hardware se dividen en Hardware Básico y Hardware Complementario

Hardware Básico: Son las piezas fundamentales e imprescindibles para que la computadora funcione como son: Placa base, monitor, teclado y ratón.

Hardware Complementario: Son todos aquellos dispositivos adicionales no esenciales como pueden ser: impresora, escáner, cámara de vídeo digital, webcam, etc". http://www.masadelante.com/faqs/software-hardware

SOFTWARE

"El Software es el soporte lógico e inmaterial que permite que la computadora pueda desempeñar tareas inteligentes, dirigiendo a los componentes físicos o hardware con instrucciones y datos a través de diferentes tipos de programas.

El Software son los programas de aplicación y los sistemas operativos, que según las funciones que realizan pueden ser clasificados en:

- Software de Sistema
- Software de Aplicación
- Software de Programación" http://www.masadelante.com/faqs/software-hardware

Software de Sistema: Maneja el hardware del sistema operativo.
Software de Aplicación: Son los aplicativos como lo que es ofimática.
Software de Programación: Son aplicaciones específicas ejemplo programas de contabilidad, diseño etc.

¿QUE ES UN SERVIDOR Y PARA QUE SIRVE?

Un servidor es un tipo de software que provee servicios a diferentes usuarios.

El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos.

Los archivos para cada sitio de Internet se almacenan y se ejecutan en el servidor. Hay muchos servidores en Internet y muchos tipos de servidores, pero comparten la función común de proporcionar el acceso a los archivos y servicios.

En el mercado existen una infinidad de servidores, pero para el caso de la empresa Marketwatch se va a analizar los servidores con los que cuenta la misma como son los de correo y web.

- Servidor de Correo
- Servidor Web

SERVIDOR DE CORREO

El servidor de correo es una herramienta informática que permite enviar y recibir mensajes como también adjuntar archivos, intercambiar correos con los contactos que se tiene en la empresa entre otras aplicaciones.

La principal función de un servidor de correo es la transferencia de archivos para cual usa un programa llamado MTA el cual se encarga de trasferir los datos de un equipo a otro.

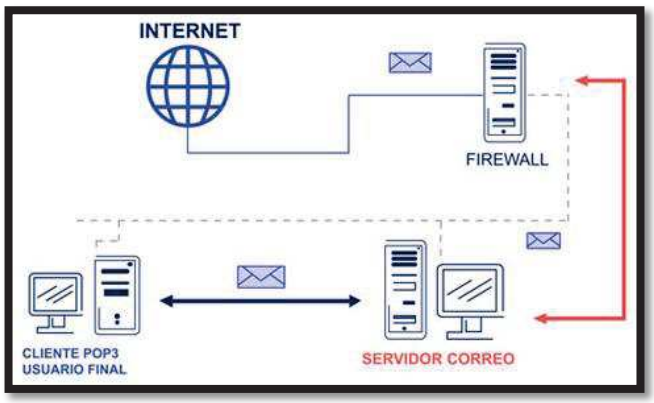


Fig 1.6 Esquema Servidor de Correo

http://culturacion.com/2010/11/%C2%BFque-es-un-servidor-de-correo/

SERVIDOR WEB

> "Un servidor Web se define como un programa que escucha las peticiones de los usuarios o navegantes y las atiende o satisface.
>
> Por medio de la especificación de la búsqueda, el servidor Web buscará una página específica o ejecutará un programa, pero, necesariamente, enviará algún resultado sobre la búsqueda recibida.
>
> Los sistemas operativos más utilizados por los servidores son Windows y Linux, siendo este último más estable y por lo tanto de uso más frecuente". http://www.editum.org/Que-Es-Un-Servidor-Web-p-401.html

Entre los diferentes servidores web se puede mencionar muchos pero uno de los más usados en la actualidad es Apache.

CAPÍTULO II: ELABORACIÓN DEL LEVANTAMIENTO DE LA INFORMACIÓN DE LA RED

2.1 ESTADO DE LA INFORMACIÓN

2.1.1 ELABORACIÓN DEL DISEÑO DE LA INFRAESTRUCTURA DE RED

Fig 2.1: Diagrama de red

Figura realizada por Carlos Vergara

2.2 TIPOS DE SERVIDORES

La empresa cuenta con un servidor interno HP Proliant ML110G6 con sistema operativo Windows Server 2008, para la administración interna de dominios, contraseñas mediante directorio activo.

Además cuenta con dos servidores externos como son los de correo y web que administra ATI - Activa Tecnología Informática, el cual es un proveedor local.

2.3 INFRAESTRUCTURA

En cuanto a lo que a infraestructura se refiere, la empresa cuenta con un rack empotrado en la pared de (26x50)cm en el cual se encuentran los siguientes equipos:

- 2 Switchs Dlink – Des 1024 (24 puertos).
- 1 Patch Panel
- 1 Router Dlink – Dir 300 802.11b/g (Para la conexión vía wireless).
- 1 Switch Siemon (ISP).
- 1 router cisco 1700.

Los equipos se encuentran ubicados en 5 bandejas distintas para una mejor distribución y fácil mantenimiento.

SWITCH DLINK DES-1024A
24-PORT FAST ETHERNET SWITCH

Fig 2.2 Switch Dlink

http://www.dlinkla.com/home/productos/producto.jsp?idp=1416

DESCRIPCIÓN DEL EQUIPO

El DES-1024A es un Switch No Administrable de 24 puertos Fast Ethernet10/100BASE-TX. No requiere de configuración y su instalación es fácil y rápida. Soporta MDI/MDI-X en todos sus puertos. Diseño libre de ventilador que proporciona un funcionamiento sin ruido.

24 PUERTOS FAST ETHERNET AUTO SENSING

Este switch provee de 24 puertas con soporte Nway. Las puertas tienen la capacidad de negociar las velocidades de red entre 10BASE-T y 100BASE-TX, como también el modo de operación en Half o Full Dúplex

ROUTER DLINK DIR-300

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.
Firewall avanzado & Seguridad.
Soporta VPN Passthrough.
Soporta encriptación WPA (TKIP) y WPA2 (AES).
Asistente de configuración amigable Quick Router Setup.
Smart QoS (Calidad de Servicio Inteligente).

Fig 2.3 Router Dlink

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

ROUTER CISCO 1700

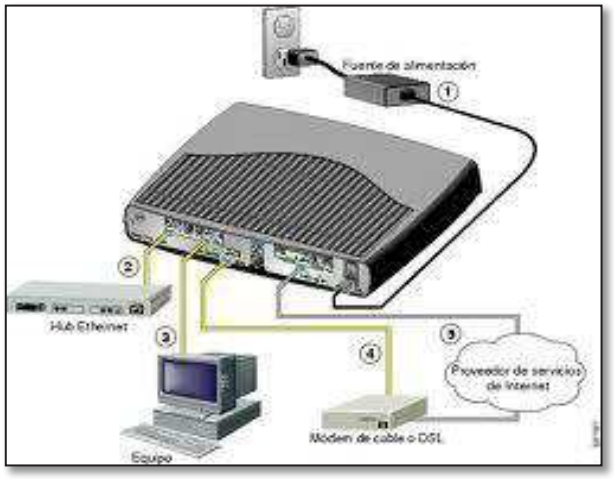


Fig 2.4 Router Cisco

http://www.cisco.com/en/US/docs/routers/access/1700/1711/hardware/quick/guide/171Xq_sp.html

CARACTERÍSTICAS PRINCIPALES

"Los routers Cisco de la serie 1700 proporcionan un rápido, fiable y seguro acceso a Internet y a redes remotas a través de diferentes tecnologías de acceso WAN de alta velocidad.

La serie 1700 ofrece una extensa familia de características de seguridad integradas como protección por firewall túneles VPN". http://www.abox.com/productos.asp?pid=557

COMPONENTES QUE NECESITA PROPORCIONAR

"Según el entorno de red de que disponga, necesitará proporcionar algunos de los siguientes componentes para instalar el router:

Cables Ethernet rectos (RJ-45 a RJ-45) para conectar el router a un módem de banda ancha (xDSL o cable) y a un hub o switch.

Cables rectos o cruzados para conectar tarjetas WIC a los servicios WAN adecuados (los puertos switch integrados operan en modo de detección automática).

Switch o hub Ethernet para conectar el router a la red local o un módem de cable o xDSL para conectar el router al proveedor de servicios.

Servidor u otro equipo con una tarjeta de interfaz de red (NIC) u otro dispositivo en red (como un hub o un switch) para conectarlo al switch Ethernet 10/100 Mbps de 4 puertos integrado". http://www.cisco.com/en/US/docs/routers/access/1700/1711/hardware/quick/guide/171Xq_sp.html

CONECTIVIDAD HACIA EL SERVIDOR

Actualmente están conectadas 10 máquinas al servidor interno HP Proliant ML110 G6 de la empresa, el cual es administrado por el departamento de sistemas y el jefe del departamento es la única persona que tiene acceso a las contraseñas tanto del servidor como de la red inalámbrica.

CABLEADO HORIZONTAL Y VERTICAL

En lo que se refiere al backbone que sube por el edificio, este llega a través de fibra óptica al armario de telecomunicaciones de cada piso.

Fig 2.5 Conexión Fibra Backbone

Después la conexión a cada oficina es mediante HCC (Horizontal Cross Conection) cableado horizontal unifilar UTP Siemon categoría 6.

Dentro de la cableado interno de la oficina se tiene estructurada una topología tipo estrella con cable UTP Panduit categoría 5e, el mismo que es certificado punto por punto.

2.4 EQUIPOS TERMINALES

La empresa cuenta con 19 equipos terminales de los cuales el 90 % cuentan con Windows 7 y el restante 10 % está instalado Windows Xp ya que son máquinas en las que el trabajo no es tan fuerte en cuanto a procesamiento de información por lo que se optó por dejarlas con este sistema operativo.

Todas las máquinas cuentan con el antivirus AVG Internet Security 2012.

Además hay que acotar que, cada uno de los equipos terminales, están configurados por medio del directorio activo para que cada 15 días estén obligados a cambiar la contraseña de cada máquina en la empresa.

CAPÍTULO III: AUDITORÍA

Para las distintas evaluaciones que se van a realizar, se utilizará software o páginas web especializadas en pruebas de auditoría de sistemas para cada apliación tanto en lo que es software y hardware.

Para lo que es software, en los equipos con sistema operativo windows se realizarán las siguientes pruebas:

- Evaluación Antivirus
- Evaluación Contraseñas
- Evaluación Servidor DNS
- Evaluación Listas negras
- Evaluzacuón Open Relay
- Evaluación Página web

Para la parte de hardware se utilizará las mismas herramientas que windows provee como es el administrador de tareas para realizar las siguientes pruebas:

- Rendimiento del sistema
- Rendimiento memoria RAM

EVALUACIÓN SOFTWARE

3.1 EVALUACIÓN DEL ANTIVIRUS

La empresa no cuenta con antivirus licenciado, por lo que se optó por instalar el antivirus AVG Internet Security Business Edition 2012 el cual es crackeado y se encuentra instalado en todas las estaciones de trabajo que tiene la empresa.

Para evaluar la efectividad del antivirus instalado en la empresa se va a proceder a realizar las pruebas con EICAR.

EICAR (EICAR Standard Anti-Virus Test File)

EICAR es una prueba que contiene varios archivos mediante los cuales permite probar que tan efectivo es el antivirus que está instado en los equipos de la empresa, además que una de las ventajas de realizar pruebas con EICAR es que no conlleva ningún riesgo para las máquinas.

Para efecto de evaluación se procede a realizar pruebas ingresando a la página web http://www.vsantivirus.com/eicar-test.htm en la cual mediante el archivo de EICAR se realiza algunas pruebas con el fin de comprobar si el antivirus es efectivo o no.

A continuación se muestra los pasos a seguir para realizar una de las pruebas.

- Para la primera prueba con extensión .COM mediante el enlace http://www.eicar.org/download/eicar.com

1. Se empieza en el escritorio.
2. Se crea un nuevo documento de texto.
3. Se coloca el siguiente código.
   "***X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*"***http://www.vsantivirus.com/eicar-test.htm
4. Se guarda el archivo con cualquier nombre y colocando al final la extensión .com.
5. Al momento de guardar, el antivirus arroja el siguiente mensaje.

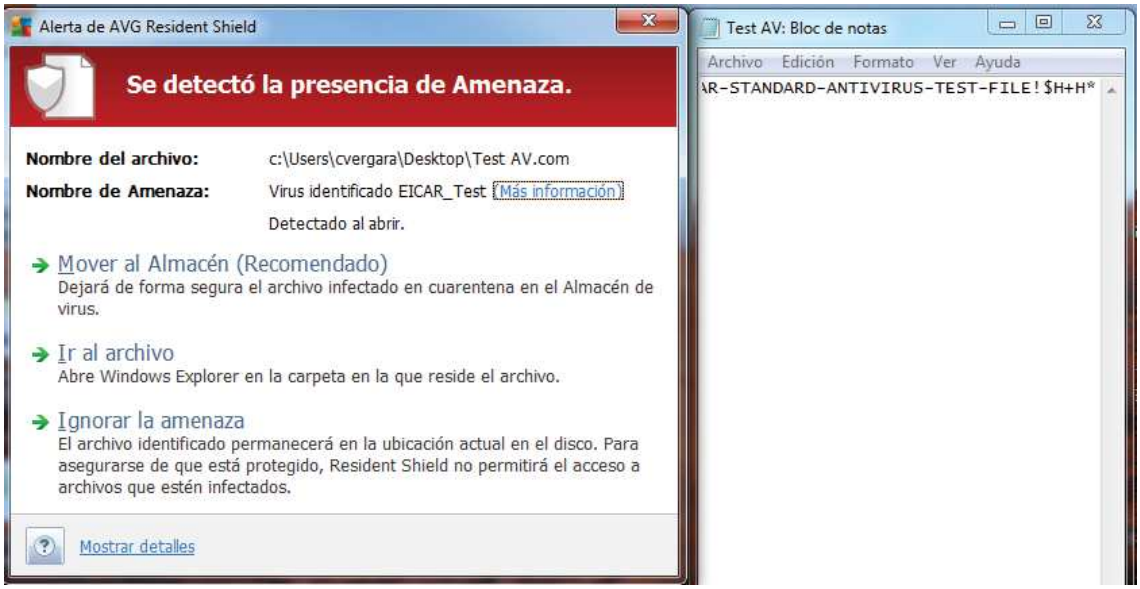


Fig 3.1 Prueba Eicar

En el caso de que el antivirus que está instalado en cualquiera de las máquinas no detectara ninguna amenaza, significa que dicho antivirus no es confiable y hay que cambiar inmediatamente a otro.

- Otra prueba que se realiza es para verificar un código como un archivo .TXT mediante el enlace http://www.eicar.org/download/eicar.com.txt

Fig 3.2 Prueba Eicar Archivos txt

Como se ve el antivirus si lo detectó.

- Otra prueba con extensión .ZIP mediante el enlace http://www.eicar.org/download/eicar_com.zip

Fig 3.3 Prueba Eicar Archivos Zip

Como se observa al tratar de ejecutar el link de EICAR para archivos comprimidos, igual detectó el antivirus la amenaza para este tipo de extensiones.

- La última prueba se realizará al tratar de enviar un correo electrónico con un el archivo adjunto de EICAR.

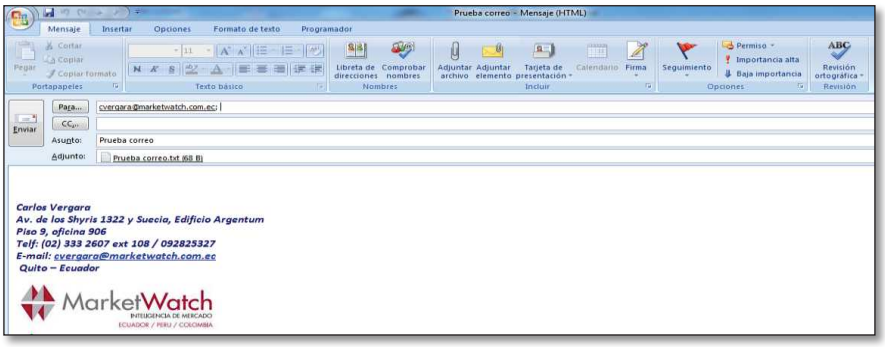


Fig. 3.4Prueba Eicar Correo Electrónico

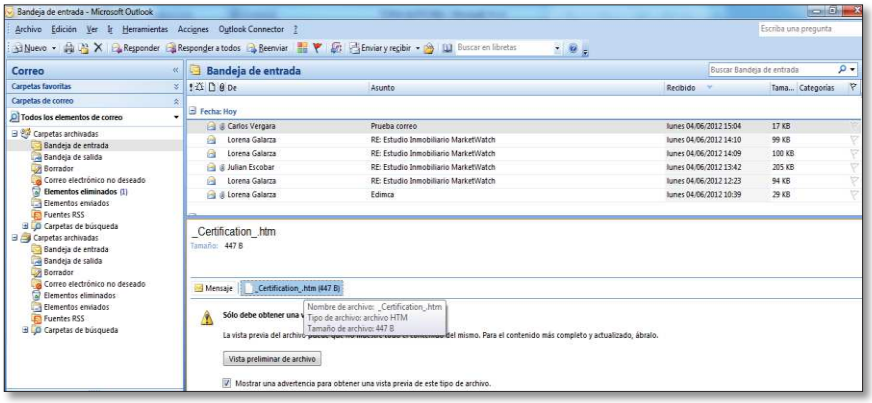


Fig 3.5 Apertura archivo adjunto

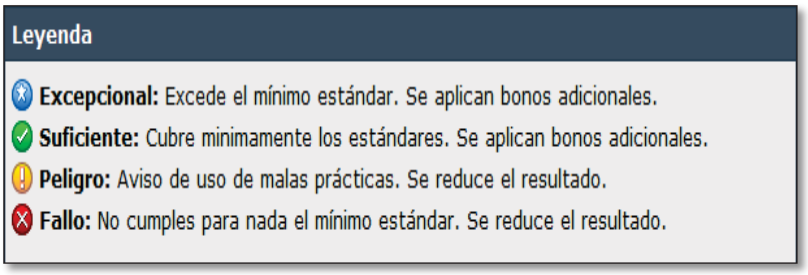
Al tratar de abrir el archivo adjunto el antivirus muestra el siguiente mensaje

Fig 3.6 Resultado Prueba Correo

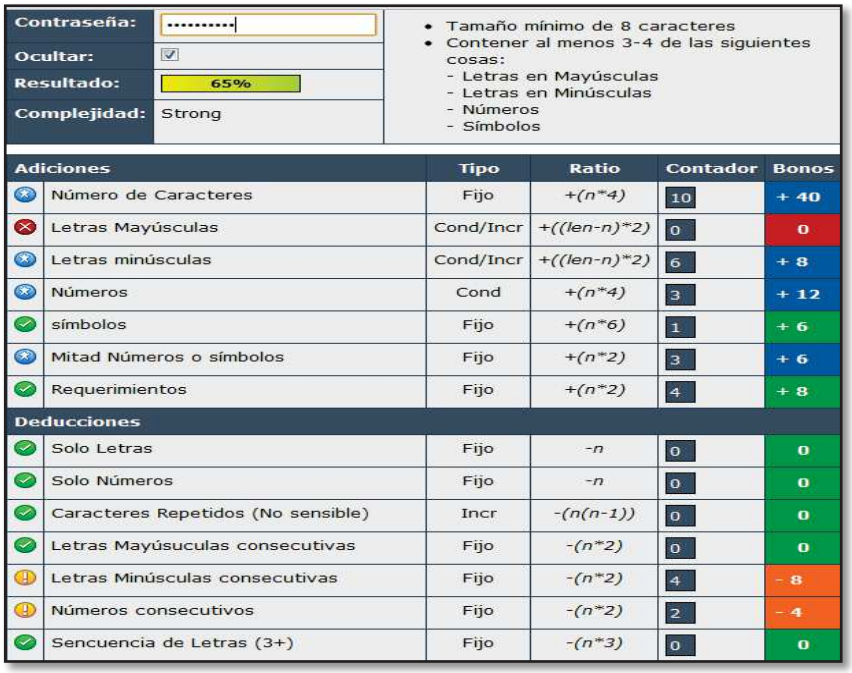
3.2 EVALUACIÓN DE CONTRASEÑAS

Para el proceso de evaluación de contraseñas se utilizará un software en línea, que ingresando a la página web http://password.es/comprobador/, se procederá a realizar las pruebas para ver que tan seguras o no, son las contraseñas en cuanto a su robustez en las estaciones del área de operaciones y del servidor.

A continuación se encuentra la leyenda para saber cuáles son los parámetros que nos arrojen las pruebas realizadas en las diferentes estaciones de trabajo.



Estación 1



Contraseña:	••••••••••|
Ocultar:	☑
Resultado:	65%
Complejidad:	Strong

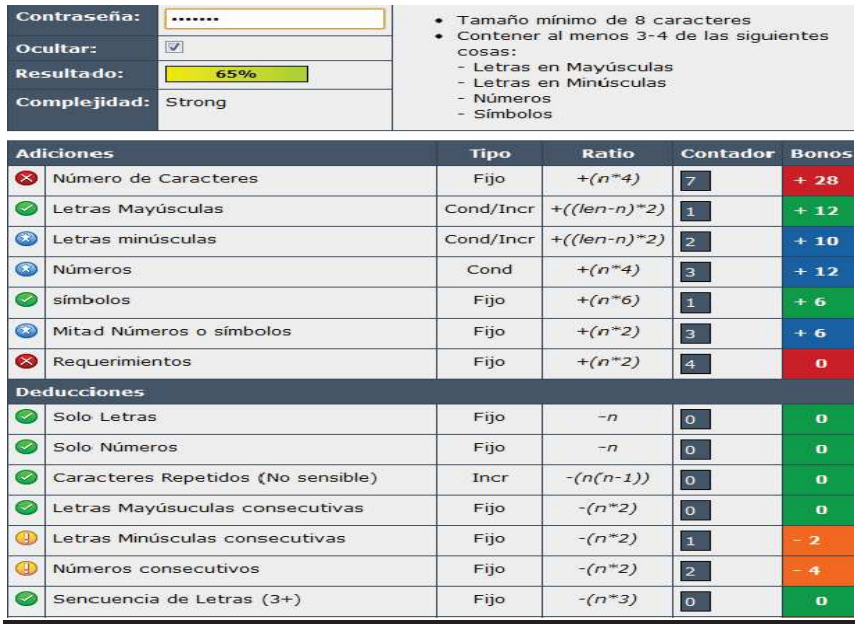
- Tamaño mínimo de 8 caracteres
- Contener al menos 3-4 de las siguientes cosas:
  - Letras en Mayúsculas
  - Letras en Minúsculas
  - Números
  - Símbolos

Adiciones	Tipo	Ratio	Contador	Bonos
Número de Caracteres	Fijo	+(n*4)	10	+ 40
Letras Mayúsculas	Cond/Incr	+((len-n)*2)	0	0
Letras minúsculas	Cond/Incr	+((len-n)*2)	6	+ 8
Números	Cond	+(n*4)	3	+ 12
símbolos	Fijo	+(n*6)	1	+ 6
Mitad Números o símbolos	Fijo	+(n*2)	3	+ 6
Requerimientos	Fijo	+(n*2)	4	+ 8
Deducciones				
Solo Letras	Fijo	-n	0	0
Solo Números	Fijo	-n	0	0
Caracteres Repetidos (No sensible)	Incr	-(n(n-1))	0	0
Letras Mayúsculas consecutivas	Fijo	-(n*2)	0	0
Letras Minúsculas consecutivas	Fijo	-(n*2)	4	- 8
Números consecutivos	Fijo	-(n*2)	2	- 4
Sencuencia de Letras (3+)	Fijo	-(n*3)	0	0

Fig 3.7 Prueba de Evaluación de Contraseña Estación 1

En esta estación se puede ver que la contraseña que se aplicó a esta máquina es una contraseña fuerte, en donde la mayoría de los componentes se encuentran dentro de los parámetros de seguridad.

Estación 2



Contraseña:	•••••••
Ocultar:	☑
Resultado:	65%
Complejidad:	Strong

- Tamaño mínimo de 8 caracteres
- Contener al menos 3-4 de las siguientes cosas:
  - Letras en Mayúsculas
  - Letras en Minúsculas
  - Números
  - Símbolos

Adiciones		Tipo	Ratio	Contador	Bonos
✗	Número de Caracteres	Fijo	+(n*4)	7	+ 28
✓	Letras Mayúsculas	Cond/Incr	+((len-n)*2)	1	+ 12
✓	Letras minúsculas	Cond/Incr	+((len-n)*2)	2	+ 10
✓	Números	Cond	+(n*4)	3	+ 12
✓	símbolos	Fijo	+(n*6)	1	+ 6
✓	Mitad Números o símbolos	Fijo	+(n*2)	3	+ 6
✗	Requerimientos	Fijo	+(n*2)	4	0
Deducciones					
✓	Solo Letras	Fijo	-n	0	0
✓	Solo Números	Fijo	-n	0	0
✓	Caracteres Repetidos (No sensible)	Incr	-(n(n-1))	0	0
✓	Letras Mayúsuculas consecutivas	Fijo	-(n*2)	0	0
!	Letras Minúsculas consecutivas	Fijo	-(n*2)	1	- 2
!	Números consecutivos	Fijo	-(n*2)	2	- 4
✓	Sencuencia de Letras (3+)	Fijo	-(n*3)	0	0

Fig 3.8 Prueba de Evaluación de Contraseña Estación 2

A diferencia de la estación anterior, en esta se tiene una contraseña que se la puede considerar como fuerte pero se la puede reforzar al menos en el número de caracteres.

Estación 3

Contraseña:	•••••••
Ocultar:	☑
Resultado:	72%
Complejidad:	Strong

- Tamaño mínimo de 8 caracteres
- Contener al menos 3-4 de las siguientes cosas:
  - Letras en Mayúsculas
  - Letras en Minúsculas
  - Números
  - Símbolos

Adiciones	Tipo	Ratio	Contador	Bonos
Número de Caracteres	Fijo	*+(n*4)*	8	+ 32
Letras Mayúsculas	Cond/Incr	*+((len-n)*2)*	1	+ 14
Letras minúsculas	Cond/Incr	*+((len-n)*2)*	3	+ 10
Números	Cond	*+(n*4)*	4	+ 16
símbolos	Fijo	*+(n*6)*	0	0
Mitad Números o símbolos	Fijo	*+(n*2)*	3	+ 6
Requerimientos	Fijo	*+(n*2)*	4	+ 8
Deducciones				
Solo Letras	Fijo	*-n*	0	0
Solo Números	Fijo	*-n*	0	0
Caracteres Repetidos (No sensible)	Incr	*-(n(n-1))*	2	- 2
Letras Mayúsuculas consecutivas	Fijo	*-(n*2)*	0	0
Letras Minúsculas consecutivas	Fijo	*-(n*2)*	2	- 4
Números consecutivos	Fijo	*-(n*2)*	3	- 6
Sencuencia de Letras (3+)	Fijo	*-(n*3)*	0	0

Fig 3.9 Prueba de Evaluación de Contraseña Estación 3

Esta contraseña a diferencia de las anteriores, tiene un porcentaje más alto de seguridad, pero igual se le debe aumentar algunos parámetros para que sea más segura.

Servidor

Contraseña:	•••••••••••
Ocultar:	☑
Resultado:	100%
Complejidad:	Very Strong

- Tamaño mínimo de 8 caracteres
- Contener al menos 3-4 de las siguientes cosas:
  - Letras en Mayúsculas
  - Letras en Minúsculas
  - Números
  - Símbolos

Adiciones		Tipo	Ratio	Contador	Bonos
✓	Número de Caracteres	Fijo	+(n*4)	12	+ 48
✓	Letras Mayúsculas	Cond/Incr	+((len-n)*2)	1	+ 22
✓	Letras minúsculas	Cond/Incr	+((len-n)*2)	3	+ 18
✓	Números	Cond	+(n*4)	5	+ 20
✓	símbolos	Fijo	+(n*6)	3	+ 18
✓	Mitad Números o símbolos	Fijo	+(n*2)	7	+ 14
✓	Requerimientos	Fijo	+(n*2)	5	+ 10
Deducciones					
✓	Solo Letras	Fijo	-n	0	0
✓	Solo Números	Fijo	-n	0	0
!	Caracteres Repetidos (No sensible)	Incr	-(n(n-1))	6	- 6
✓	Letras Mayúsculas consecutivas	Fijo	-(n*2)	0	0
!	Letras Minúsculas consecutivas	Fijo	-(n*2)	1	- 2
!	Números consecutivos	Fijo	-(n*2)	3	- 6
✓	Sencuencia de Letras (3+)	Fijo	-(n*3)	0	0

Fig 3.10 Prueba de Evaluación de Contraseña Servidor

Como se aprecia en la prueba realizada a la contraseña del servidor de la empresa, se puede ver que la misma es bastante segura y cumple con los requerimientos que debe tener la contraseña de un servidor.

3.3 EVALUACIÓN DE SERVIDOR DNS

> “Los servidores DNS no son más que computadoras que en sus discos duros almacenan enormes bases de datos en las que tienen registrada la relación que existe entre cada nombre de dominio y su dirección IP correspondiente.
>
> Los seres humanos identificamos los sitios de internet mediante nombres, como son Google.com, Yahoo.es, Apple.com, etc. lo que los hace más fácil de recordar y de escribir, estos nombres es lo que conocemos como nombres de dominio”. http://norfipc.com/internet/servidores-dns.html

Antes de empezar con esta evaluación, cabe señalar que el servidor DNS de la empresa esta hosteado, y se realizará las pruebas correspondientes para verificar su rendimiento y comparar los tiempos de respuesta con otros servidores.

Para la evaluación del servidor DNS, se utilizará el software llamado **Domain Name Server Benchmark** el cual realiza análisis comparativos, estadísticos, además de chequear el tiempo de respuesta del servidor DNS cuando existe una petición.

A continuación se detalla las diferentes pruebas de eficiencia del servidor DNS de la empresa.

Lo primero que se debe hacer para realizar las diferentes pruebas, es instalar el programa DNS Benchmark y hacer clic sobre el ícono Run Benchmark

Pestaña Name

Proporciona los nombres de los servidores que encontró.

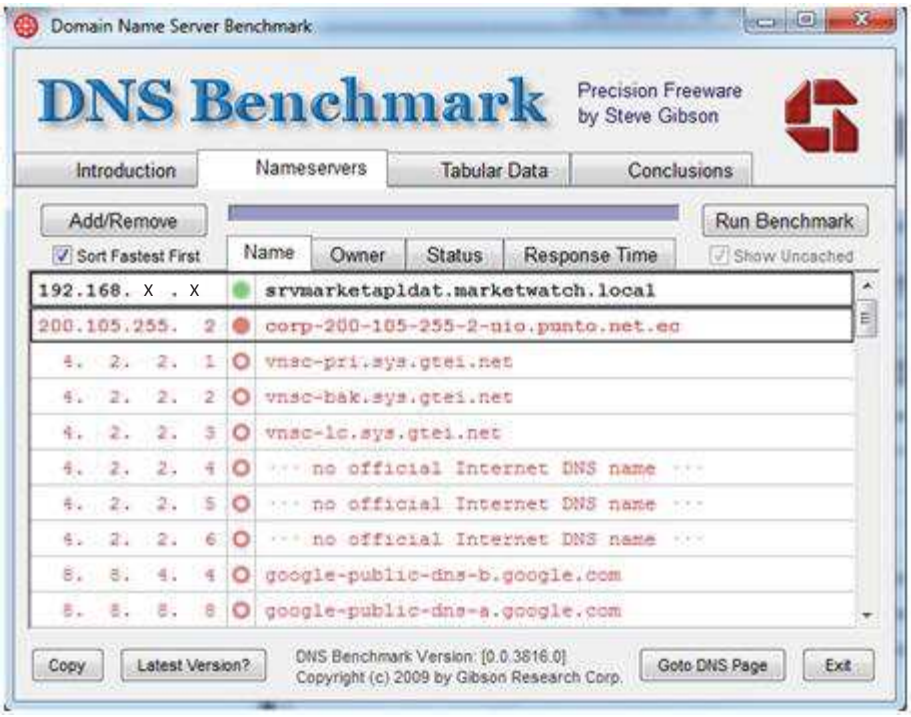


Fig 3.11 Nombre y Direcciones Servidores

Realizado esto se despliega una lista de servidores, la cual puede llegar hasta 200 nombres de servidores DNS tanto públicos como privados.

Pestaña Owner

En cambio al hacer clic sobre la pestaña Owner se puede ver la información del propietario del servidor, en este caso la empresa propietaria es Puntonet, como muestra la figura 3.12.

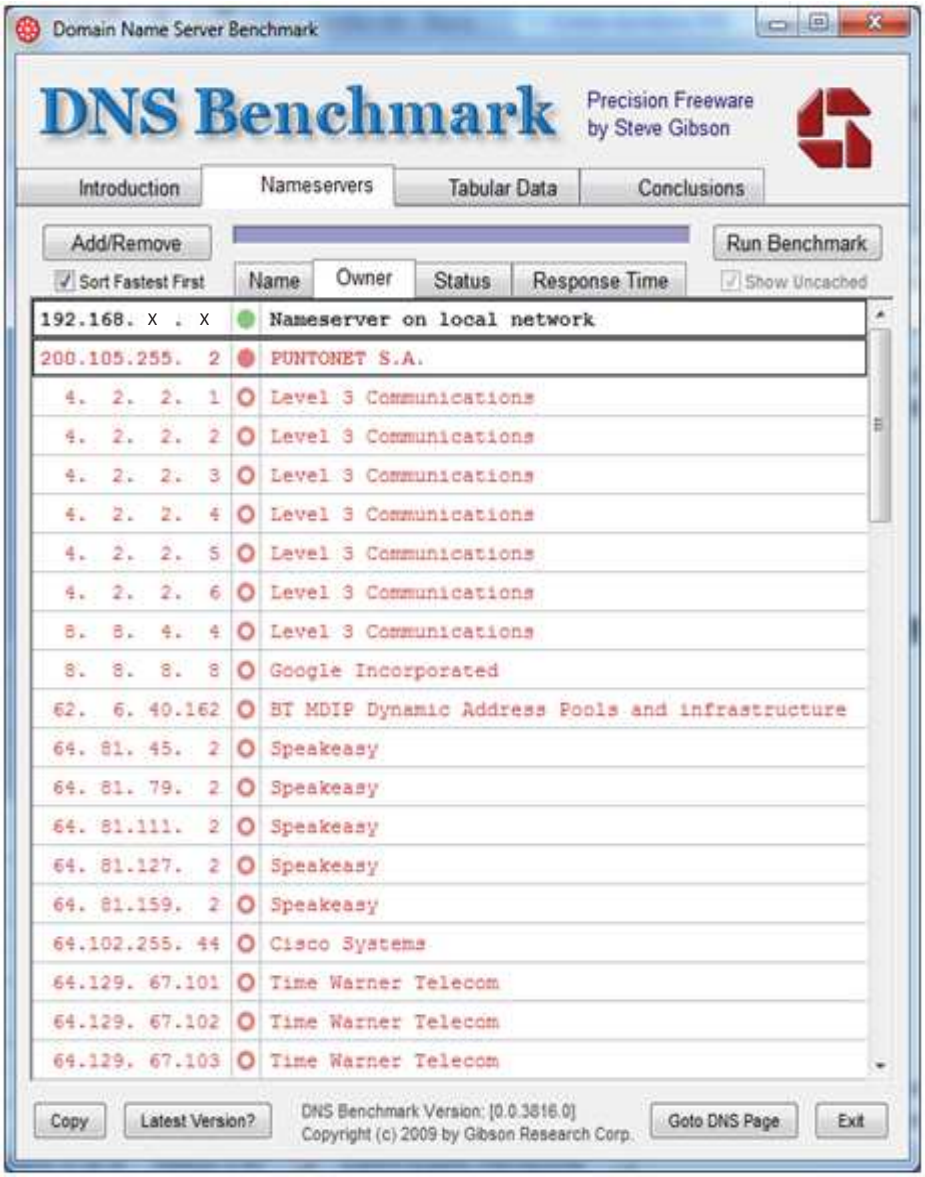


Fig 3.12 Nombre Servidor Propietario

Pestaña Status

La pestaña Status nos indica que el servidor de la empresa se encuentra activo y que está trabajando sin aparentes problemas, además permite identificar cualquier consulta que realiza el servidor DNS y reporta cuando alguna de ellas no es respondida, como muestra la figura 3.13.

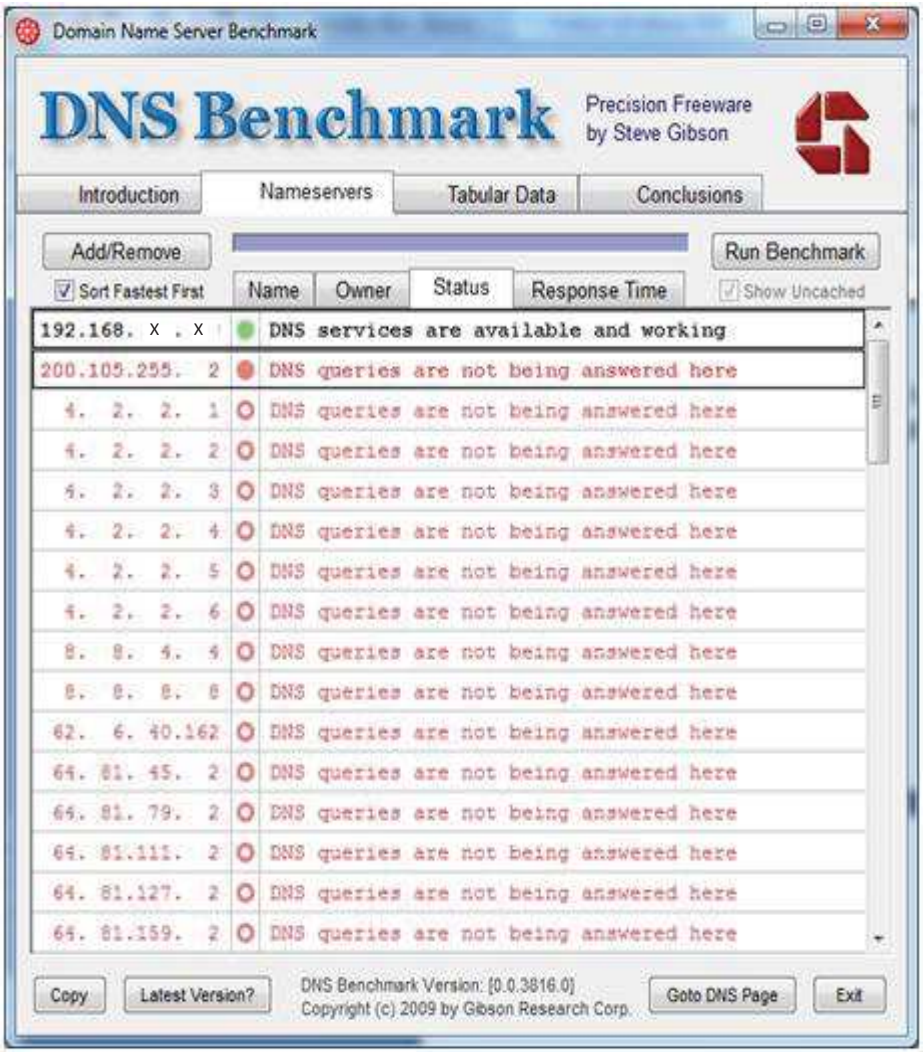


Fig 3.13 Actividad Servidor Empresa

Pestaña Response Time

La pestaña Response Time proporciona una representación gráfica del tiempo de respuesta fig. 3.14.

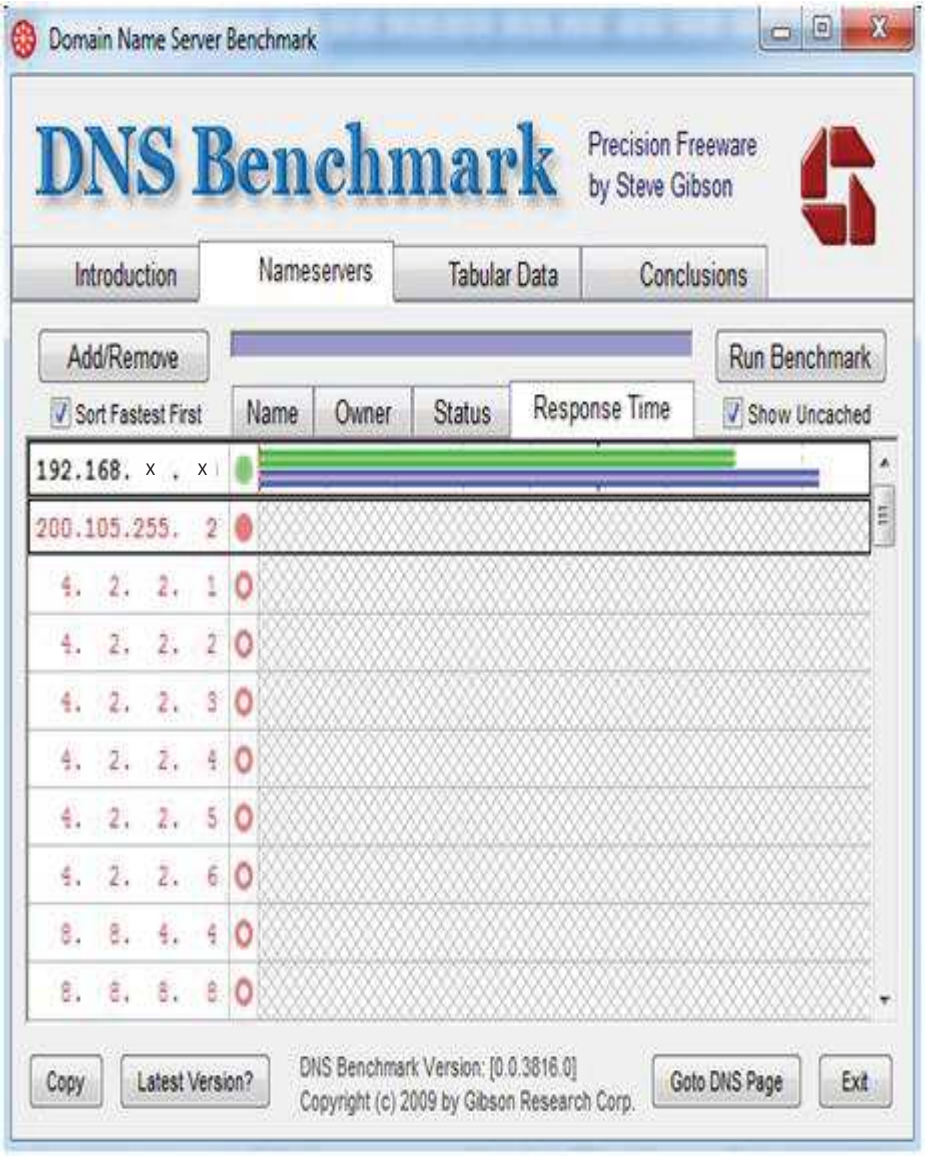


Fig 3.14 Tiempo Respuesta Servidor

3.4 EVALUACIÓN DE LISTAS NEGRAS

> "Las listas negras generan una base de datos de servidores de correo que están mal configurados (open-relay) y han sido o serán fuentes de spam, dependiendo de la política de cada una de ellas. Para entendernos: las máquinas dadas de alta en esta base de datos son etiquetadas como poco fiables y siempre serán fuente de algún tipo de problema". http://www.rediris.es/mail/abuso/ln.es.html

Para realizar la evaluación de listas negras de la empresa se ha utilizado la siguiente página web http://www.mxtoolbox.com/.

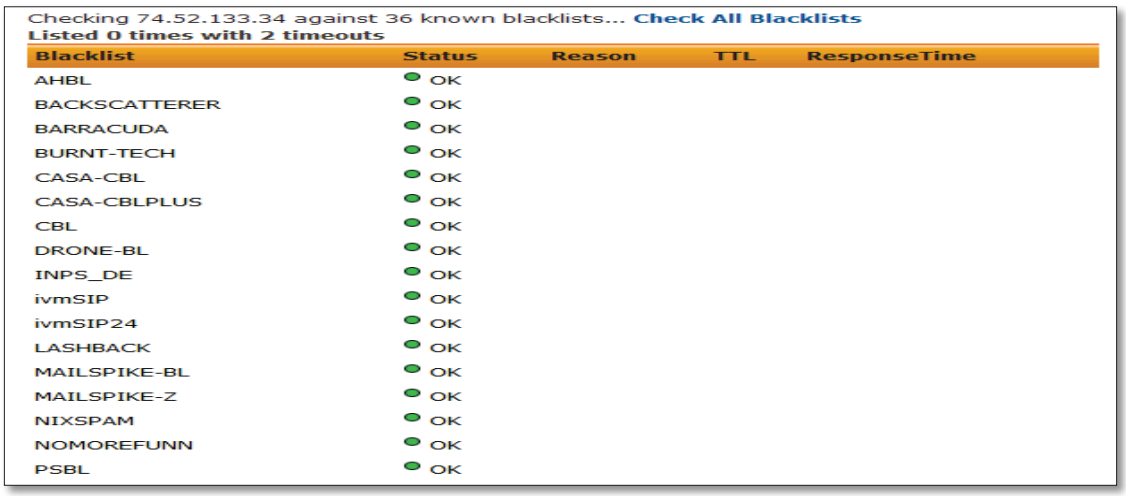
Lo que se debe hacer primero, es ingresar la dirección IP o el dominio de la empresa fig. 3.15.

Fig 3.15 Página Principal mxtoolbox.com

Como se puede observar en el menú principal de la página mxtoolbox.com, además de evaluar listas negras, también se pueden evaluar otros servicios,

pero por el momento solo se va a chequear si es que el dominio de la empresa se encuentra en algún servidor de listas negras.

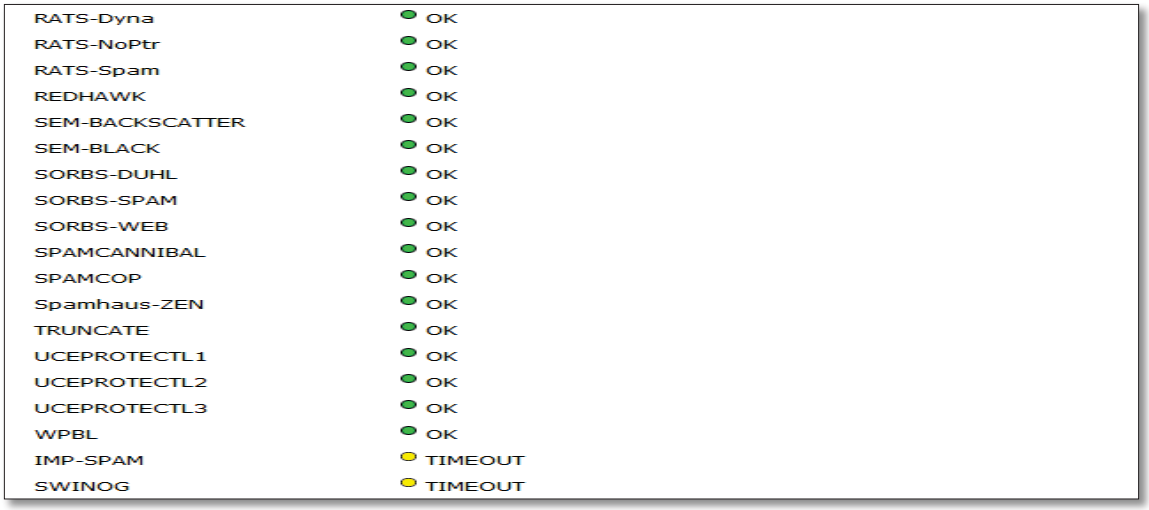
A continuación se hace clic sobre **Blacklist Check** y se despliega la lista de servidores de listas negras como se ve a continuación.



Checking 74.52.133.34 against 36 known blacklists... Check All Blacklists
Listed 0 times with 2 timeouts

Blacklist	Status	Reason	TTL	ResponseTime
AHBL	OK			
BACKSCATTERER	OK			
BARRACUDA	OK			
BURNT-TECH	OK			
CASA-CBL	OK			
CASA-CBLPLUS	OK			
CBL	OK			
DRONE-BL	OK			
INPS_DE	OK			
ivmSIP	OK			
ivmSIP24	OK			
LASHBACK	OK			
MAILSPIKE-BL	OK			
MAILSPIKE-Z	OK			
NIXSPAM	OK			
NOMOREFUNN	OK			
PSBL	OK			

Fig 3.16 Servidores Listas Negras



RATS-Dyna	OK
RATS-NoPtr	OK
RATS-Spam	OK
REDHAWK	OK
SEM-BACKSCATTER	OK
SEM-BLACK	OK
SORBS-DUHL	OK
SORBS-SPAM	OK
SORBS-WEB	OK
SPAMCANNIBAL	OK
SPAMCOP	OK
Spamhaus-ZEN	OK
TRUNCATE	OK
UCEPROTECTL1	OK
UCEPROTECTL2	OK
UCEPROTECTL3	OK
WPBL	OK
IMP-SPAM	TIMEOUT
SWINOG	TIMEOUT

Fig 3.17 Servidores Listas Negras

Como se puede observar, en la gran mayoría de servidores salen OK, pero en el caso que saliera la palabra Listed indica que la IP se encuentra en lista negra y dependiendo de la lista, hay que realizar varios pasos para sacar la IP de la lista, previamente se debe encontrar la causa y arreglar el problema.

3.5 EVALUACIÓN DE OPEN RELAY

Open Relay es un término que se utiliza para describir cuando un servidor de correo procesa un mensaje de correo, donde ni el remitente ni el destinatario es un usuario local, este método es utilizado como puente ya sea por hackers o spammers para el envío de correo basura o malware en forma indiscriminada.

Para realizar la evaluación al servidor de correo para ver si es vulnerable open relay, primero se debe buscar cual es la dirección IP del servidor de correo, para lo cual se ingresa el ejecutar el comando cmd.

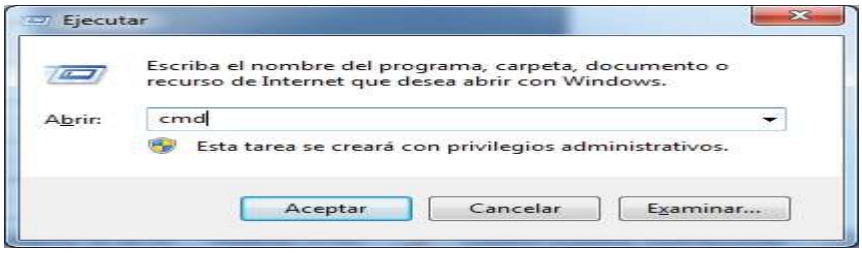


Fig 3.18 Comando Ejecutar

A continuación se debe ingresar el comando **nslookup,** el cual permite obtener información relacionada con el dominio que se quiere acceder.

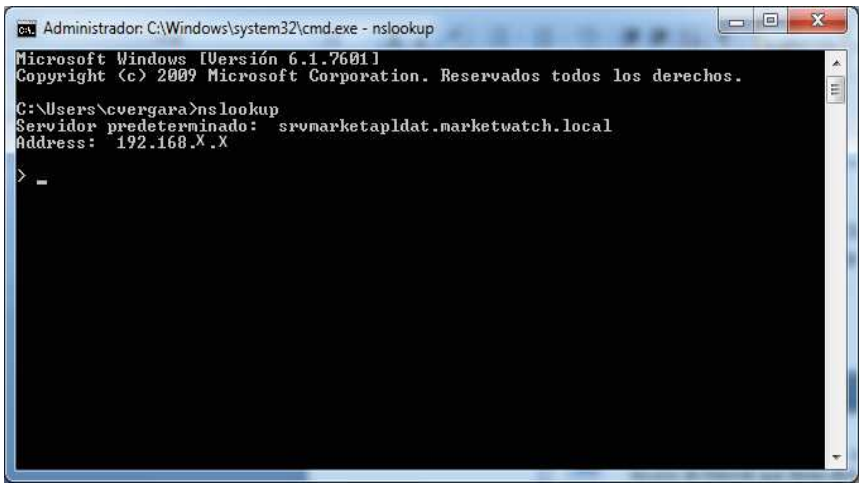


Fig 3.19 Comando nslookup

Se ingresa el comando **set type = mx** y a continuación el dominio para que se muestre la dirección IP del servidor de correo para proceder a realizar las pruebas de evaluación.

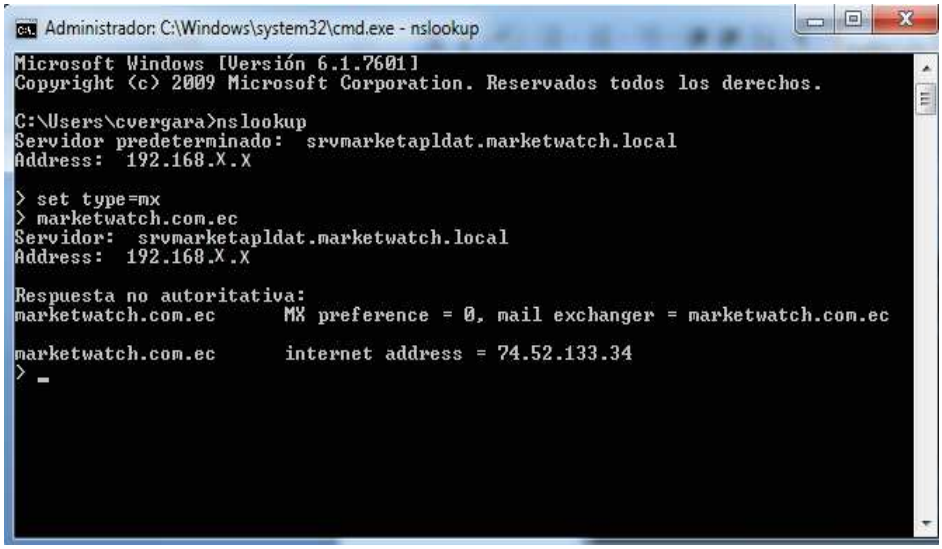


Fig 3.20 Comando set type = mx

Para la evaluación de open relay se utilizó la página web http://www.mailradar.com/openrelay/ en la cual se coloca la dirección que muestra el servidor mx en la figura 3.20.

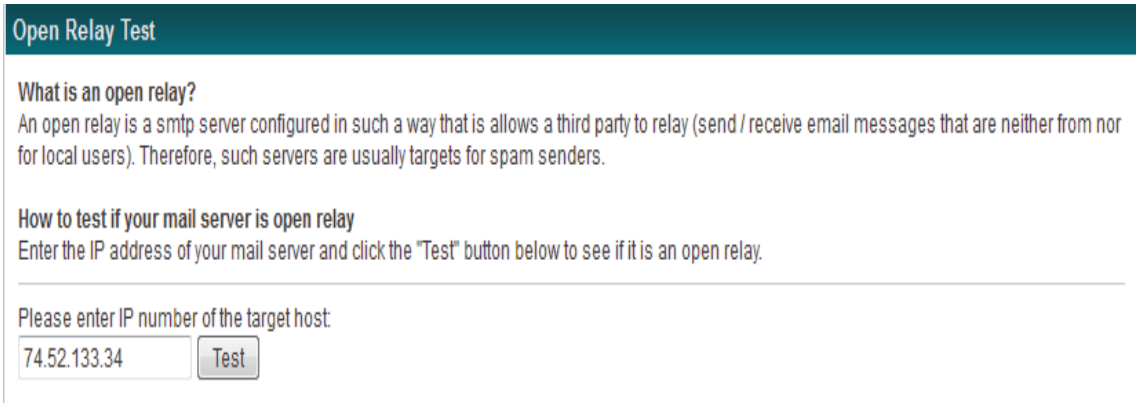


Fig 3.21 Dirección IP dominio Empresa

Y se hace clic en test y empieza a hacer las pruebas al servidor de correo.

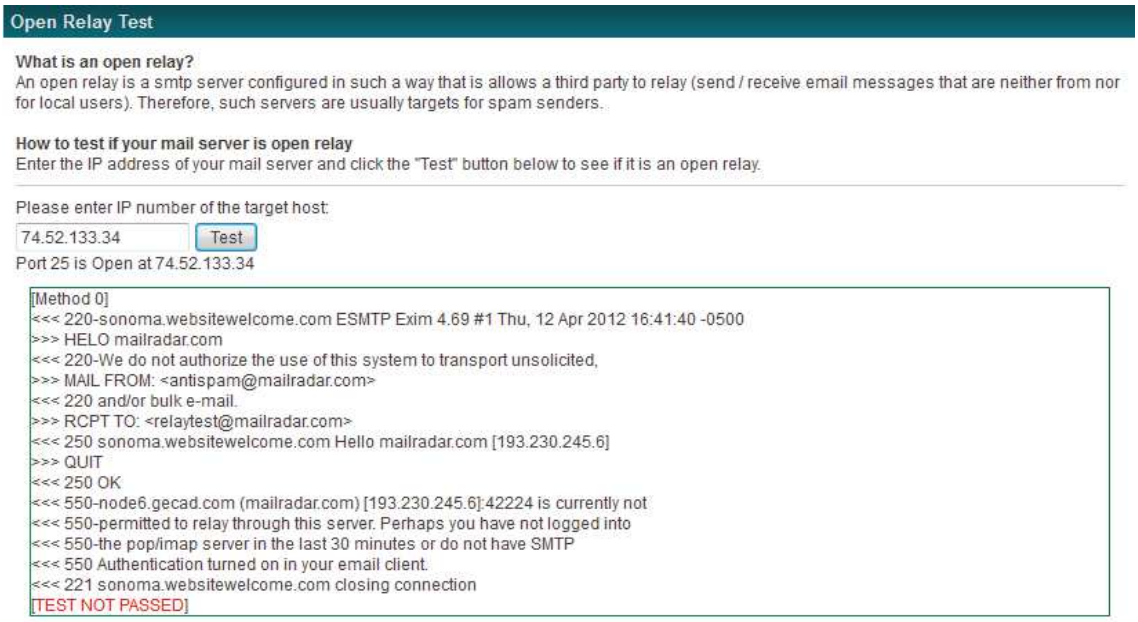


Fig 3.22 Prueba Open Relay

Aquí lo que está haciendo es enviando comandos para realizar las pruebas, los comandos que se pueden visualizar entre otros están HELO, MAIL FROM, RCPT TO; QUIT.

HELO: Inicia comunicación.

MAIL FROM: Quién envía.

RCPT TO: Destinatario.

QUIT: Fin sesión.

El programa sigue haciendo pruebas en distintos métodos.

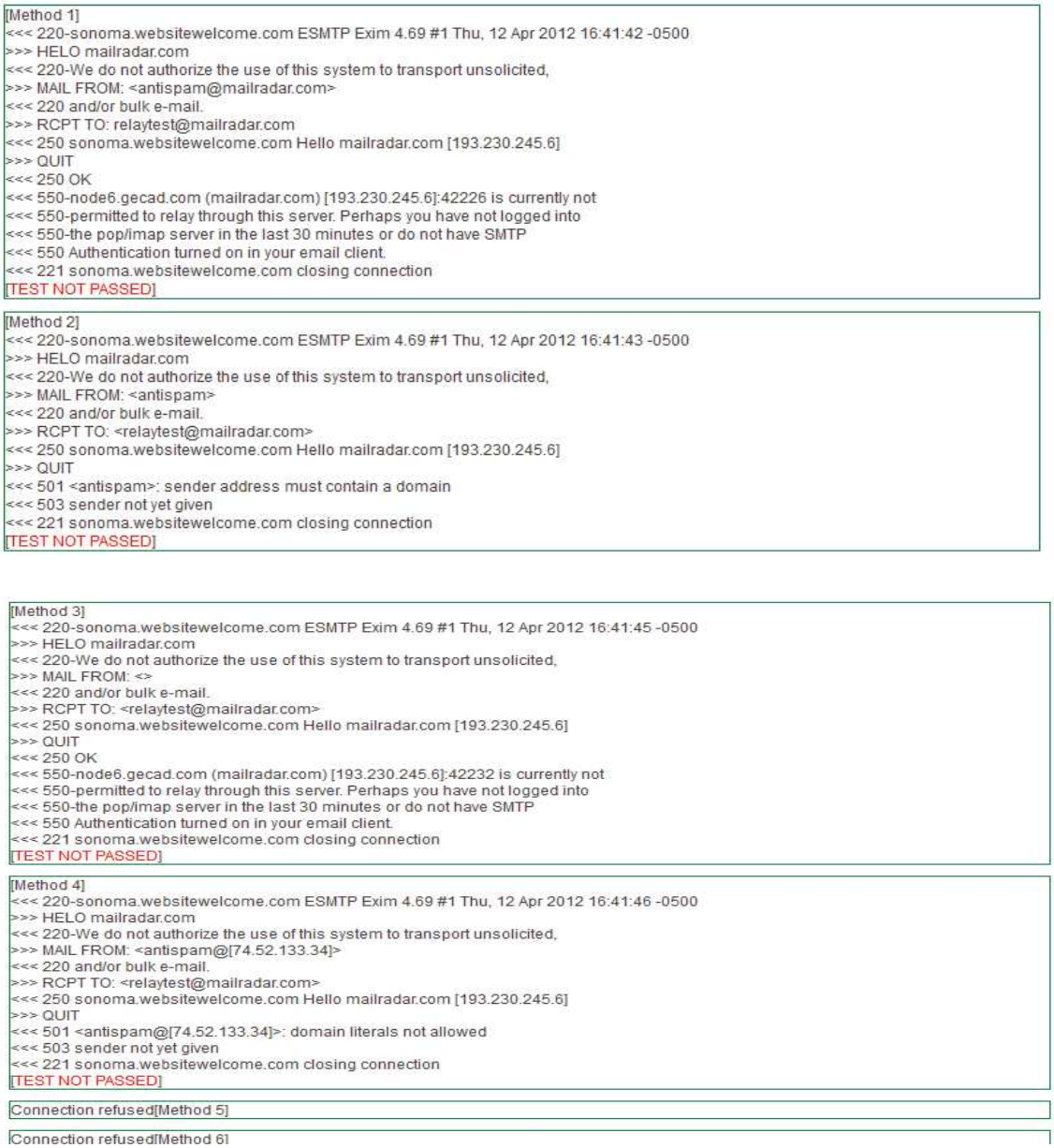


Fig 3.23 Prueba Open Relay

3.6 EVALUACIÓN PÁGINA WEB

En esta prueba se va a evaluar, cual es la velocidad con la que se accede a la página web de la empresa Marketwatch y de esta manera ver si es óptima o no.

Se va a realizar 2 tipos de pruebas utilizando el siguiente web site http://www.webmasterlibre.com/2006/09/05/tests-de-velocidad-de-carga-de-sitios-web/

Website Speed Test

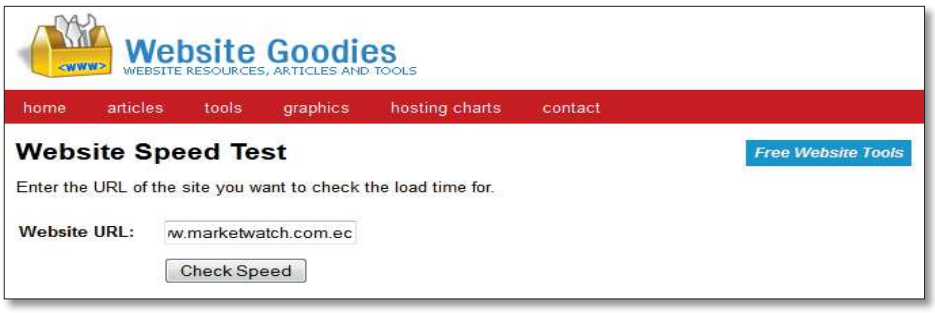


Fig 3.24 Ingreso Website Empresa

Se ingresa la dirección web de la empresa para evaluar la velocidad de la página.

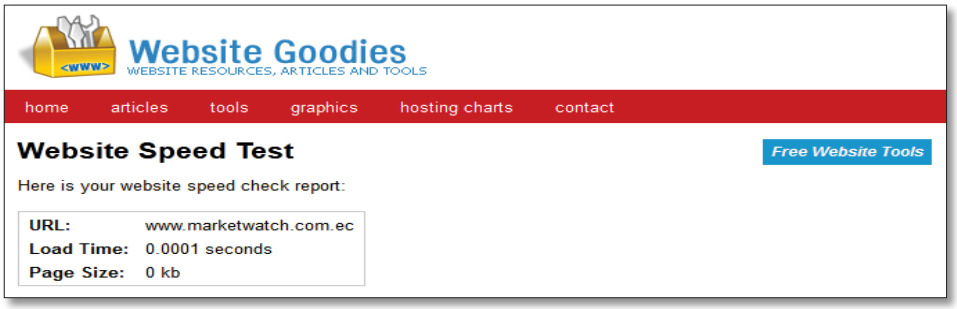


Fig 3.25 Tiempo Respuesta Website

Con este test se medirá el tiempo de carga y el tamaño de la página web.

Web Page Analyzer

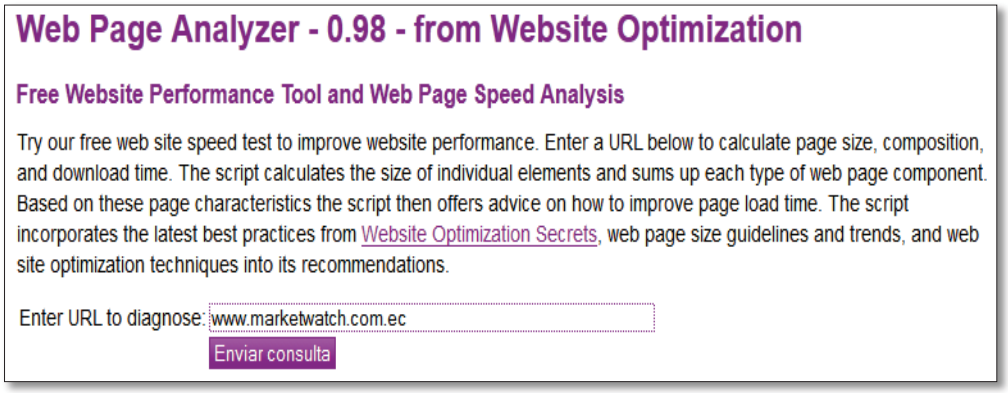


Fig 3.26 Consulta Website

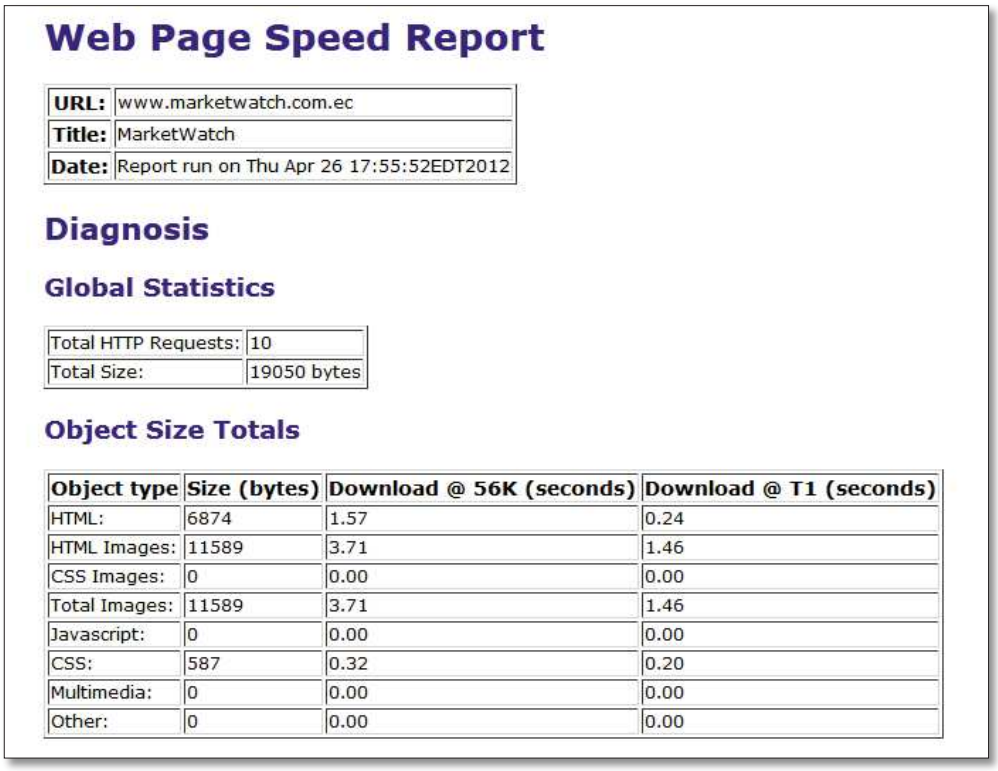


Fig 3.27 Resultados Website

Este test a más de analizar el tiempo de carga de la página, muestra la información referente a imágenes, código HTML, css, scripts entre otros.

EVALUACIÓN HARDWARE

3.7 EVALUACIÓN RENDIMIENTO DEL SISTEMA

Para realizar esta prueba se consideró hacerlo a diferentes horas del día, para de esta manera tener una visión más amplia de cómo está el funcionamiento de los equipos en el área de operaciones.

Los horarios para realizar las pruebas en los 3 equipos del área de operaciones serán las siguientes:

- 8h30
- 12h30
- 17h30

Estación 1

Hora Prueba: 8:30

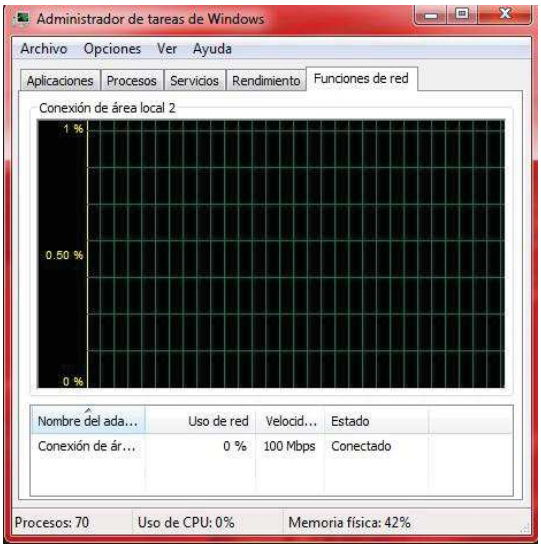


Fig 3.28 Análisis Función de Red

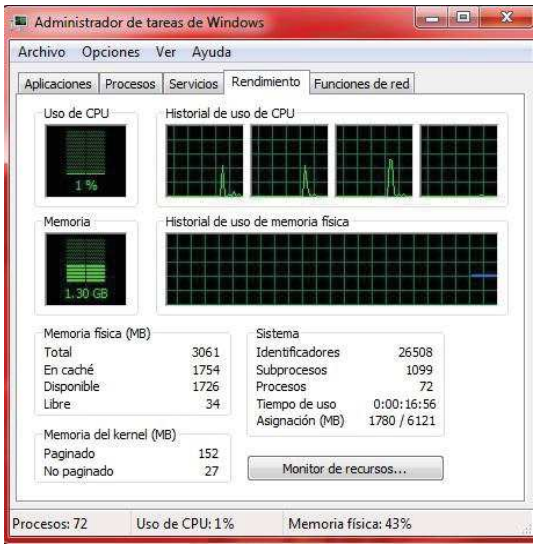
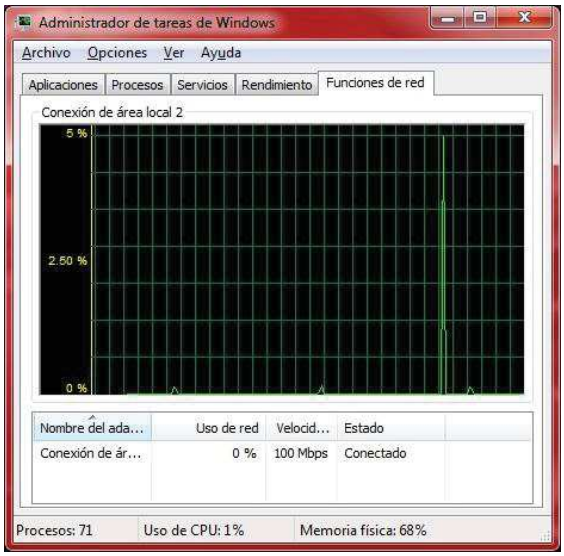


Fig 3.29 Análisis Memoria RAM

Hora Prueba: 12:30



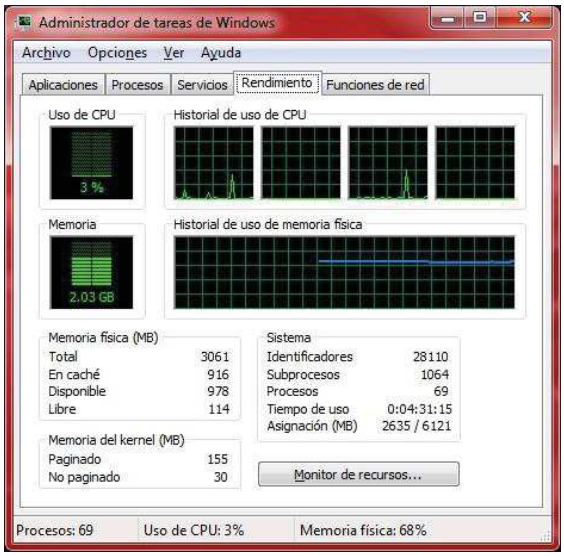
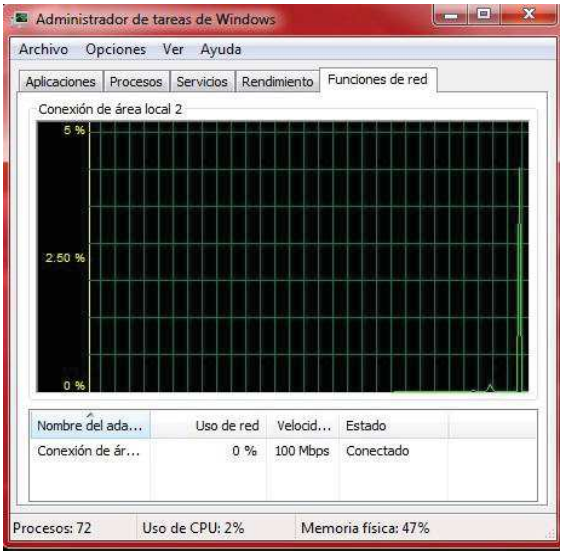


Fig 3.30 Análisis Función de Red

Fig 3.31 Análisis Memoria RAM

Hora Prueba: 17:30



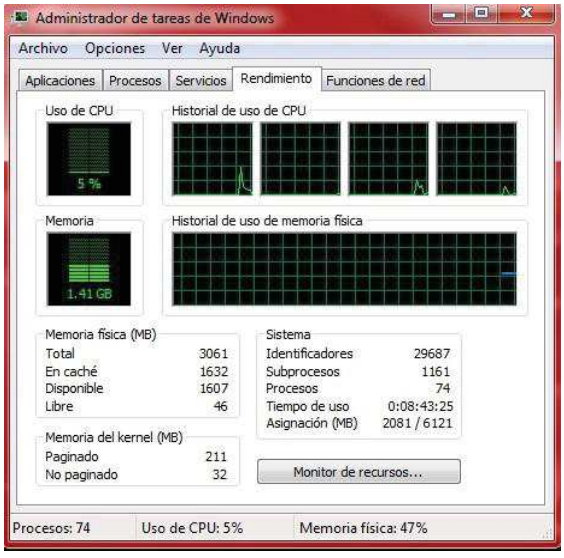


Fig 3.32 Análisis Función de Red

Fig 3.33 Análisis Memoria RAM

Estación 2

Hora Prueba: 8:30

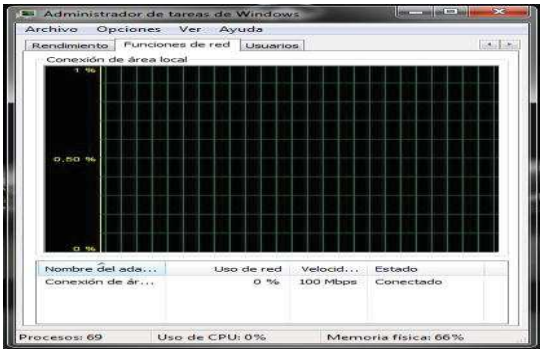


Fig 3.34 Análisis Función de Red

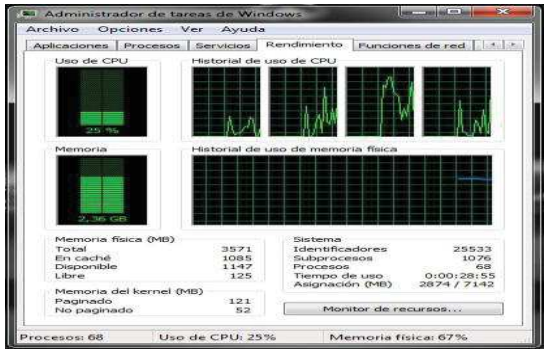


Fig 3.35 Análisis Memoria RAM

Hora Prueba: 12:30

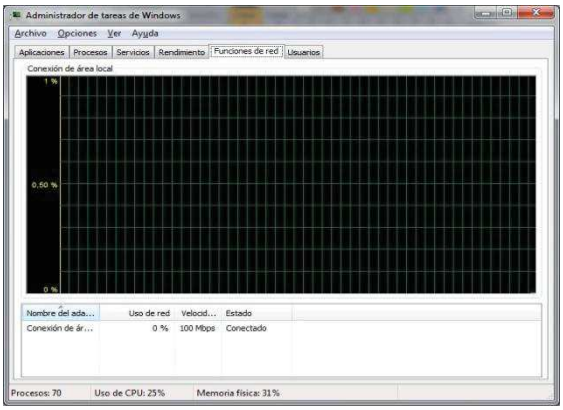


Fig 3.36 Análisis Función de Red

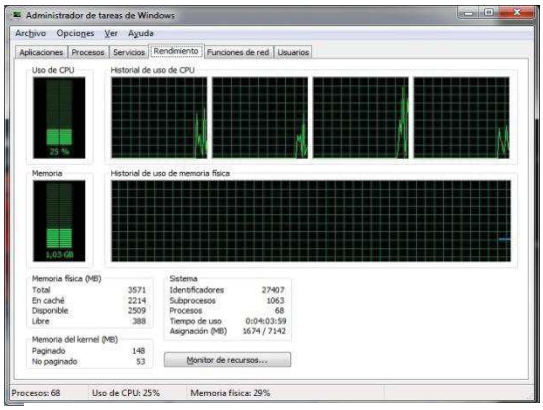


Fig 3.37 Análisis Memoria RAM

Hora Prueba: 17:30

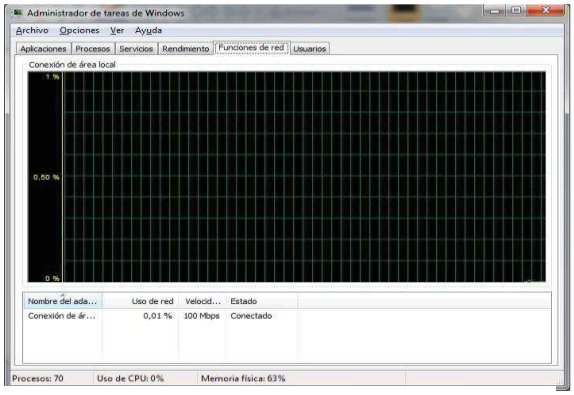


Fig 3.38 Análisis Función de Red

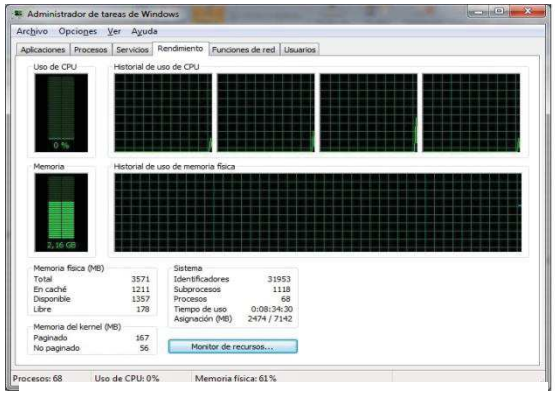


Fig. 3.39 Análisis Memoria RAM

Estación 3

Hora Prueba: 8:30

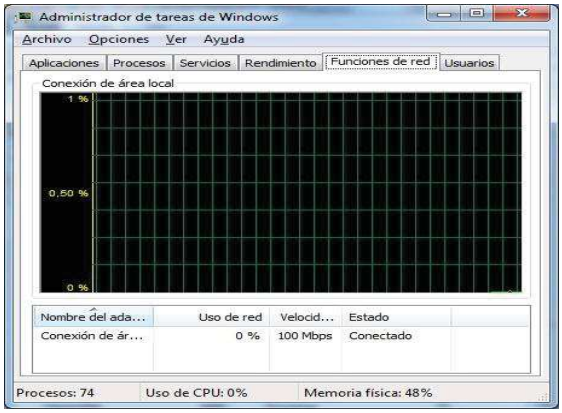


Fig 3.40 Análisis Función de Red

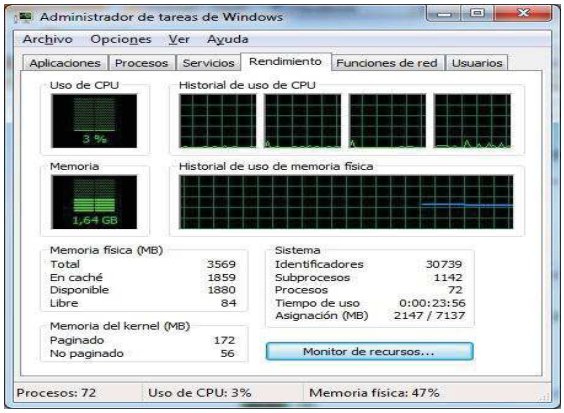


Fig 3.41 Análisis Memoria RAM

Hora Prueba: 12:30

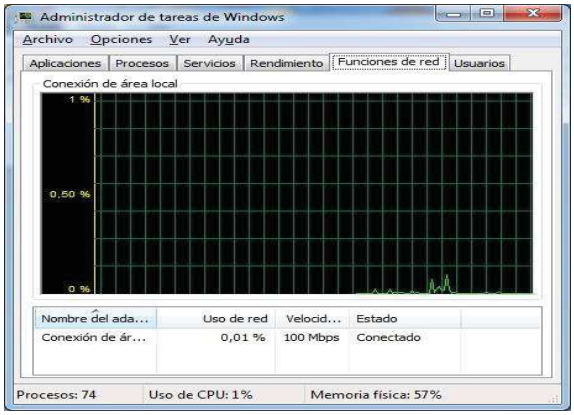


Fig 3.42 Análisis Función de Red

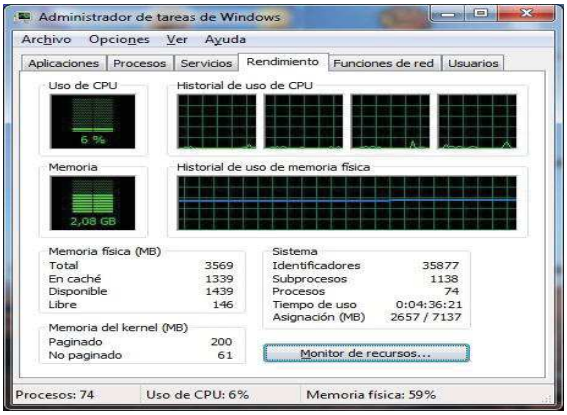


Fig 3.43 Análisis Memoria RAM

Hora Prueba: 17:30

Fig 3.44 Análisis Función de Red

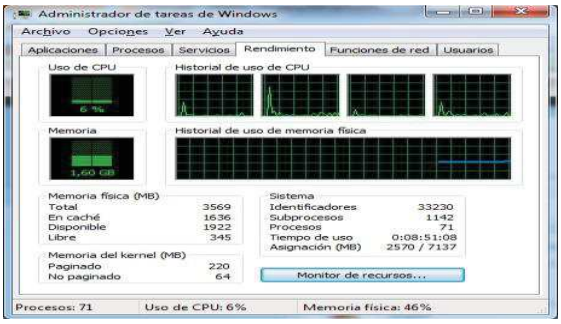


Fig 3.45 Análisis Memoria RAM

CAPÍTULO IV: INFORME FINAL AUDITORÍA

EMPRESA AUDITADA: Marketwtach S.A.

Señor Gonzalo Rueda

GERENTE GENERAL

El presente documento tiene el fin de entregarle el informe final de la Auditoria de Seguridad Interna y Perimetral de la empresa Marketwatch en el Área de Operaciones.

Misma que se realizó en la ciudad de Quito desde el 17 de diciembre 2011 hasta el 16 de junio 2012 en la cual se recopiló información tanto de la parte de software como de hardware, la cual será presentada a detalle en el presente informe.

4.1 HARDWARE

En este informe final en lo concerniente a la parte de hardware, se realizó las pruebas tanto de rendimiento y consumo de memoria, a diferentes horarios en el transcurso del día, para determinar el desempeño de los equipos en el área de operaciones, de lo cual se obtuvo los siguientes resultados.

Cabe señalar que las pruebas se efectuaron en 3 horarios diferentes del día para ver como se encuentra el comportamiento de cada estación de trabajo.

Rendimiento del Sistema

Horario / Estaciones	8h30	12h30	17h30
PC1	1%	3%	5%
PC 2	25%	25%	0%
PC 3	3%	6%	6%

Fig 4.1 Tabla Resultados Rendimiento Sistema

Según los resultados que nos arroja la tabla de rendimiento del sistema se concluye que 2 de las 3 máquinas tienen un rendimiento óptimo dentro de los parámetros normales, cabe señalar que la máquina que presenta un rendimiento del 25%, se debe a que dicha máquina utiliza programas que consumen más procesamiento y memoria, además de manejar bases de datos que contienen grandes registros.

Uso Memoria RAM

Horario / Medición / Estaciones Trabajo	8h30	12h30	17h30
PC1	1.30 GB	2.03 GB	1.41 GB
PC 2	2.36 GB	1.03 GB	2.16 GB
PC 3	1.64 GB	2.08 GB	1.60 GB

Fig 4.2 Tabla Resultados Rendimiento Memoria RAM

En cambio en la tabla del uso de la memoria RAM, se observa que hay un consumo aceptable de memoria en el transcurso del día ya que la memoria total que tiene cada máquina es de 8GB.

4.2 SOFTWARE

4.2.1 AUDITORIA SISTEMA OPERATIVO

El sistema operativo instalado en las PCS de la empresa Marketwatch, es Windows 7 Professional, todas con licencia.

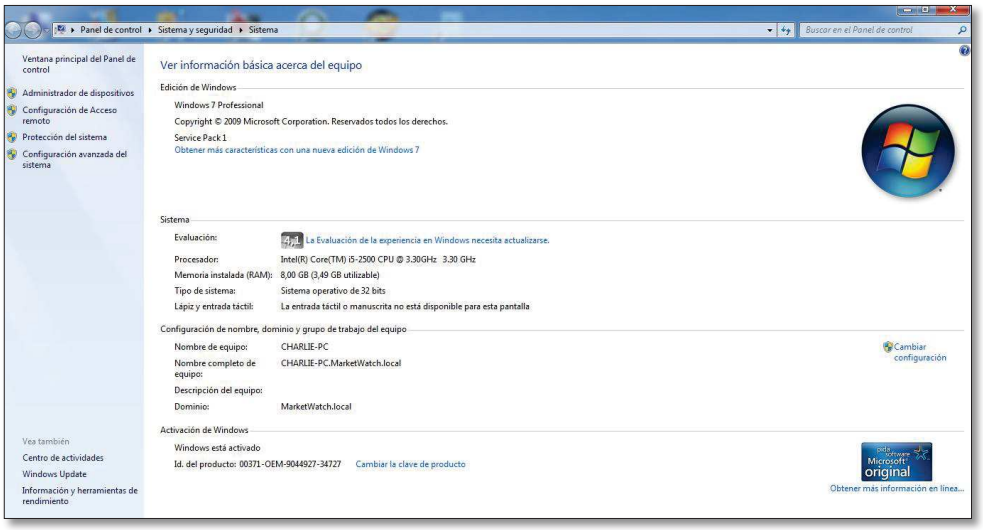


Fig 4.3 Licencia Sistema Operativo

A continuación se muestra un cuadro descriptivo del porcentaje de máquinas que tienen el sistema operativo Windows 7 Professional y su licenciamiento.

SISTEMA OPERATIVO	MÁQUINAS	LICENCIAMIENTO
Windows 7 Professional	100%	100%
Linux (Servidor)	100%	100%

Fig 4.4 Tabla Resultados Sistemas Operativos Empresa

Como se puede apreciar en la tabla, todas las máquinas del área de operaciones tienen el mismo sistema operativo y su respectiva licencia, incluyendo el servidor con sus respectivas licencias CAL.

CONCLUSIONES

- El sistema operativo actual es acorde a los requerimientos que la empresa necesita en estos momentos.

- Software totalmente licenciado.

RECOMENDACIONES

- Mantener actualizado el sistema operativo con las actualizaciones automáticas que provee en mismo Windows cada vez que estén disponibles.

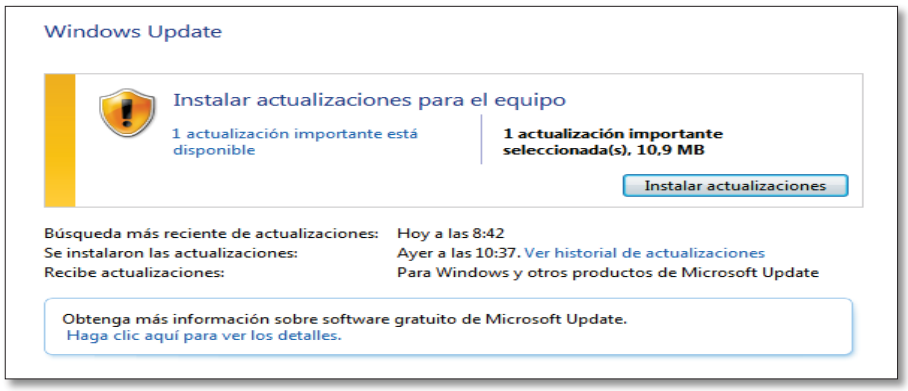


Fig 4.5 Ventana Actualizaciones Automáticas

- Realizar mantenimientos preventivos de hardware (Semestralmente), para así de esta manera optimizar las tareas que realiza el usuario en el equipo y así evitar un pago innecesario a futuro por soporte técnico.

- Verificar programas y aplicaciones (Software) que no se usen regularmente y eliminarlas para de esta manera liberar espacio en el disco duro y optimizar el rendimiento del equipo.

4.2.2 AUDITORÍA DE ANTIVIRUS

La auditoría que se hizo al antivirus AVG Internet Security Business 2012, mismo que se encuentra instalado en las todas las maquinas de la empresa, no se tiene licencia (Software crackeado).

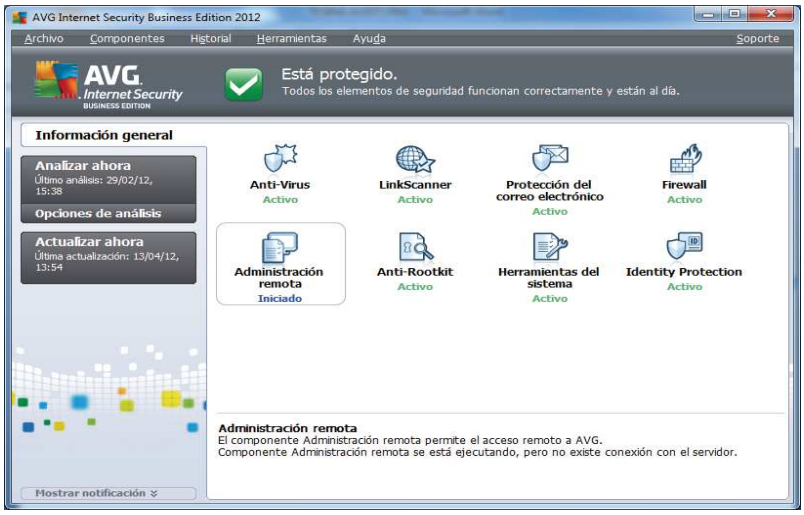


Fig 4.6 Ventana Antivirus AVG

Además de este antivirus algunas de las máquinas también cuentan con otro antivirus gratuito como lo es Microsoft Security Essentials fig 4.6.

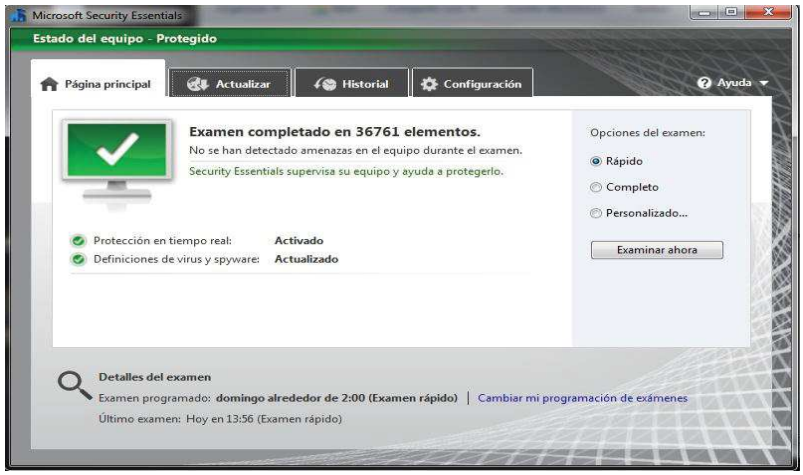


Fig 4.7 Ventana Antivirus Microsoft Essentials

Para esta auditoría de antivirus se realizó las pruebas con el software de EICAR, del cual se obtuvieron los siguientes resultados:

ANTIVIRUS	MÁQUINAS	LICENCIAMIENTO	Eicar Resultado
AVG Internet Security Business 2012	100%	No Software Crackeado	100%
Microsoft Security Essentials 2012	66%	Free	100%

Fig 4.8 Tabla Resultados Antivirus

Según estas pruebas se demuestra que ambos antivirus tienen una efectividad buena para detectar amenazas que pudieran llegar a dañar el sistema operativo de alguna de las máquinas de la empresa.

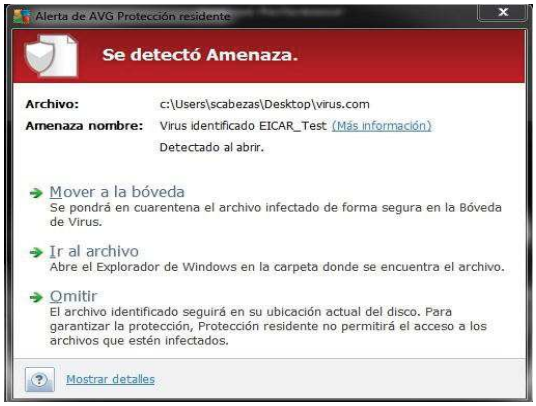


Fig 4.9 Resultado Prueba AVG **Fig 4.10 Resultado Prueba Essentials**

CONCLUSIONES

- Ambos antivirus se los puede considerar seguros para detectar cualquier amenaza a pesar de ser un software crackeado.

- La base de virus se actualiza automáticamente a diario, lo cual optimiza tiempo.

RECOMENDACIONES

- Adquirir software licenciado ya que las versiones free o crackeadas no garantizan su funcionamiento y no podrían detectar todas las amenazas que existen en la red.

- Analizar dispositivos externos antes de abrir cualquier documento que se encuentren en el mismo para evitar infecciones en o los equipos.

- No tener instalado más de un antivirus, ya que muchos de estos programas suelen detectar como virus al otro, lo que puede generar problemas o bajo rendimiento del sistema.

4.2.3 AUDITORÍA OFIMÁTICA

La empresa Marketwatch utiliza como herramienta de ofimática Microsoft Office 2007 Professional en todas sus estaciones de trabajo.

APLICACIÓN	LICENCIADO
Microsoft Office 2007 Professional	90%

Fig 4.11 Tabla Resultados Herramienta Ofimática

CONCLUSIÓN

- Se debe tratar de que todas las estaciones cuenten con licenciamiento.

RECOMENDACIÓN

- Adquirir software original para evitar futuras sanciones o problemas en el equipo, las cuales generalmente se producen cuando hay actualizaciones del sistema operativo.

CONCLUSIONES Y RECOMENDACIONES GENERALES DE LA AUDITORÍA REALIZADA A LA EMPRESA MARKETWATCH

Finalizada la auditoría a la empresa Marketwatch, se procede a generar algunas observaciones acerca de las prioridades en las que tiene que poner énfasis la empresa, así como también algunas recomendaciones para ayudar al mejoramiento de la empresa en general tanto en la parte de software como hardware.

OBSERVACIONES

- ✓ El funcionamiento de la red se encuentra acorde al tamaño de la empresa.
- ✓ No existen políticas para regular el uso de la red de la empresa Marketwatch.
- ✓ No existe una seguridad para los datos dentro de la red.
- ✓ La seguridad física de los equipos de telecomunicaciones no es la más óptima ya que están a vista y acceso de cualquier persona que ingrese a la oficina.
- ✓ No existe documentación del cableado de la red.
- ✓ No se deben colocar contraseñas para acceso a equipos en lugares visibles.
- ✓ El acceso a internet no tiene políticas implementadas.

- ✓ Las políticas de acceso a equipos de escritorio, están implementadas mediante directorio activo.
- ✓ No se evaluó la parte eléctrica.
- ✓ No se obtuvo respuesta positiva por parte del proveedor para realizar pruebas perimetrales.
- ✓ No se realizaron pruebas en la red inalámbrica, ya que en el departamento de operaciones, no existe.

CONCLUSIONES

- ✓ Finalizada las pruebas al servidor DNS de la empresa se puede decir que es un servidor que no reporta problemas a la hora de una conexión en ninguna de las pruebas realizadas anteriormente.

- ✓ Finalizada la prueba de open relay se logró detectar 5 métodos y en los cuales se aprecia que no están utilizando este servidor para que envíe correo basura (SPAM) en forma indiscriminada como se conoce al open relay.

- ✓ Finalizada las pruebas a los antivirus de la empresa, no se detectaron vulnerabilidades.

- ✓ Finalizada la prueba de listas negras se reporta que no posee ningún problema de generación de SPAM.

- ✓ Finalizada la verificación de contraseñas de la empresa se concluye que las máquinas del área de operaciones poseen contraseñas fuertes que difícilmente podrán ser vulneradas.

- ✓ Finalizada la prueba a la página web muestra que el tiempo de respuesta es el óptimo para acceder a la información de la misma

RECOMENDACIONES

- ✓ Los equipos de comunicaciones deben estar en un armario de telecomunicaciones y de fácil acceso para cuando se requiera realizar mantenimiento de la red o corregir algún error en la misma.
- ✓ Se debe tener una política de mantenimiento tanto preventivo como correctivo de todos los equipos.
- ✓ Tener un plan de licenciamiento de software.
- ✓ Realizar backups incrementales de manera semanal, para esto, implementar servidor de almacenamiento NAS.
- ✓ Se debe sacar respaldos de información de usuario, así como archivos de trabajo, nada de música, videos etc.
- ✓ Se recomienda utilizar un firewall de hardware.
- ✓ El desempeño del antivirus utilizado es correcto, no existe antivirus 100% seguro, se recomienda reemplazar el antivirus actual y reemplazarlo por uno licenciado.
- ✓ Tener una persona quién se encargue de llevar e implementar políticas de contraseñas en la empresa (Administrador de Red o encargado de sistemas).

GLOSARIO

“ETHERNET

También conocido como estándar IEEE 802.3, es un estándar de transmisión de datos para redes de área local.

GIGABIT ETHERNET

También conocida como GigaE, es una ampliación del estándar Ethernet que consigue una capacidad de transmisión de 1gigabit por segundo.

TIA/EIA-606-A

Estándar para la administración de infraestructura de telecomunicaciones en edificios comerciales.

MAC

Son las siglas de (Media Access Control) y se refiere al control de acceso al medio físico, o sea que la dirección MAC es una dirección física.

SOFTWARE DEL SISTEMA

Es un software diseñado para operar en el hardware del equipo y proporcionar y mantener una plataforma para ejecutar software de aplicación.

SOFTWARE DE APLICACIÓN

Es aquel que hace que el computador coopere con el usuario en la realización de tareas típicamente humanas, tales como gestionar una contabilidad o escribir un texto.

SOFTWARE DE PROGRAMACIÓN

Es un tipo especial de software que nos permite crear/desarrollar/programar otras aplicaciones. Los softwares de programación son los que dan origen a los programas que utilizamos día a día.

MTA

Agente de Transferencia de Correo (Mail Transport Agent) es uno de los programas que ejecutan los servidores de correo y tiene como fin transferir un conjunto de datos de una computadora a otra.

ETHERNET 10 BASE T

Esta es la extensión IEEE 802.3i del estándar Ethernet que especifica el uso de UTP como medio.

Ethernet 10BASE-T es el primer estándar para redes locales (LAN) que considera las recomendaciones hechas en un sistema de cableado estándar.

ETHERNET 100 BASE-TX

Es la forma predominante de Fast Ethernet a 100Mbit/s perteneciente al estándar 100Base-T. Utiliza dos pares de hilos Cat5 o mejores.

HALF DUPLEX

Cuando dos equipos se comunican en una LAN, la información viaja normalmente en una sola dirección a la vez, dado que las redes en banda base usadas por las redes LAN admiten solo una señal.

FULL DUPLEX

Son dos sistemas que se pueden comunicar simultáneamente en dos direcciones.

VPN

Una VPN (Virtual Private Network) conecta hosts de una red a otra red, virtualmente se genera un túnel atravesando internet, permitiendo la comunicación entre ambas redes, con la misma seguridad disponible en una red privada.

Cuando un túnel se genera los hosts de un extremo pueden establecer contacto directo con los hosts del otro extremo.

ENCRIPTACIÓN WPA

Su finalidad es evitar intrusos en una red wifi, el mayor inconveniente es que no son muchos los dispositivos wifi que la soportan.

ENCRIPTACIÓN TKIP

(Temporal Key Integrity Protocol). En criptografía, TKIP es un protocolo de seguridad usado en WPA (Wi-Fi Protected Access) para mejorar el cifrado de datos en redes inalámbricas. WPA es utilizado en redes Wi-Fi para corregir deficiencias en el antiguo estándar de seguridad WEP.

ENCRIPTACIÓN WPA2

Este producto es compatible con productos anteriores que utilizan WPA. La principal diferencia entre WPA y WPA2 es que WPA2 requiere el estándar de encriptación avanzado (AES).

AES

Conocida como Estándar de Encriptación Avanzada (Advanced Encryption Standard). AES es una técnica de cifrado de clave simétrica que remplazará el Estándar de Encriptación de Datos (DES) utilizado habitualmente.

CALIDAD DE SERVICO

QoS es un conjunto de estándares y mecanismos que aseguran la calidad en la transmisión de los datos en programas habilitados para QoS.

DES

(Data Encryption Standard - Algoritmo de Encriptación Estándar). Desarrollado por IBM, es un algoritmo de cifrado que utiliza bloques de datos de 64 bits y clave de 56 bits. No es suficientemente seguro, pues es vulnerable al ataque por fuerza bruta, lográndose, por ejemplo, romper su seguridad en 24 horas.

CLAVE SIMÉTRICA

El cifrado mediante clave simétrica significa que dos o más usuarios, tienen una única clave secreta, esta clave será la que cifrará y descifrará la información transmitida a través del canal inseguro.

Es decir, la clave secreta la debe tener los dos usuarios, y con dicha clave, el usuario A cifrará la información, la mandará a través del canal inseguro, y a continuación el usuario B descifrará esa información con la misma clave que ha usado el usuario A.

CLAVE ASIMÉTRICA

Es el método criptográfico que usa un par de claves para el envío de mensajes; las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

LICENCIAS CAL

Si los PCs de la compañía están conectados en red, usted utiliza un servidor en red y los PCs de la red acceden al software del servidor (o servidores) para realizar determinadas funciones como compartir archivos e imprimirlos, para poder acceder a este software de manera legal, usted necesita una **Client Access License** o **CAL**. Una CAL no es un software; es una licencia que le da al usuario el derecho a utilizar los servicios de un servidor.

CABLE DE RED UNIFILAR Y MULTIFILAR

El cable unifilar trae un solo filamento por pin y es rígido, en cambio el multi filar trae varios filamentos por pin, lo que lo hace más flexible". Tomadas de internet, referencia en bibliografía

REFERENCIAS

http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

http://vbarreto.ve.tripod.com/keys/audi/audi01.htmlhttp://archivosauditoria.blogspot.com/2009/11/auditoria-informatica-de-comunicaciones.html

http://www.masadelante.com/faqs/software-hardware

http://www.masadelante.com/faqs/servidor

http://www.masadelante.com/faqs/tipos-de-servidores

http://www.segu-info.com.ar/firewall/firewall.htm

http://contenido.metrocuadrado.com/contenidom2/noticias_m2/juliode2007/ARTICULO-WEB-PL_DET_NOT_REDI_M2-3583266.html

http://www.dlinkla.com/home/productos/producto.jsp?idp=1416

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

http://www.mapelectronica.com.ar/centrales_telefonicas_panasonickx-tes824.htm

http://translate.google.com.ec/translate?hl=es&sl=en&u=http://www.cisco.com/en/US/docs/routers/access/1700/1720/hardware/installation/guide/intro.html&ei=uzUXT7HSII2rsALu7dCkAg&sa=X&oi=translate&ct=result&resnum=4&sqi=2&ved=0CEwQ7gEwAw&prev=/search%3Fq%3Drouter%2Bcisco%2B1700%2Bcaracteristicas%26hl%3Des%26fhp%3D1%26biw%3D1034%26bih%3D619%26prmd%3Dimvns

http://www.vsantivirus.com/eicar-test.htm

http://password.es/comprobador/

http://www.softonic.com/s/dns-benchmark

http://www.mxtoolbox.com/

http://www.mailradar.com/openrelay/

http://www.webmasterlibre.com/2006/09/05/tests-de-velocidad-de-carga-de-sitios-web/

http://es.kioskea.net/contents/technologies/ethernet.php3

http://es.scribd.com/doc/54477905/50/ACTUALIZACION-ESTANDAR-EIA-TIA-606-A

http://www.internetmania.net/int0/int55.htm

http://www.tiposdesoftware.com/tipos-de-software-de-sistema.htm

http://www.bloginformatico.com/software-de-aplicacion.php

http://www.webadicto.net/blogs/webadicto/post/2011/01/24/Que-es-un-Software-de-Programacion.aspx

http://www.textoscientificos.com/redes/ethernet/10base-t

http://www.alegsa.com.ar/Dic/100base-tx.php

http://www.mailxmail.com/curso-conceptos-basicos-redes/comunicaciones-half-duplex-full-duplex

http://www.taringa.net/posts/info/905575/Que-es-una-VPN_.html

http://www.configurarequipos.com/doc537.html

http://www.alegsa.com.ar/Dic/tkip.php

http://www.linksysbycisco.com/LATAM/es/learningcenter/WPAyWPA2

http://www.bitzipper.com/es/aes-encryption.html

http://technet.microsoft.com/es-es/library/cc779870(v=ws.10).aspx

http://www.alegsa.com.ar/Dic/des.php

http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

http://www.multicomp.com.mx/noticias/licenciamiento-microsoft-%C2%BFque-es-una-client-access-license-cal-2/

http://foro.elhacker.net/redes/que_diferencia_entre_cable_de_red_unifilar_y_multifilar-t54929.0.html