FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

ESCUELA DE TECNOLOGÍA EN REDES Y TELECOMUNICACIONES.

AUDITORÍA DE SEGURIDAD INFORMÁTICA INTERNA Y PERIMETRAL PARA LA EMPRESA CAROLINA CONSTRUCCIONES.

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

JOHANNA SORAYA CHICAIZA PINEIDA

Año

2012

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con la estudiante Johanna Chicaiza, 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.

Número Cédula

C.I: 1711476083

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”

JOHANNA SORAYA CHICAIZA PINEIDA

Número Cédula

C.I:1724359409

AGRADECIMIENTOS

A mis padres que con su amor y bondad me dieron la oportunidad de crecer y dejar huellas en las personas que han compartido conmigo. A la Universidad de las Américas que en conjunto con sus docentes inculcaron valores morales y éticos en mí.

DEDICATORIA

Este trabajo se lo dedico en especial a Dios por darme una fuerza inexplicable para afrontar la vida con amor, perseverancia, convicción y por colmar de bendiciones a mi familia.

RESUMEN

El presente trabajo tiene como finalidad desarrollar una Auditoría de Seguridad Informática Interna y Perimetral para la empresa de ING. ELECTRICA CAROLINA CONSTRUCCIONES.

Con el fin de revelar la consistencia de los sistemas de información y la red. La eficiencia y efectividad de los programas, operaciones , el cumplimiento de políticas y normas tanto en Hardware y Software, como resultado se detallan las debilidades encontradas y se emiten recomendaciones formulando un documento con el diseño adecuado y configuración de la red.

El objetivo es elaborar un reporte en base al análisis de los resultados obtenidos y realizar recomendaciones que contribuyan a mejorar los niveles de seguridad.

En el proyecto se utilizará la metodología explicativa e investigativa.

ABSTRACT

The present work aims to develop an Internal Audit and Information Security Perimeter for the company ING. CAROLINA ELECTRIC CONSTRUCTION. In order to reveal the consistency of information systems and the network. The efficiency and effectiveness of programs, operations, compliance with policies and standards both in hardware and software, as a result details the weaknesses identified and recommendations are issued a document asking the right design and network configuration.

The aim is to produce a report based on the analysis of the results and make recommendations to help improve safety levels.

The project will use the explanatory and investigative methodology.

INDICE.

Introducción.

En el presente documento se detalla la **Auditoría de Seguridad Informática Interna y Perimetral para la empresa de Ing. Eléctrica CAROLINA CONSTRUCCIONES.**

“Desde los inicios de la Humanidad distintas culturas han dado una importancia enorme a los temas de contabilidad y por tanto también han necesitado de medios que permitieran verificar sus registros, es decir, de la auditoría. De hecho se piensa que la invención de la escritura surgió como respuesta a la necesidad de auditar, Flesher (1993): por lo que la de auditor sería una de las profesiones más antiguas.

A partir de 1950, la informática se convierte en una herramienta muy importante en las labores de auditoria financiera ya que permite llevar a cabo de forma rápida y precisa, operaciones que manualmente consumirían demasiados recursos. Empieza la denominada “auditoria con el computador” que no puede considerarse verdadera auditoría informática, sino que utiliza el computador como herramienta del auditor financiero.

Sin embargo al convertirse los sistemas de información de la empresa cada vez más dependientes de los computadores, surge la necesidad de verificar que los sistemas informáticos funcionan correctamente, empezándose a finales de los años sesenta a descubrirse varios casos de fraude cometidos con ayuda del computador que hacen inviable seguir conformándose con la auditoria “alrededor del computador” Surge así la necesidad de una nueva especialidad dentro de la auditoría, cuyo objetivo es precisamente verificar el funcionamiento correcto eficaz y eficiente de la informática.” (Piattini, 2005)

A inicios del año 3000 A.C aparecen los primeros indicios de la seguridad. Las obras como la Biblia, Homero, Cicerón muestran evidencias de ciertos rasgos de seguridad en el gobierno y la guerra.

Descubrimientos arqueológicos en Egipto que muestran al dios Anubi representado con una llave. La civilización Maya que ocultaba sus secretos, descubrimientos y los protegía con mucho cuidado.

Nuestros ancestros en la antigüedad utilizaban métodos defensivos para evitar ser atacados. La ciudad de Roma que fue una cultura organizada y segura, con el paso del tiempo fue dando lugar a que el concepto de seguridad creciera, así como los descubrimientos de los científicos.

La seguridad moderna nace con la seguridad industrial y Henry Fayol en 1919 identifica la seguridad como una de las funciones empresariales.

Es una necesidad para todas las empresas proteger la información y mantener una adecuada infraestructura en la red, las nuevas tecnologías informáticas ofrecen un nuevo campo de acción a conductas antisociales y delictivas.

La falta de medidas de seguridad en las redes, genera problemas que permiten a los atacantes informáticos, especializarse cada día más para causar daño en la red, provenientes del exterior o interior de la organización.

En este trabajo se realizará una breve introducción de conceptos de Auditoria y Seguridad Informática, su importancia en la actualidad.

A continuación se procederá con el levantamiento de información y con la auditoria de la infraestructura de red. A partir del análisis existente y conociendo las limitaciones encontradas se irán perfilando las posibles recomendaciones de seguridad informática, resumiendo los resultados de la evaluación del proyecto.

Con la realización de este documento se demostrará como, mediante la utilización de políticas de seguridad existentes en la actualidad, se puede reducir la problemática de seguridad en hardware, software y disminuir el riesgo de vulnerabilidad en la red.

1. Capítulo I Fundamentación Teórico.

1.1 Definición del proyecto.

Auditoria de Seguridad Informática Interna y Perimetral para la empresa de ING. ELECTRICA CAROLINA CONSTRUCCIONES.

1.1.1 Antecedentes

- Se tiene una red de cableado antigua Cat.5E motivo por el cual la velocidad de transmisión de datos máxima es de 100BaseT.
- No existe un Administrador de red que proporcione seguridad a la información y realice un monitoreo en la red constantemente.
- No existen políticas de Seguridad.
- No se ha elaborado un análisis de los reportes y servicios de mantenimiento correctivo y preventivo de la red.
- El 87 % de antivirus no es licenciado y no se realizan las actualizaciones respectivas.
- El 50 % de las contraseñas de usuarios en las PC no son robustas.
- El Cuarto de Equipos no tiene etiquetado adecuado.
- No existe un plano de red ni documentos donde se puedan encontrar las contraseñas y programas instalados en las PC.
- El direccionamiento IP es inadecuado.

1.1.2 Formulación del problema

- La falta de un Administrador de red genera un alto riesgo de pérdida de información.
- La falta de elaboración de un análisis de mantenimiento correctivo y preventivo de red hace más vulnerable a la red tanto en hardware como en software en caso de accidentes, daños, pérdida de la información, escalabilidad o la implementación de nuevas tecnologías.

- La utilización de antivirus desactualizados son parcialmente mejor que ninguno lo que limita al administrador de red al proteger la información y evitar ataques de software malicioso.
- El desorden y la falta de nomenclatura de los cables de red generan conflictos para administrar la red.
- La falta de planos y documentos que especifiquen como está constituida la red dificulta el mantenimiento y soporte.
- Mala configuración en la red impide la comunicación entre PC y difícil administración de la misma.

1.1.3 Objetivos.

1.1.3.1 Objetivo General.

Recomendar políticas de seguridad de red adecuadas a la necesidad de la empresa CAROLINA Construcciones mediante la Auditoria por realizar para evitar amenazas no deseadas que pueden ingresar por la mala administración y puertos de acceso externo (*firewall*) mal configurados. Cumpliendo con distintos parámetros y políticas que le permitan ser una red moderna, eficaz, segura y con posibilidad de expansión a otras tecnologías, redes y aplicaciones.

1.1.3.2 Objetivo Específico.

- Recomendar la necesidad de tener un administrador de red para que asigne direcciones *IP* adecuadas y realice una buena configuración y mantenimiento permanente en los dispositivos de *hardware* y *software*.
- Realizar una Auditoría generando un documento para detectar posibles vulnerabilidades y dar las recomendaciones necesarias de acuerdo a sus necesidades.
- Recomendar seguridad informática modificando las contraseñas de los dispositivos de redes constantemente y la utilización de antivirus licenciados para dar una configuración segura y evitar pérdidas de información.

- Elaborar un documento con el diseño adecuado y configuración de la red para la empresa CAROLINA Construcciones con el reporte de mantenimiento correctivo y preventivo de la red.

1.1.4 Alcance.

En esta Auditoria se realizará un diseño adecuado de la red y se dará a conocer las recomendaciones respectivas, no se procederá a realizar modificaciones en los equipos, sino que se elaborará un modelo óptimo y necesario de red para contrarrestar la inadecuada administración, configuración y estructura de la red con la que actualmente la empresa CAROLINA CONSTRUCCIONES cuenta.

Detallando en un documento el diseño del plano de la red no se procederá a configurar el Router porque es propiedad del proveedor de servicio, ni se detallará su configuración , pero si las conexiones del *Switch* y las direcciones *IP´S* adecuadas a utilizarse en las *PC´S* así como las contraseñas de los *host* que utilizan los usuarios , programas instalados y antivirus usando políticas de seguridad adecuadas a la necesidad de la empresa para mejorar la administración y no tener conflictos con el funcionamiento de la red.

Se levantará la información necesaria de la infraestructura de red elaborando un documento con el detalle de las configuraciones que se realizará en ciertos dispositivos. Se mejorará la organización y el etiquetado de los cables en el Cuarto de Equipos para poder dar solución eficaz a los problemas que se presenten en el futuro y no tener una difícil administración.

1.2 Conceptos auditoría y auditoría de seguridad informática.

Una Auditoria es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar si cumple o no las condiciones que le han sido prescritas.

Una Auditoria de seguridad informática es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Fases de una auditoría.

"Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos.
- Identificación de los sistemas operativos instalados.
- Análisis de servicios y aplicaciones.
- Detección, comprobación y evaluación de vulnerabilidades.
- Medidas especificas de corrección.
- Recomendaciones sobre implantación de medidas preventivas.

Tipos de Auditoría.

- Auditoría de seguridad interna: En este tipo de auditoria se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
- Auditoría de seguridad perimetral: En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores.
- Test de intrusión: Es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la

intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.

- Análisis forense: Es una metodología de estudio ideal para el análisis posterior de incidentes , mediante el cual se trata de reconstruir como se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperabilidad del sistema, el análisis se denomina postmortem.
- Auditoría de páginas web: Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, verificación de existencia y anulación de posibilidades de Cross Site Scripting (XXS),etc.
- Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones de paginas web como de cualquier tipo de aplicación, independientemente del lenguaje empleado.” (Santos, 2010)

Metodología de Auditoría de seguridad.

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas practicas sugeridas. Existen estándares orientados a servir como base para auditorías de informática.

Uno de ellos es COBIT (Objetivos de Control de las Tecnologías de la Información), dentro de los objetivos definidos como parámetros, se encuentra el de garantizar la seguridad de los sistemas.

Adicional a este estándar podemos encontrar ISO 27002 el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.

Para la realización de una auditoria en cualquiera de los ámbitos se requiere de una metodología a seguir las metodologías mas robustas son ITIL,Cobit y la

Norma ISO 20001 estas no serán tomadas en cuenta en su totalidad por que la empresa no cuenta con procesos definidos para la evaluación de los mismos.

La norma 27002 ayuda de mejor manera a evaluar a evaluar la seguridad informática en la empresa con esta norma se llevara a cabo la evaluación de los accesos de usuario.

ITIL se basa en servicios informáticos no será considerado por que no se requiere evaluar todo el ciclo de vida de dichos servicios sino solamente la entrega.

COBIT se la considera una metodología orientada al control de los procesos dentro de la unidad Informática por lo que no se tomaran en cuenta.

La metodología utilizada en el presente proyecto será metodología de la Auditoria Informática de las PYMES CHECKLIST basada en cuestionarios y ROA (Risk Oriented Approach) basada en evaluación de riesgos la minimización de los riesgos, que se conseguirá en función de que existan los controles y de que estos funcionen en conclusión se deberá revisar estos controles y su funcionamiento.

“Con una auditoría de seguridad se da una visión exacta del nivel de exposición de sus sistemas de información a nivel de seguridad.

En la auditoría se verifica la seguridad en la autenticidad, confidencialidad, integridad, disponibilidad y auditabilidad de la información tratada por los sistemas.

Los objetivos de una auditoría de seguridad de los sistemas de información son:

- Revisar la seguridad de los entornos y sistemas.
- Verificar el cumplimiento de la normativa y legislación vigentes.
- Elaborar un informe independiente.

La metodología para una auditoria de sistemas de información establece su ejecución por fases:

- ✧ Definir el alcance de la auditoria: análisis inicial y plan de auditoria.
- ✧ Recopilación de información, identificación y realización de pruebas de auditoría, incluyendo si se acuerda, acciones de hacking ético o análisis de vulnerabilidad de aplicaciones.
- ✧ Análisis de las evidencias, documentación de los resultados obtenidos y conclusiones.
- ✧ Informe de la auditoría en el que se recogen las acciones realizadas a lo largo de la auditoria y las deficiencias detectadas. El Informe contiene un resumen ejecutivo en el que se resaltan los apartados más importantes de la auditoría.
- ✧ Plan de Mejora con el análisis y las recomendaciones propuestas para subsanar las incidencias de seguridad encontradas y mantener en el futuro una situación estable y segura de los sistemas de información.

Las áreas de riesgo son:

1. Riesgo en la continuidad del proceso.
2. Riesgo en la eficacia del servicio.
3. Riesgo en la eficiencia del servicio.
4. Riesgo de la seguridad Física.
5. Riesgo de la seguridad Lógica.

Riesgo en la continuidad del proceso: Situaciones que pudieran afectar a la realización del trabajo informático o incluso paralizarlo.

Riesgo en la eficacia del servicio: La realización de los trabajos encomendados en la eficacia serán aquellos que alteren dicha realización o que afecten a la exactitud de los resultados ofrecidos por sistema informático.” (Santos, 2010)

“Riesgo en la eficiencia del servicio informático: La mejor forma de realizar los procesos o trabajos, ya sea a nivel económico o técnico, pretendiendo con el análisis de estos riesgos mejorar la calidad de servicio.

Riesgos económicos directos.

Se analizaran aquellas posibilidades de desembolsos directos inadecuados, gastos varios que no deberían producirse, e incluso aquellos gastos derivados de acciones ilegales con o sin consentimiento de la empresa.

Riesgos de la seguridad lógica.

Todo aquello que posibilite accesos no autorizados a la información mecanizada mediante técnicas informáticas o de otros tipos.

Riesgos de la Seguridad física.

Todo aquello que actué sobre sobre el deterioro o apropiación de elementos de información de manera física.

Valoración de los resultados.

En el primer sistema se responderá con SI NO N/A estos cuestionarios tendrán un valor numérico de 1 a 10

En el segundo sistema no existirá un número guía de ponderación y será el propio usuario quien deberá dar una valoración a la respuesta en estos casos los controles comenzaran con la propuesta evalué y la valoración que habrá que dar estará anexada a la pregunta con los valores máximos y mínimos.

Una vez que se finalice el cuestionario se sumaran los valores de la casilla SI y se restaran los del NO lo que nos dará un valor que pondremos comparar.” (Piattini, 2005)

CONTROLES	SI	NO	N/A
Existen planes a largo plazo para el departamento de informática.		7	
Valore la conexión de estos planes con planes generales de la empresa.			*
Cubren los planes del D.I. los objetivos a largo plazo de la empresa, valórelo.		7	
Existen un comité de planificación o dirección del departamento de informática.		*	
Dicho comité está compuesto por directivos de departamento de usuario.		*	
Existe en dicho comité algún miembro con conocimientos informáticos exhaustivos.		*	

1.2.1 Seguridad Física.

"La seguridad física es uno de los aspectos más olvidados a la hora del diseño

De un sistema informático. La seguridad física consiste en la aplicación de barreras físicas procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor de la ubicación física de los sistemas informáticos, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el Hadware y medios de almacenamiento de datos.

La seguridad física está enfocada a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro." (Santos, 2010)

Las principales amenazas que se prevén en la seguridad física son:

Amenazas ocasionadas por el hombre, como robos, destrucción de información o equipos etc.

1.2.1.1 Control de Acceso.

“Los ordenadores, servidores, así como las copias de seguridad con datos importantes y el software, son elementos valiosos para las empresas y están expuestas a posibles robos y actos delictivos como sabotajes o destrozos por parte de personal ajeno o propio de la empresa.

El software es una propiedad muy fácilmente sustraíble y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

En control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

El servicio de vigilancia es el encargo del control de acceso de todas las personas al edificio. Este servicio es el encargado de colocar los guardias en lugares estratégicos para culminar con sus objetivos y controlar el acceso del personal.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por algo que posee por ejemplo una llave, o una tarjeta de identificación, o tarjeta inteligente (SmartCard).

Cada una de éstas debe tener un PIN (Personal Identification Number) único siendo este el que se almacena en una base de datos que controla el servicio de vigilancia para su posterior seguimiento, si fuera necesario. Su mayor desventaja es que estas tarjetas pueden ser copiadas, robadas, etc permitiendo ingresar a cualquier persona que la posea.

Estas credenciales se pueden clasificar de la siguiente manera:

Normal o definitiva: para el personal permanente de la empresa.

Temporal: para personal recién ingresado.

Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.

Visitas: Para un uso de horas.

Las personas también pueden acceder mediante algo que se saben (por ejemplo un número de identificación o una password) que se solicitará a su ingreso. Al igual que el caso de las tarjetas de identificación los datos de introducidos se contrastarán contra una base donde se almacenan los datos de las personas autorizadas. Este sistema tiene la desventaja que generalmente se eligen identificación sencillas, bien se olvidan dichas identificaciones o incluso las bases de datos pueden verse alteradas o robadas por personas no autorizadas.

La principal desventajas de la aplicación de personal de guardia es que éste puede llegar a ser sobornado por un tercero para lograr el acceso a sectores donde no esté habilitado, como así también para poder ingresar o salir de la empresa con materiales no autorizados. Esta situación de soborno puede ocurrir frecuentemente, por lo que es recomendable la utilización de sistemas biométricos para el control de acceso.

Soluciones de seguridad física para evitar posibles robos, como son:

- Armarios de seguridad con llave, para sistemas informáticos.
- Cables de seguridad para portátiles.
- Llaves y candados para equipos y periféricos.

Sistemas Biométricos.

La biometría es una tecnología que se realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. La forma de identificación consiste en la comparación de

características físicas de cada persona con un patrón conocido y almacenado en una base de datos. Los lectores biométricos identifican a la persona por lo que es (manos, ojos, huellas, digitales y voz).

Beneficios de una tecnología Biométrica:

- Pueden eliminar la necesidad de poseer una tarjeta para acceder, y de una contraseña difícil de recordar o que finalmente acaba siendo escrita en un papel visible por cualquier persona.
- Utilizando un dispositivo biométrico los costos de administración son más pequeños, se realiza el mantenimiento del lector, y una persona se encarga de mantener la base de datos actualizada. Sumado a esto, las características biométricos de una persona son intransferibles a otra.

Las Cámaras IP: son dispositivos autónomos que cuentan con un servidor web de video que permite transmitir imágenes a través de redes IP como redes LAN, WAM e Internet. Permiten al usuario tener la cámara en una localización y ver el video en tiempo real desde otro lugar a través del internet.

1.2.1.2 Condiciones Ambientales para la seguridad física.

Son las tempestades, tormentas, catástrofes, incendios, inundaciones y terremotos se asocian a ciertas partes del mundo y la probabilidad de que ocurran.

Incendios.

Los incendios son causados por el uso inadecuado de combustible, fallo de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad de los equipos electrónicos ya que pueden destruir fácilmente los archivos de información y programas.

Factores para reducir los riesgos de incendio a los que se encuentra sometido un centro de procesamiento de datos son:

- El área en la que se encuentran las computadoras debe estar en un área donde no exista combustible.
- El local donde debe situarse no debe estar adyacente áreas donde procesen explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben ser materiales incombustibles y extenderse desde el suelo al techo.
- Se debe construir un suelo falso con materiales, incombustibles y resistente al fuego.
- No se debe permitir el fumar en el área.
- El suelo y el techo son impermeables.
- Deben instalarse extintores manuales.

Sistema de aire acondicionado.

Se debe tener un sistema de ventilación y aire acondicionado separado, y que se encargue del enfriamiento de los equipos.

Inundaciones.

La invasión de agua por exceso de escurrimiento superficial o por acumulación en terrenos planos, ocasionadas por falta de drenaje es un desastre para el sistema de informática red.

Factor para reducir el inconveniente por inundaciones es construir un techo impermeable y acondicionar las puertas para contener el agua.

Terremotos.

Fenómeno sísmico pueden ser intensos como suaves estos ocurren si previo aviso.

Sistema de Alimentación ininterrumpida.

Trabajar con computadoras implica trabajar con electricidad para esto se debe utilizar un dispositivo que gracias a sus baterías puede proporcionar energía tras un apagón a todos los dispositivos que tenga conectado durante un tiempo limitado.

Evaluar y controlar permanentemente la seguridad física del área de los dispositivos informáticos y de la red es la base para comenzar a integrar la seguridad como una función primordial dentro del organismo.

1.2.2 Seguridad Lógica.

Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a personas autorizadas.

- Restringir el acceso al sistema operativo programas y archivos.
- Asegurar que los usuarios puedan trabajar sin una supervisión minuciosa y que no puedan modificar los programas ni archivos.
- Asegurar que se esté utilizando los datos, archivos y programas correctos.

1.2.2.1 Identificación y Autenticación.

Se denomina identificación al momento en que el usuario se da a conocer en el sistema.

Autenticación a la verificación que realiza el sistema sobre esta identificación.

Técnicas que permiten realizar la autenticación de la identidad del usuario.

- Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso , una clave criptográfica, un numero de identificación personal.
- Algo que la persona posee : por ejemplo una tarjeta magnética .

- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.

- Algo que el individuo es capaz de hacer, por ejemplo los patrones de escritura.

Limitaciones a los servicios.

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o prestablecidos por el administrador del sistema.

Modalidad de acceso.

Se refiere al modo de acceso que se permite al usuario sobre los recursos y la información.

- Lectura: El usuario puede únicamente leer o visualizar la información pero no puede alterarla.

- Escritura: Permite agregar datos modificar, borrar información

- Ejecución: Este acceso otorga al usuario el privilegio de ejecutar programas.

- Borrado: Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos).

Administración.

Es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimiento, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

Es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones mas criticas.” (Santos, 2010)

1.2.2.2 Actualización de sistemas y aplicaciones.

Mientras hacemos uso del Internet y sus servicios, los ciberdelincuentes desarrollan virus y otros programas maliciosos para aprovechar cualquier vulnerabilidad en el sistema a través del cual infectarlo es de vital importancia actualizar los sistemas, tanto el sistema operativo como el resto de aplicaciones, tan pronto como sea posible. Se recomienda activar las actualizaciones automáticas de las aplicaciones mas utilizadas sistema operativo, navegadores, programas, reproductores multimedia.

Justificación de la actualización del software:

Reparar las vulnerabilidades detectadas

Proporcionar nuevas funcionalidades.

Descarga de la página web del fabricante del programa los ficheros necesarios.

1.2.3 Seguridad informática de Redes.

La seguridad informática indica el índice en que el sistema informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir (según los especialistas es imposible) en un 100 % por lo que solo se habla de fiabilidad y se la define como “la probabilidad de que un sistema se comporte tal y como se espera de él.” (HUERTA Antonio Villalón.”Seguridad Unix Redes”. Versión 1.2 Digital – Open Publication Licence v.10) "figura 1.6" (http://3ronatmanda.blogspot.com/2008/03/criptografa.html)

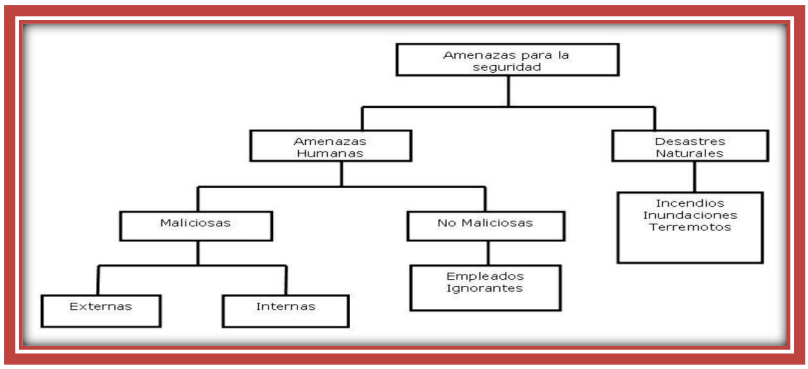


Figura 1.1 Amenazas para la seguridad.

1.2.3.1 Amenazas para la Seguridad.

Se tiene tres tiempos en la que las amenazas pueden ser analizadas: antes, durante y después del ataque estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático evitando ataques y pérdidas de la información.

- La Prevención (antes): Mecanismos que aumentan la seguridad de un sistema durante su funcionamiento por ejemplo el cifrado de información para su posterior transmisión.
- La Detección (Durante): Mecanismos orientados a revelar violaciones a la seguridad generalmente son programas de auditoría.
- La recuperación (Después): Mecanismos que se aplican cuando la violación del sistema ya se ha detectado, para retornar este a su funcionamiento normal por ejemplo la recuperación desde las copias de *Backups* realizadas.

1.2.3.1.1 Clasificación de los Ataques

Los ataques se pueden clasificar en dos pasivos y activos.

Ataques pasivos: El intruso no altera la información solo escucha o monitoriza para saber qué información se está transmitiendo y analizar el tráfico con esto se obtiene:

- El origen y destino de la comunicación con la lectura de las cabeceras de los paquetes.
- Control de tráfico entre entidades monitorizadas para tener información de operatividad o inoperatividad inusual.
- Saber y controlar las horas habituales de intercambio de información.

Ataques activos: Implican la modificación del flujo de datos transmitidos o la creación de datos falsos. Esto es realizado por Hackers, piratas informáticos, o intrusos que lucran por su trabajo.

Y estos ataques se dividen en las siguientes categorías:

- Transmisión Normal: Cuando la transmisión de datos que se envía no sufre ningún percance en el trayecto y llega a su destino.

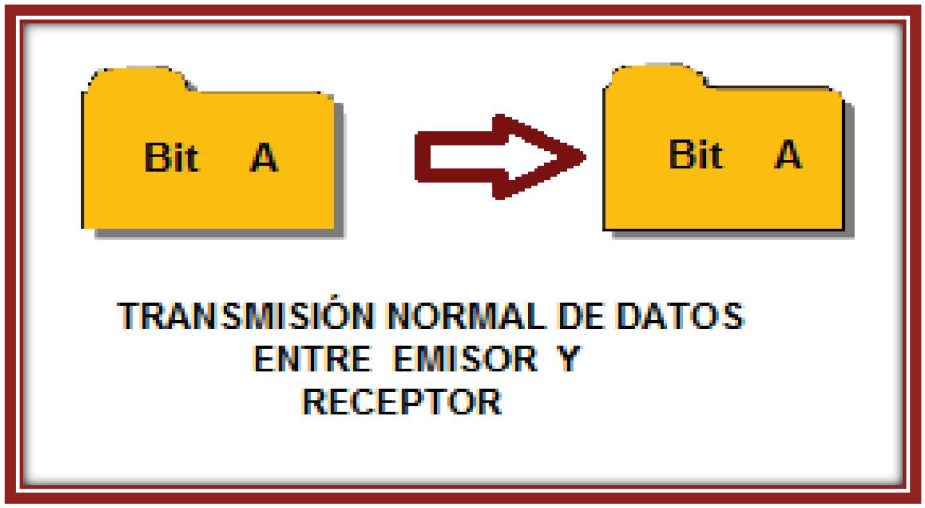


Fig.1.2 Ataques transmisión normal de datos.

Autor: Johanna S. Chicaiza Pineida. 03/02/2012

- Interrupción: Cuando hace que un objeto del sistema se pierda y este se vuelva inutilizable.

Fig.1.3 Ataques Interrupción

Autor: Johanna S. Chicaiza Pineida. 03/02/2012

- Intercepción: Cuando un elemento no autorizado consigue los permisos necesarios y se infiltra en el sistema.

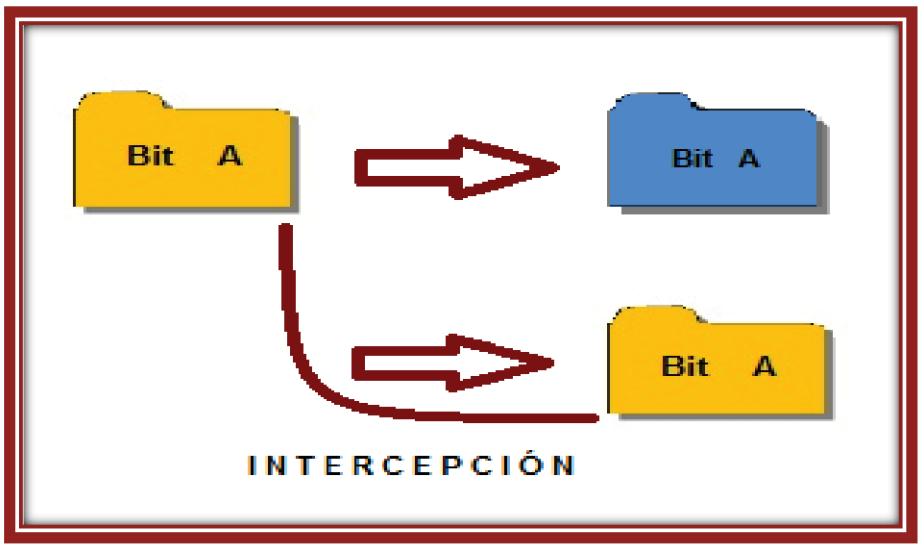


Fig.1.4 Ataques Intercepción.

Autor: Johanna S. Chicaiza Pineida. 03/02/2012

- Modificación: Cuando consigue los permisos necesarios y modifica parte del sistema.

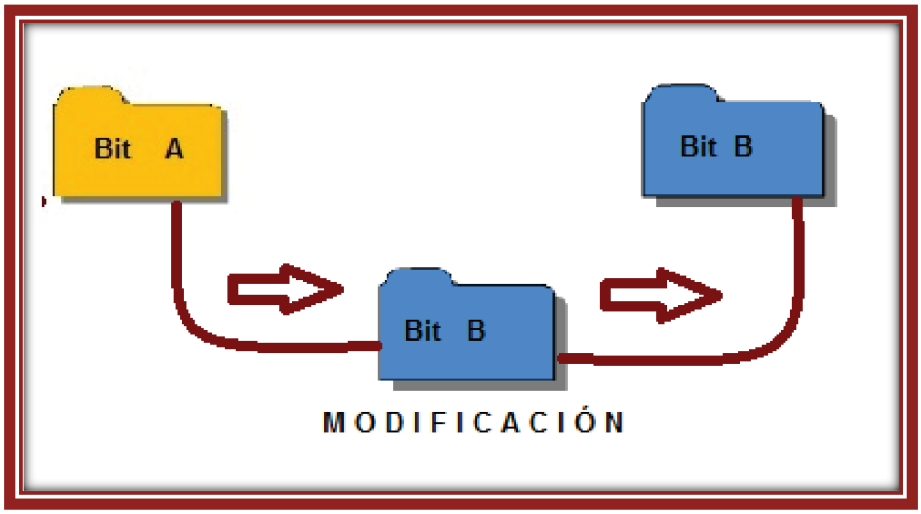


Fig.1.5 Ataques Modificación.

Autor: Johanna S. Chicaiza Pineida. 03/02/2012

- Fabricación: Se tiene un objeto similar al original atacando y es muy difícil distinguir al verdadero.

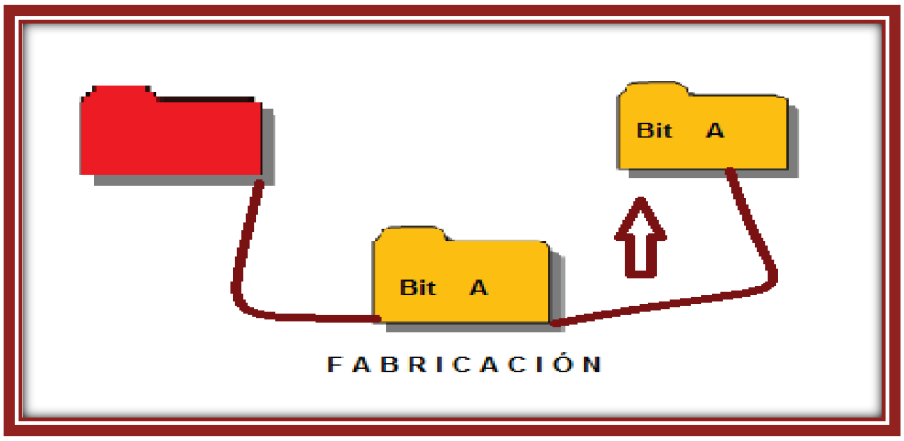


Fig.1.6 Ataques Fabricación.

Autor: Johanna S. Chicaiza Pineida. 03/02/2012

- Destrucción: Cuando se inutiliza a todo el sistema.

Fig.1.7 Ataques Destrucción.

Autor: Johanna S. Chicaiza Pineida. 03/02/2012

1.2.3.2 Contraseñas.

Las contraseñas son métodos de seguridad que poseen una cadena de caracteres alfanuméricos para verificar la identidad de los usuarios. Pero también existen las frases de contraseñas que son de mayor longitud y contienen diversas palabras.

En la actualidad muchas personas tienen varias contraseñas o frases de contraseñas sobre todo si utilizan el Internet o poseen cuentas de correo electrónico, realiza transacciones bancarias utilizan acceso restringido.

Las contraseñas pueden ser el punto más vulnerable de un sistema y el que tiene más probabilidades de ser atacado. Los sistemas corporativos de empresas de mayor envergadura deben auditar la seguridad de su sistema o red.

Para la creación de una contraseña segura se deben plantear las necesidades de protección del sistema o red. De esa forma obligamos al posible atacante a buscar un rango mayor de caracteres.

Las contraseñas o frases de contraseñas deben ser seguras y difíciles de averiguar o vulnerar, por lo que es recomendable que todas las cuentas de usuario del equipo tenga una.

Una contraseña se considera segura cuando:

- Hay 12 caracteres mínimo.
- No se utiliza el nombre verdadero de usuario o institución.
- No completa la idea de una palabra.
- Trata significativamente de ser diferente de otras comunes.
- Debe contener caracteres alfanuméricos.

Una frase de contraseña se considera segura cuando:

- Existen entre 20 y 30 caracteres de longitud.
- Forma una serie de palabras.

- No contiene frases que se encuentren comúnmente en la literatura o música.
- No contiene palabras que se pueda utilizar en el diccionario.
- Es significativamente diferente de otras comunes.
- No utiliza el nombre verdadero de usuario o institución.

Pero en algunas ocasiones por más que se utilicen todos los caracteres de contraseña o frase de contraseña pueden ser inseguras.

Ejemplo: ***Ecuador4Q!*** completa todos los parámetros necesarios para ser una contraseña segura, pero es insegura porque completa una palabra lo recomendable sería: ***3cuad0r 4 Q!*** de esta manera se remplaza las letras con números y se utiliza espacios. Pero es recomendable que sea más larga.

Contraseñas con código ASCII.

Sistema que asigna valores numéricos a letras signos gramaticales, números o caracteres. Este código se compone de 255 símbolos que no se encuentran en el teclado. Aumenta la cantidad de caracteres disponibles para elegir pero hay que tomar en cuenta que los caracteres sean compatibles con los programas que se utilizan en el equipo.

1.2.3.3 Clave de seguridad para Redes Inalámbricas.

El acceso protegido en una red WI-FI admite usar una frase de contraseña que se transforma en clave y se usa para el cifrado (Forma de mejorar la seguridad de un mensaje realizando codificación del contenido) de manera que solo pueda tener acceso el destinatario que posee la clave para descifrarlo.

El acceso protegido WI-FI (WPA Y WPA2) se asegura de que la clave de seguridad de red no haya sido modificada y autentica a los usuarios para garantizar que solo personas autorizadas puedan tener acceso a la red.

WPA: está diseñada para trabajar con todos los adaptadores de red inalámbricos pero no con Access Point o enrutadores demasiado antiguos.

Puede utilizarse con un servidor de autenticación 802.1x distribuyendo diferentes claves a cada usuario a esto se le denomina WPA-Enterprise.

También existe WAP-Personal en la que se puede usar el modo de clave previamente compartida (PSK) donde cada usuario recibe la misma contraseña.

WPA2: Es más seguro que WPA pero no funciona con adaptadores de red antiguos.

La privacidad equivalente por cable (WEP):

Es un método de seguridad para dispositivos antiguos al habilitarlo se configura una clave que cifra la información que un equipo envía a otro pero no es recomendable ya que es sencillo de vulnerar.

La Autenticación 802.1x mejora la seguridad de redes inalámbricas 802.11 y redes Ethernet se usa un servidor de autenticación para validar a los usuarios y proporcionar acceso a la red, puede funcionar con claves WPA y WPA2.

1.2.3.4 Software Malicioso.

Es cualquier programa que puede ser capaz de infectar a otros resultando peligroso, dañino y dependiendo de cómo actúa en el sistema se lo puede clasificar de la siguiente manera:

"**Virus**: Programas que se introducen en los ordenadores de diversas formas, correo, Internet dispositivos de almacenamiento y se caracterizan porque al ejecutarse realizan acciones molestas o incluso dañinas para el usuario.

Gusanos: Son similares a los virus pero su acción se limita a hacerse copias de sí mismo a tal velocidad que colapsan la red.

Troyanos: Estos son también similares a los virus, pero actúan de forma inofensiva pero al ejecutarse se instala lo que se llama una puerta trasera a través de la cual se puede controlar el PC infectado.

Backdoors: Este malware también se basa en la confianza del usuario, siendo inofensivo al principio pero al ejecutarse hace lo mismo que un troyano.

Dialer: Cuelga la conexión telefónica existente y hace una nueva usando un teléfono de tarificación especial, “las líneas hot”.

Phishing: Consisten en el envío de correos electrónicos que parecen provenir de contactos fiables que intentan conseguir información confidencial de la víctima como por ejemplo números de cuentas bancarias, contraseñas, tarjetas de crédito, etc.

Vulnerabilidad: Se trata de un fallo en la programación de una aplicación a través del cual se puede vencer la seguridad de nuestra maquina.

Spyware: Estos programas recogen datos de hábitos del uso de Internet de los usuarios y los envía a empresas de publicidad con el consentimiento de los usuarios.

Adware: Se trata de un software que muestra publicidad de cualquier tipo sin el consentimiento del usuario.

Hoax: Son mensajes de correo electrónico con advertencias sobre falsos virus que se difunden masivamente por Internet sembrando el pánico.

Joke: Son programas inofensivos que simulan el comportamiento de un virus. Su único objetivo es gastar una broma.

Los rootkits: Son programas malintencionados que conceden a los atacantes de Internet un acceso ilimitado a un sistema, al tiempo que ocultan su presencia. Una vez que han accedido al sistema explotando alguna vulnerabilidad, usan funciones del propio sistema operativo para evitar su detección por parte del antivirus: ocultan procesos, archivos y datos de registro de Windows. Por ello, es casi imposible detectarlos con las técnicas de detección normales.

Spam: Se trata del envío indiscriminado de mensajes de correo no solicitados, generalmente publicitarios."
(http://www.redesyseguridad.es/clasificacion-del-software-malicioso/)

1.2.3.5 Antivirus.

Son programas que desarrollan empresas que se dedican a la elaboración de software, detecta y elimina inteligentemente la mayoría de los virus de un disco infectado sin intervención del usuario. Dándole protección a su equipo contra el código malicioso. Pero hay que tener en cuenta que un antivirus debe estar bien configurado, para su correcto funcionamiento y que no se puede decir que se tiene una protección definitiva al 100%.

Los antivirus tienen tres importantes funciones detectar vacunar y eliminar.

• Detectar: Examina los archivos que están dentro del disco duro que tiene un control y codificación para detectar los códigos maliciosos que permitan capturarlos.

• Vacuna: Es un programa que se encarga de remediar los daños provocados por programas maliciosos, escaneando el disco duro en busca de virus que pueden encontrarse en el ordenador, y cuando lo localiza trata de eliminarlo o ponerlo en cuarentena.

• Eliminar: Cuando se logra capturar al código malicioso y eliminarlo.

1.2.4 Cableado Estructurado.

Es el cableado que se puede hacer en una oficina, en uno o varios edificios en los que se puede interconectar equipos activos de diferente o igual tecnología integrando servicios que dependen del tendido de cables como datos y telefonía.

“El concepto estructurado lo definen los siguientes puntos:

• **Solución Segura:** El cableado se encuentra instalado de tal manera que los usuarios del mismo tienen la facilidad de acceso a lo que deben de tener y el resto del cableado se encuentra perfectamente protegido.

• **Solución Longeva:** Cuando se instala un cableado estructurado se convierte en parte del edificio, así como lo es la instalación eléctrica, por tanto este tiene que ser igual de funcional que los demás servicios del edificio. La gran mayoría de los cableados estructurados pueden dar servicio por un periodo de hasta 20 años, sin importar los avances tecnológicos.

• **Modularidad:** Fácil capacidad de integrar varias tecnologías sobre el mismo cableado voz, datos, video. Fácil administración: El cableado estructurado se divide en partes manejables que permiten hacerlo confiable y perfectamente administrable, pudiendo así detectar fallas y repararlas fácilmente"

(http://www.consultec.es/sistemas/pdf/cableado_estructurado.pdf)

1.2.4.1 Categorías.

"Figura.1.13" (http://www.consultec.es/sistemas/pdf/cableado_estructurado.pdf)

Categoría	Topologías soportadas	Velocidad Max. De Transferencia	Distancias máximas entre repetidores	Requerimientos de materiales posibles a utilizar	Status
Cat. 3	Voz Arcnet – 2 Mbits. Ethernet -10 Mbits.	10Mbits	100 metros.	Cable y conectores coaxiales o cable y conectores UTP de menos de 100 Mhz.	Obsoleto
Cat.5	Inferiores y Fast Ethernet	100 Mbits	90 Mts. + 10 En patchcords	Cable UTP y conectores Categoria 5 de 100 – 150 Mhz.	Obsoleto
Cat.5e	Inferiores y ATM	165 Mbits	90 Mts. + 10 mts. En patch cords.	Cable UTP/FTP y conectores Categoria 5e de 150 – 350 Mhz.	Obsoleto
Cat.6	Inferiores y Gigabit Ethernet	1000 M bits.	90 Mts. + 10 mts.En patchcords.Con cable de cobre Cat.6 1 Km. En fibra multimodo 2 Km. En fibra monomodo	Cable de cobre y conectores Categoria6 y fibra Óptica	Actual
Cat.7	Desempeño a 10Gb/s y más, excediendo todos los requisitos de desempeño para 10GBASE-T.	1 Gbps.	Comutador mecánico Entre pares superiores e inferiores.	Especifica una gama de frecuencias de 1 a 600 Mhz. Conector GG45	Su desempeño a prueba de futuro y su flexibilidad hacen que TERA sea ideal para data centers, imágenes médicas y aplicaciones financieras.

Figura 1.8 Categorías de cable UTP.

1.2.4.2 Partes que integran un cableado estructurado.

“Área de trabajo: Su nombre lo dice todo, es el lugar donde se encuentran el personal trabajando con las computadoras, impresoras, etc. En este lugar se instalan los servicios (nodos de datos, telefonía, energía eléctrica, etc.) Closet de comunicaciones. Es el punto donde se concentran todas las conexiones que se necesitan en el área de trabajo.

Cableado Horizontal: Es aquel que viaja desde el área de trabajo hasta el closet de comunicaciones.

Closet de Equipo: En este cuarto se concentran los servidores de la red, el conmutador telefónico, etc. Este puede ser el mismo espacio físico que el del closet de comunicaciones y de igual forma debe ser de acceso restringido.

Entrada (Acometida): Es el punto donde entran los servicios al edificio y se les realiza una adaptación para unirlos al edificio y hacerlos llegar a los diferentes lugares del edificio en su parte interior. (no necesariamente tienen que ser datos pueden ser las líneas telefónicas, o Back Bone que venga de otro edificio, etc.

Cableado Vertical (Back Bone): Es el medio físico que une 2 redes entre sí.”

(http://www.consultec.es/sistemas/pdf/cableado_estructurado.pdf)

1.2.4.3 Etiquetado.

“La norma EIA/TIA-606 especifica que cada terminación de hardware debe tener alguna etiqueta que lo identifique de manera exclusiva. Un cable tiene dos terminadores, por tanto, cada uno de estos extremos recibirá un nombre.

No es recomendable la utilización de un sistema de etiquetado con relación a un momento concreto, es mejor, utilizar nomenclaturas neutras. Por ejemplo, si etiquetamos un PC como <<PC de Dirección>>, y luego cambia el lugar del

edificio en donde se ubica la Dirección, habría que cambiar también el etiquetado, sin embargo, se trata de que el etiquetado sea fijo.

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. Por ejemplo, se podría etiquetar un cable con el siguiente identificador:

03RS02-05RS24

Este cable indicaría que está tendido desde la roseta (RS) número 02 de la sala 03 hasta la roseta 24 de la sala 05. Las rosetas en las salas 03 y 05 irían etiquetadas con 03RS02 y 05RS24 respectivamente."

(http://www.mailxmail.com/curso-redes-area-local/etiquetado-cables-cableado-estructurado)

1.2.5 Router y Switch.

El Router es un dispositivo de interconexión de redes opera en la capa red del modelo OSI. Toma decisiones lógicas con respecto a cuál es el camino o ruta más adecuada para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y puerto de salida adecuados. Se basa en diversos parámetros y protocolos para comunicarse entre si y compartir información.

El Switch o conmutador es un dispositivo de interconexión de redes de ordenadores, opera en la capa enlace del modelo OSI. Interconecta dos o más segmentos de red. Funciona de forma similar a los Bridge o puentes pasando datos de una red a otra de acuerdo con la dirección MAC de destino de los datagramas en la red.

1.2.5.1 Cuadro Comparativo Switch y Router.

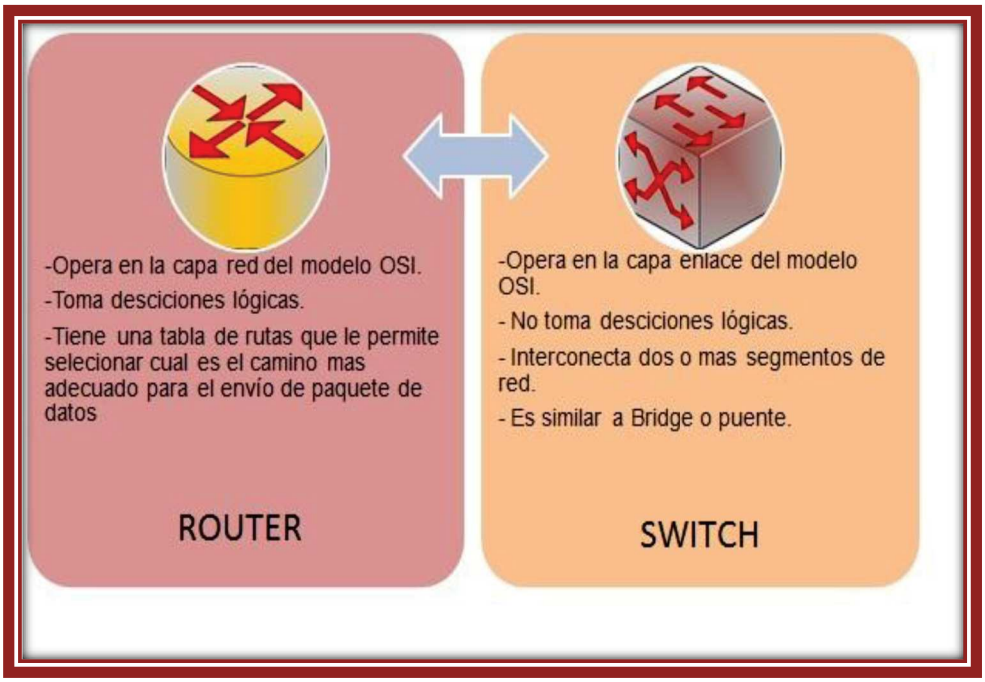


Fig.1.9 Cuadro comparativo del Router y Switch

Autor: Johanna S. Chicaiza Pineida. 08/04/2012

1.2.6 Firewall y Servidores de Red.

1.2.6.1 Firewall.

Un firewall es un sistema que protege a un ordenador o a una red de ordenadores, contra posibles ataques que provienen del Internet, permite denegar o permitir tráfico entre dos redes en función de las reglas que se establecen.

El firewall ayuda a impedir que personas mal intencionadas o software malicioso puedan tener acceso a un equipo de la red de la organización o empresa mediante el Internet .También puede impedir que el equipo envié software malicioso a otros.

Es un filtro que controla todas las comunicaciones que pasan de una red a otra, las políticas que se pueden implementar, permiten o deniegan el tráfico, examina el tipo de servicio al que corresponde y decide si lo pasa o no.

Con el firewall de Windows se puede limitar algunos servicios.

"Figura 1.15" (http://yordanisp.blog.com.es)

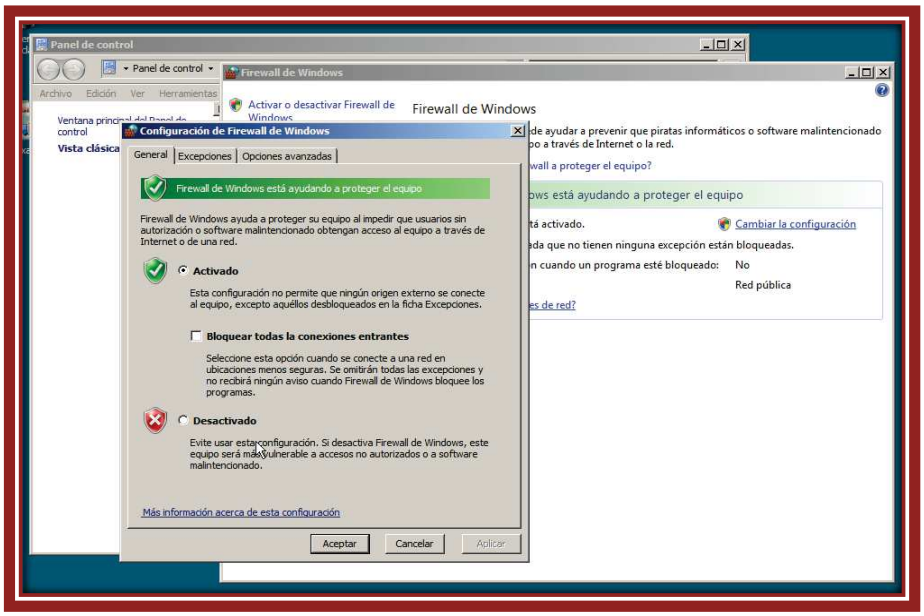


Figura.1.10 Firewall de Windows.

1.2.6.2 Servidor Correo.

Es una aplicación que permite enviar correos de unos usuarios a otros, utiliza un software especial, usa protocolos estandarizados tanto en el envío de imágenes, archivos adjuntos, existen dos clases de servidor de correo público y privado.

Un cliente de correo: permite al usuario enviar y recibir correo electrónico mediante la comunicación con los servidores. Cuando se envía un correo electrónico el *ISP* (Proveedor de Servicio Internet) para pasar su mensaje utiliza el protocolo *SMTP* (*SEND MAIL TRANSFER PROTOCO*L). Las

cabeceras de información no son visibles para el cliente de correo, sin embargo están incluidos en todos los correos.

El mensaje de correo se envía junto a la dirección y este a su vez atravesará varios Router y el mensaje llegará a su destino, cuando el servidor de correo electrónico receptor, tiene el correo lo almacena en un buzón virtual y el correo se queda ahí hasta que el destinatario vuelva utilizar su cliente de correo. El servidor de correo que reciben se llama *POP3* (*POST OFFICE PROTOCOL 3*).

1.2.6.3 Servidor DHCP.

DHCP (DYNAMIC HOST CONFIGURACTION PROTOCOL) protocolo de configuración dinámica de servidores permite a los dispositivos, obtener su propia información de configuración de red es decir asigna direcciones IP automáticamente también asigna DNS, Gateway o puerta de enlace y servidor de dominio. Esto permite administrar fácilmente redes grandes, caso contrario se tendría que configurar manualmente los host de cada usuario que pertenecen a la red local.

Existen tres formas de asignar el protocolo DHCP:

• Manual: Utiliza una tabla con direcciones MAC (MEDIA ACCESS CONTROL ADDRESS) dirección de control de acceso al medio. Solo anfitriones con una dirección MAC definida en dicha tabla recibirá la IP asignada en la misma tabla.

• Automática: Las IP´S disponibles se encuentran dentro de un rango determinado se asignan permanentemente al que lo requiera.

• Dinámica: Arbitrariamente se determina un rango de direcciones IP y cada anfitrión conectado a la red, está configurada para solicitar su IP al servidor. La asignación de direcciones IP son temporales y se reutilizan dinámicamente.

1.2.6.4 Servidor Proxy.

Un servidor proxy es un equipo intermediario situado entre el sistema del usuario y el Internet se utiliza para registrar el uso de Internet, bloquear el acceso a ciertas páginas. Funciona como cortafuegos y desactiva el acceso o filtra las solicitudes de contenidos a ciertas páginas.

Mejora el rendimiento y la velocidad de acceso guarda en la memoria caché las páginas web a las que accede los sistemas de la red 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 haciendo más rápido el ingreso a la página.

1.2.7 Metodología.

Para el presente proyecto utilizaremos la investigación descriptiva e investigativa.

“El objetivo de la investigación descriptiva consiste en llegar a conocer las situaciones, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables. Los investigadores no son meros tabuladores, sino que recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.”

(http://noemagico.blogia.com/2006/091301-la-investigacion-descriptiva.php)

“Nivel de la Investigación: El nivel de una investigación viene dado por el grado de profundidad y alcance que se pretende con la misma.

Así tenemos que una Investigación puede ser:

• Exploratoria: Cuando no existe un cuerpo teórico abundante que ilumine el estudio sobre el fenómeno observado y los resultados que se obtengan sean un aporte al reconocimiento de los elementos que lo integran.

• Descriptiva: Cuando se señala cómo es y cómo se manifiesta un fenómeno o evento, cuando se busca especificar las propiedades importantes para medir y evaluar aspectos, dimensiones o componentes del fenómeno a estudiar.

• Correlacional: Cuando se pretende hacer ver o determinar el grado de relación que pueden tener dos o más variables en una investigación.

• Explicativa: Está dirigida a responder a las causas de los eventos físicos o sociales y su interés se centra en explicar por qué y en qué condiciones ocurre un fenómeno, o por qué dos o más variables se relacionan.”

(http://www.monografias.com/trabajos89/conceptos-basicos-metodologia-investigacion/conceptos-basicos-metodologia-investigacion.shtml)

2. Capítulo II Levantamiento de la Información del proyecto.

2.1 Elaboración del plano de la infraestructura de red.

El siguiente diagrama está basado en la actual infraestructura que posee la empresa.

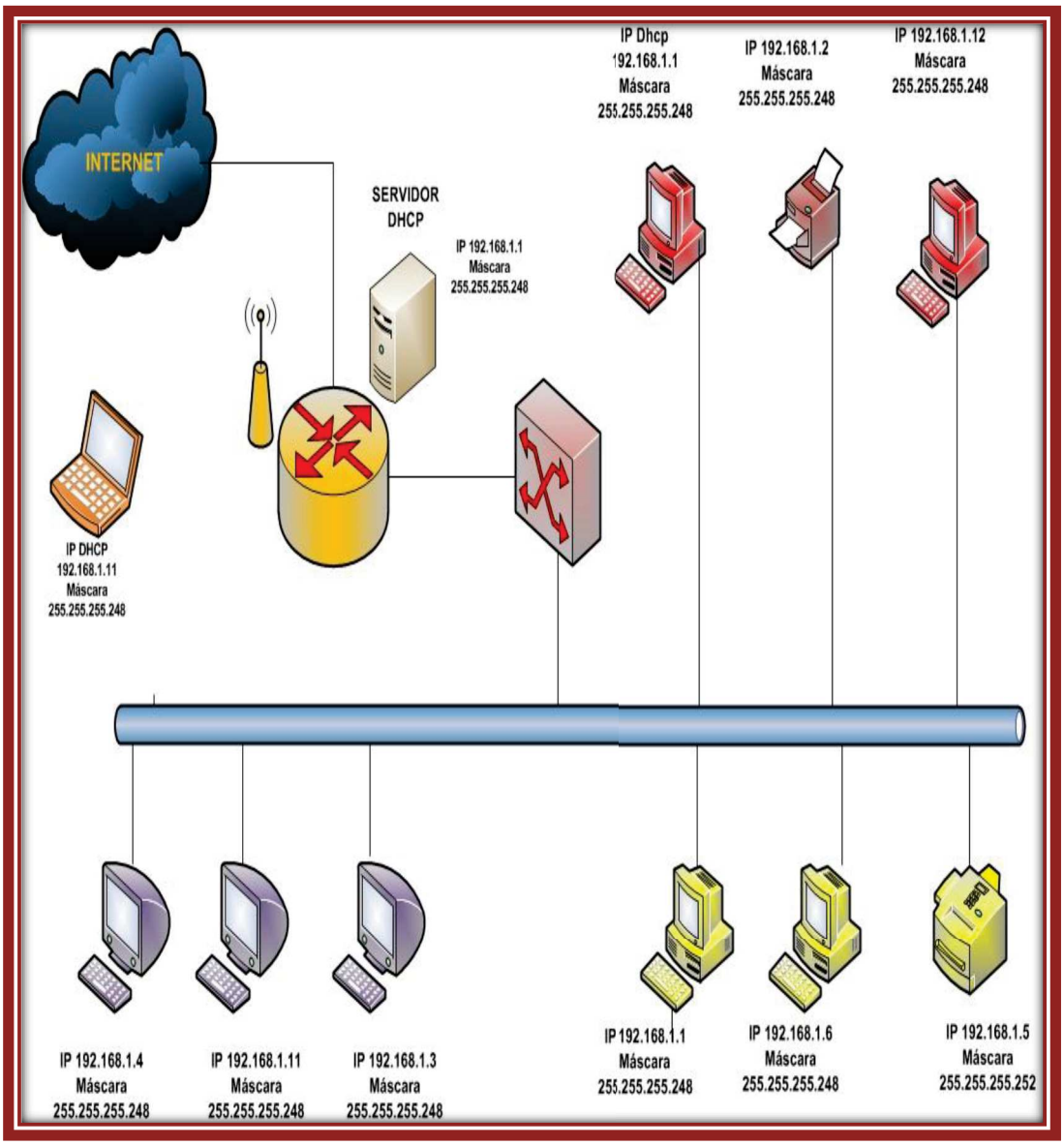


Fig.2.1 Plano de la infraestructura de red actual.

Autor: Johanna S. Chicaiza Pineida. 21/04/2012

2.2 Tipos de Servidores.

La empresa cuenta con un servidor DHCP que se encuentra por defecto en el Router HUAWEI. “Figura.2.2” (http://yordanisp.blog.com.es)

Fig.2.2. Router HUAWEI.

Se cuenta con un servidor de correo electrónico externo Hotmail que le pertenece a Microsoft.

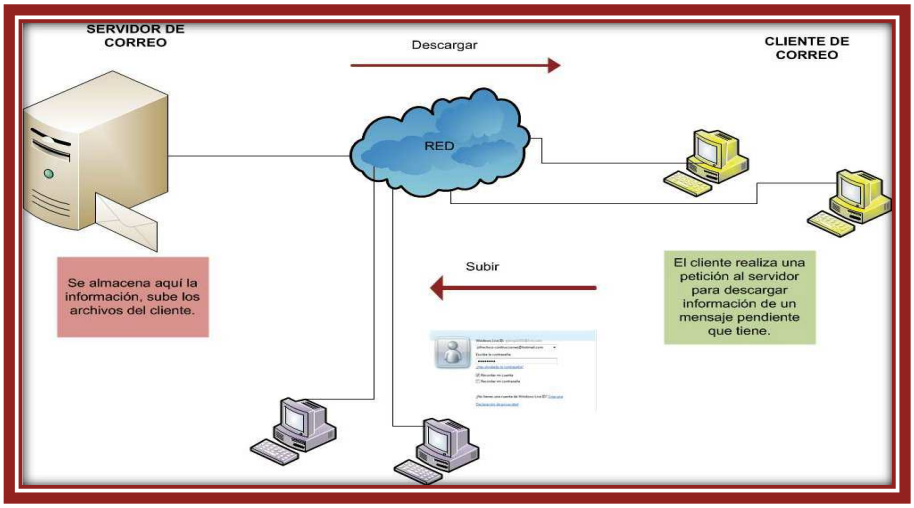


Fig.2.3. Servidor de Correo.2

Autor: Johanna S. Chicaiza Pineida. 21/04/2012

2.3 Infraestructura de la red.

En la siguiente tabla 2.1 se observara los equipos de hardware que se utilizan.

EQUIPOS	CARACTERISTICAS
1 ROUTER HUAWEI HG532c	- 300 Mbps de velocidad de transferencia. - Conexión 3G a través de su puerto USB. - Soporte para cifrado hasta WPA2-AES en WIRELESS. - cuatro puertos Ethernet 10/100 y un puerto RJ11 para la conexión ADSL. - Estabilidad en navegación. - Mejor Latencia. - Buena Cobertura WIFI.
1 SWITCH CISCO SF 100-16	- Posee 16 puertos. - No es administrable es automático. - Trabaja en la capa enlace.
1 PATCH PANEL LEMOV	- Categoría 5E
1RACK	

Tabla 2.1 Equipos y características.

2.4 Equipos Terminales.

EQUIPO	CARACTERISTICAS
1 IMPRESORA HP	- Puerto TCP/IP. - Multifuncional.
1 IMPRESORA XEROX	- Puerto USB. - Puerto TCP/IP.
1 PLOTER HP	- Puerto USB.
1 COMPUTADORAS PORTATILES HP	- Sistema operativo Windows 7 - Procesador core2duo - Memoria RAM de 4G - Soportan WIFI , WIRELESS. - **Programas Instalados:** - Antivirus AVAST Free. - AUTOCAD. - VMWARE maquina virtual. - Adobe Reader. - Ares. - Traductor Global. - OFICCE 2010. - NERO. - MOZILLA FIREFOX - Windows Live Messenger
3 COMPUTADORAS DE ESCRITORIO TOSHIBA	- Sistema operativo Windows XP - Procesador Pentium - Memoria RAM 1G - **Programas Instalados:** - Antivirus AVAST Free - MP3 Down load - AUTOCAD - OFICCE 2007 - Quick Time - MOZILLA FIREFOX - Windows Live Messenger
4 COMPUTADORAS DE ESCRITORIO HP	- Sistema operativo Windows 7 - Procesador Corei3 - **Programas instalados:** - Antivirus ESET Nod32 - AUTOCAD - VMWARE Máquina virtual - Adobe Reader - MOZILLA FIREFOX - Ares - EPSON ESCAN - OFFICE 2007 - Windows Live Messenger

Tabla 2.2 Equipos terminales.

En el siguiente diagrama se observará el porcentaje del sistema operativo que utilizan las máquinas.

Fig.2.4 Porcentaje de utilización del sistema operativo Windows y Windows XP.

Autor: Johanna S. Chicaiza Pineida. 04/08/2012

2.5 Certificación del Cableado.

Se tiene un cableado de red CAT. 5E no cuenta con certificación.

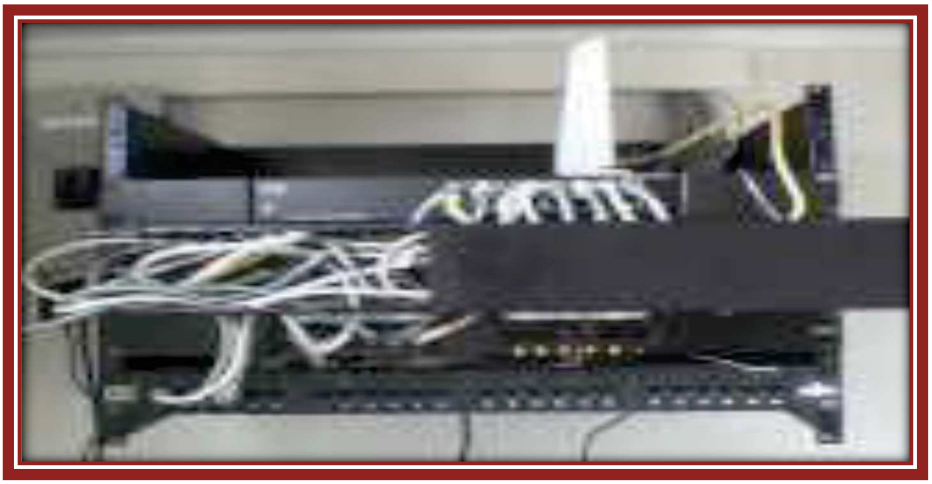


Fig.2.5 Cuarto de equipos de Carolina Construcciones.

Autor: Johanna S. Chicaiza Pineida. 22/05/2012

2.6 Administración de los servicios de la red.

No existe una persona encargada para la administración de la red se utiliza servicios por subcontratación cada vez que se presentan conflictos de red.

2.7 Medidas correctivas y preventivas para la red.

No se realiza un plan para corregir problemas y prevenir desastres que se podrían presentar en el futuro.

2.8 Direccionamiento IP mal configurado.

Existen direcciones IP duplicadas, máscaras de red inadecuadas y direcciones IP mal configuradas.

2.9 Virus y Antivirus.

Existen virus y troyanos en el 57 % de los Hosts y se tienen instalados los Antivirus Avast y EsetNot32 en los ordenadores.

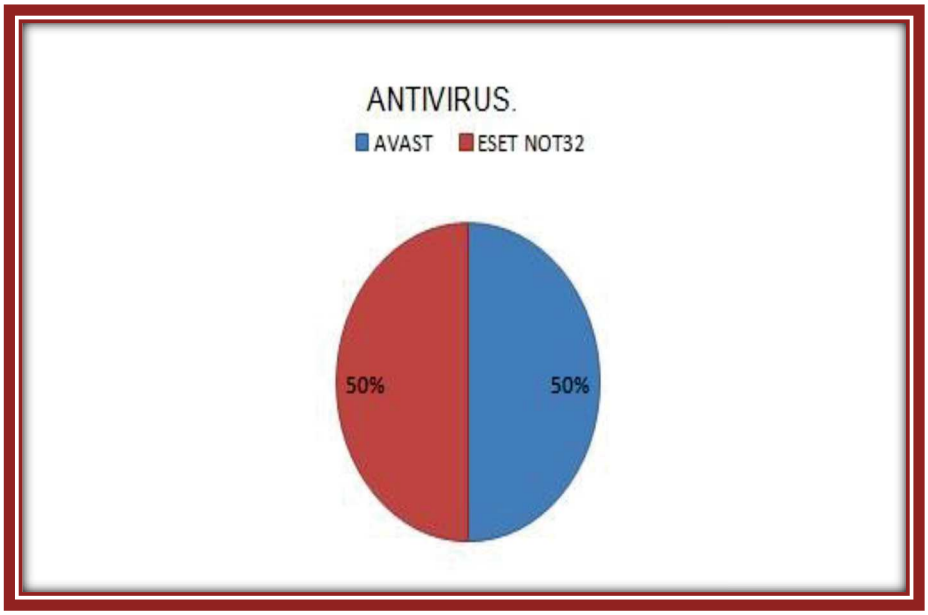


Fig.2.6. Porcentaje de los Antivirus.

Autor: Johanna S. Chicaiza Pineida. 22/05/2012

3. Capítulo III Auditoria de Infraestructura de red.

3.1 Evaluación de Contraseñas en Equipos.

Para realizar la evaluación se ingresará al panel de control, cuentas de usuarios y se verificará si el ordenador tiene cuentas de Administrador y de usuario.

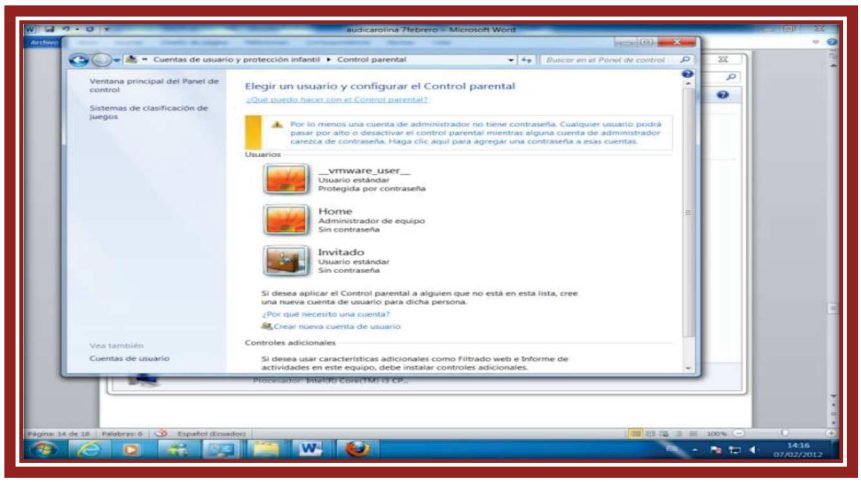


Fig.3.1. Ventana de usuarios y administrador.

Se ingresó a la página http://password.es/comprobador/ para comprobar qué tan robusta es la contraseña, se observó que el nivel de seguridad de la actual contraseña es muy bajo.

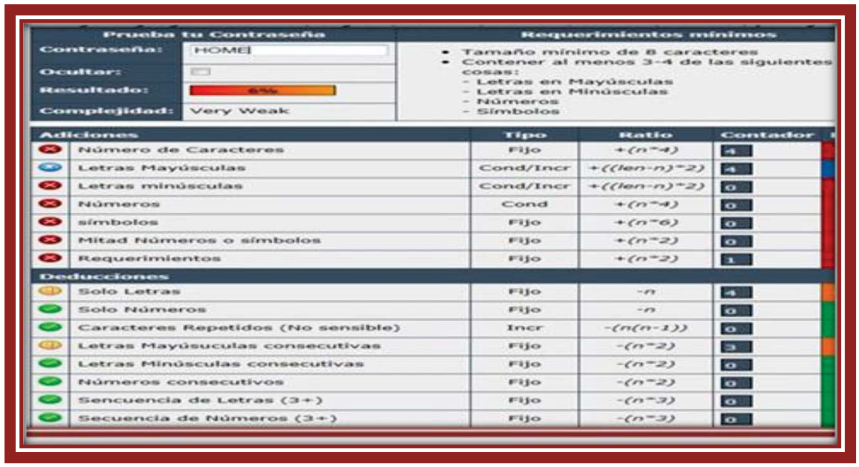


Fig.3.2. Ventana de confiabilidad de contraseñas.

Ahora se utilizará John Riper para verificar si se puede obtener las contraseñas en las estaciones de trabajo. John Riper es un programa de criptografía que rompe algoritmos de cifrado para descubrir contraseñas, permite a los Administradores saber que tan robustas son las contraseñas.

Utiliza un ataque de fuerza bruta por diccionario que va probando todas las combinaciones posibles combinando números, signos, mayúsculas, minúsculas etc.

Este programa se descarga de la siguiente dirección:

http://john-the-ripperv171.hackin9.org/html/hacker-hackin9-29-John-the-Ripper-v171.html

Luego se copiarán los archivos del pwd y John Riper en la unidad de disco C debe tomarse en cuenta que el antivirus debe estar previamente desactivado.

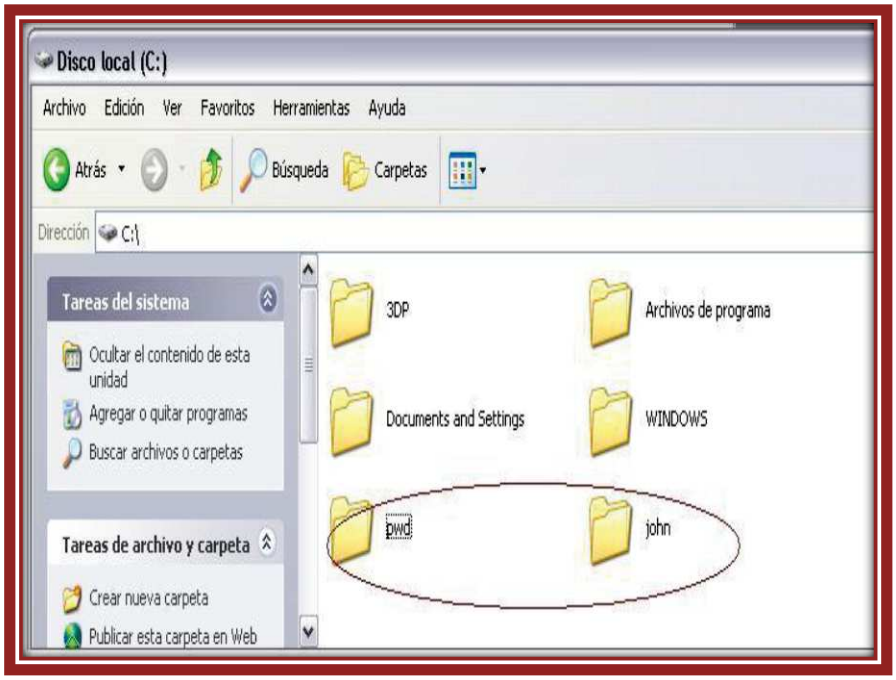


Fig.3.3. Ventana de archivos John Riper y Dump.3

Como se observará la carpeta John Riper y Dump están descomprimidas y contienen los archivos de programa como se muestra en las figuras (3.4 y 3.5)

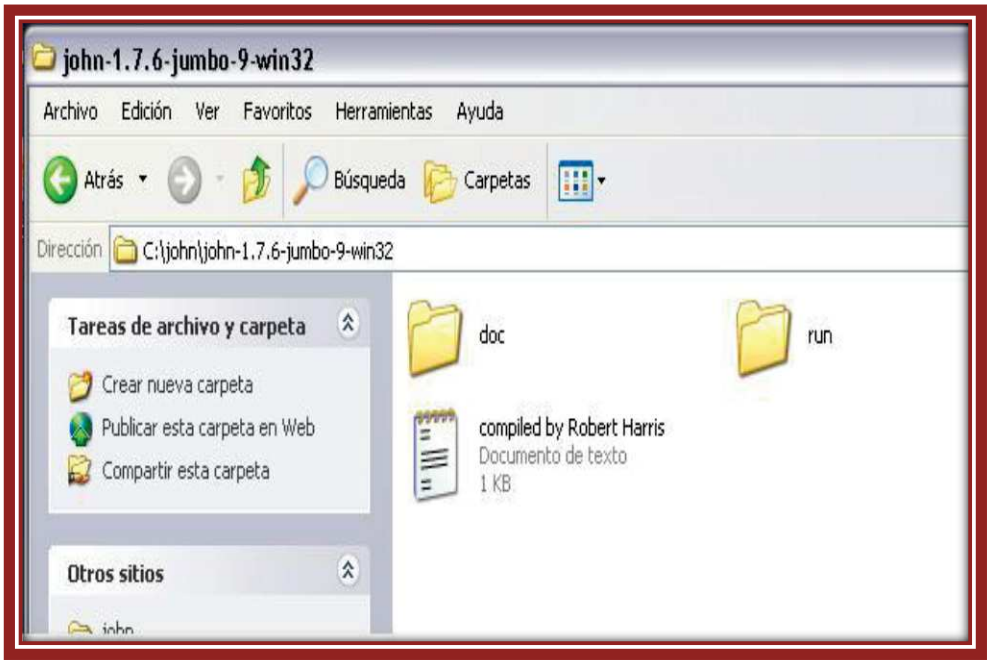


Fig.3.4. Ventana de archivos John Riper.

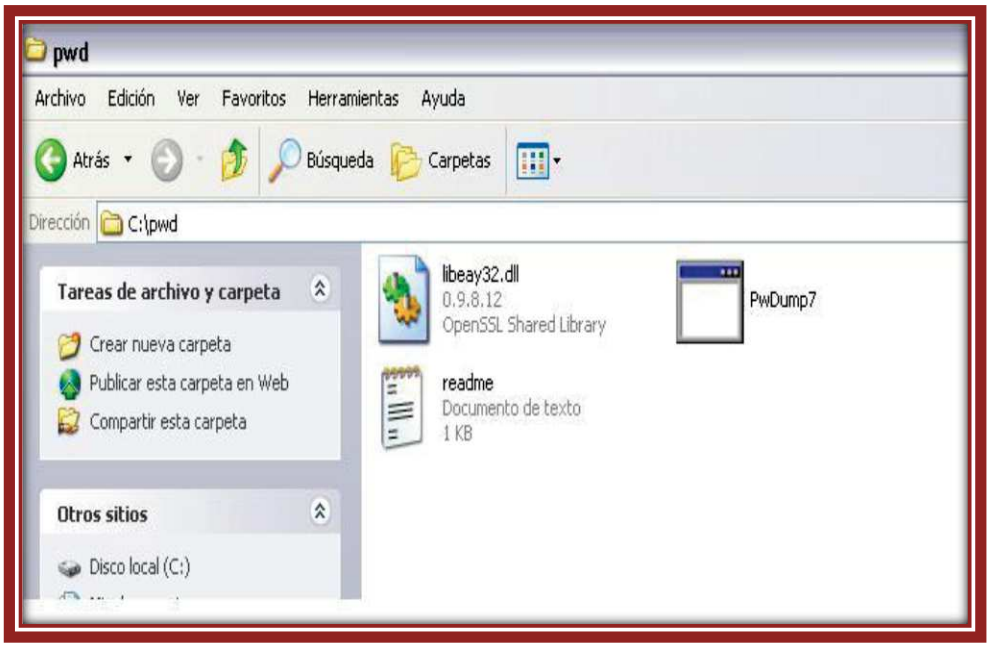


Fig.3.5. Ventana de archivos Dump7

A continuación, utilizando la consola de comandos (cmd), nos ubicaremos en la carpeta del Power Dump (pwd) para ejecutarlo, indicaremos el nombre del archivo y que se guarde el resultado. En el ordenador existen cuentas de usuario y administrador con sus respectivas contraseñas y estas contraseñas son las que el programa descifrará.

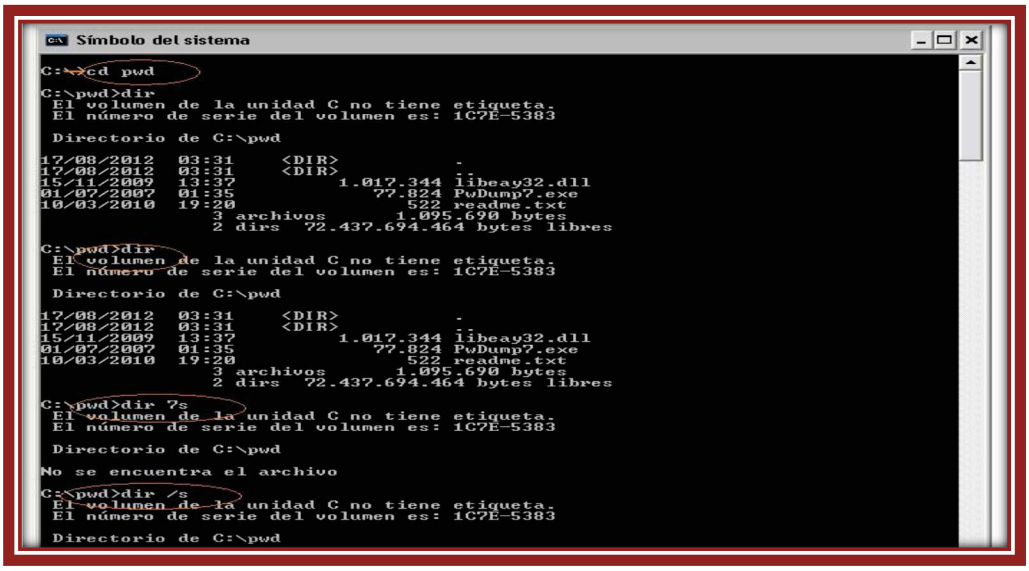


Fig.3.6. Ventana Dump7 directorio.

Luego se copiará los archivos del programa al archivo de mis claves.txt.

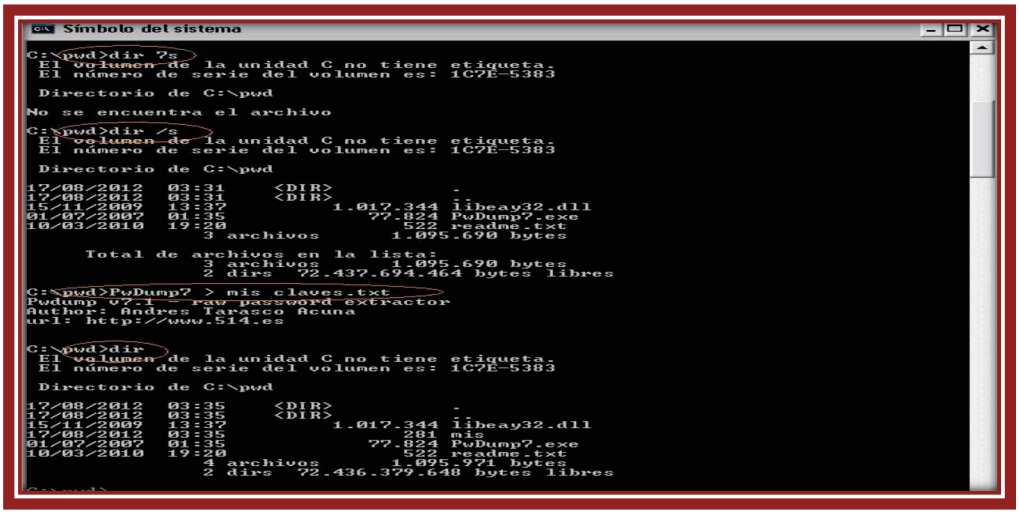


Fig.3.7. Ventana Dump7

Una vez creado el archivo de los resultados se lo puede editar. Por ejemplo se puede ver que la cuenta administrador no tiene contraseña, el usuario secretaria si posee al igual que los usuarios de prueba que se crearon.

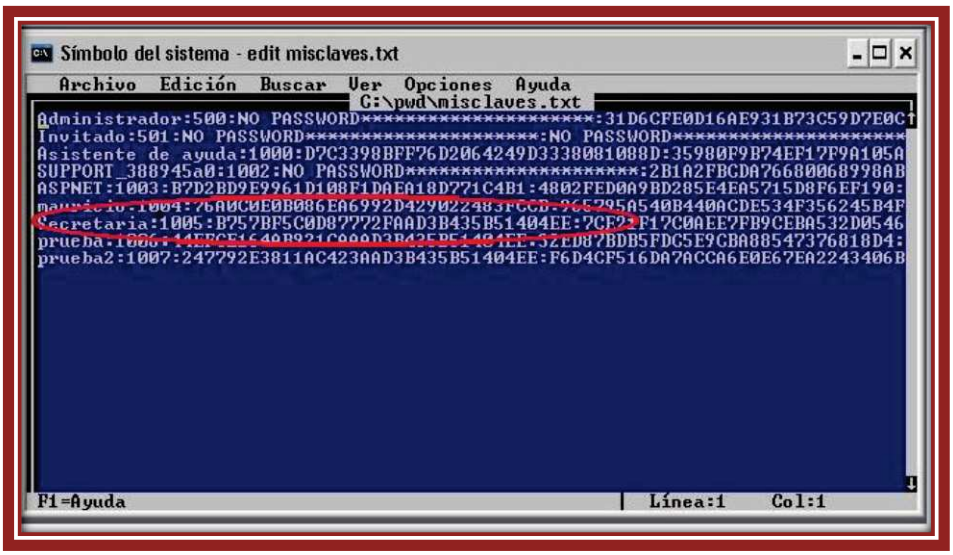


Fig.3.8. Ventana de Dump7 contraseñas.

Saldrá de la ventana azul y se copiará el archivo a la carpeta John Ripper.

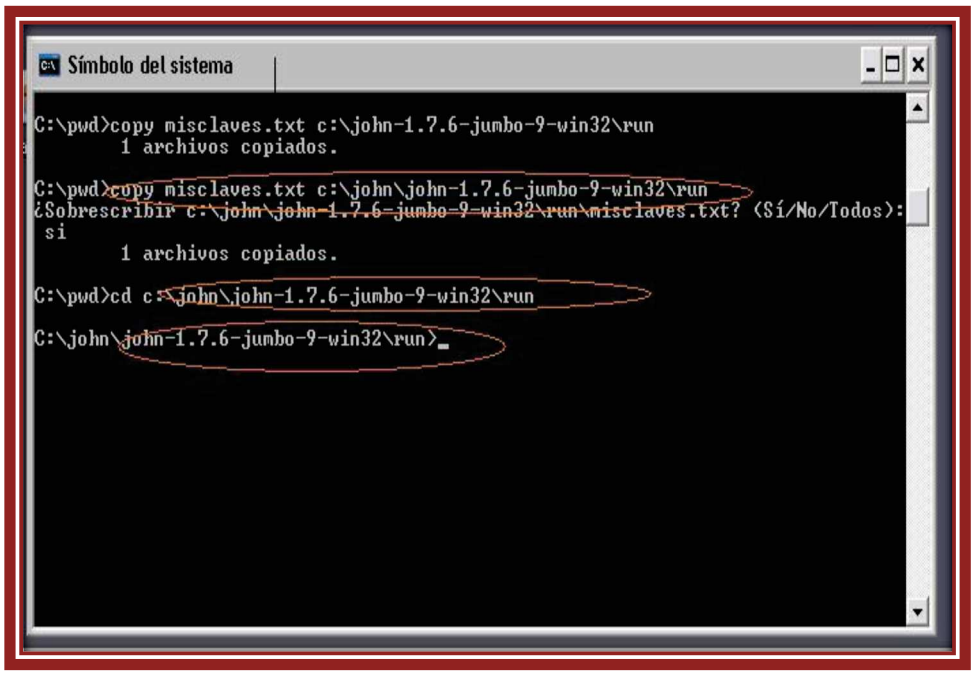


Fig.3.9. Ventana de John Ripper copia del archivo misclaves.txt

Se desplegará el directorio y la ejecución del archivo.

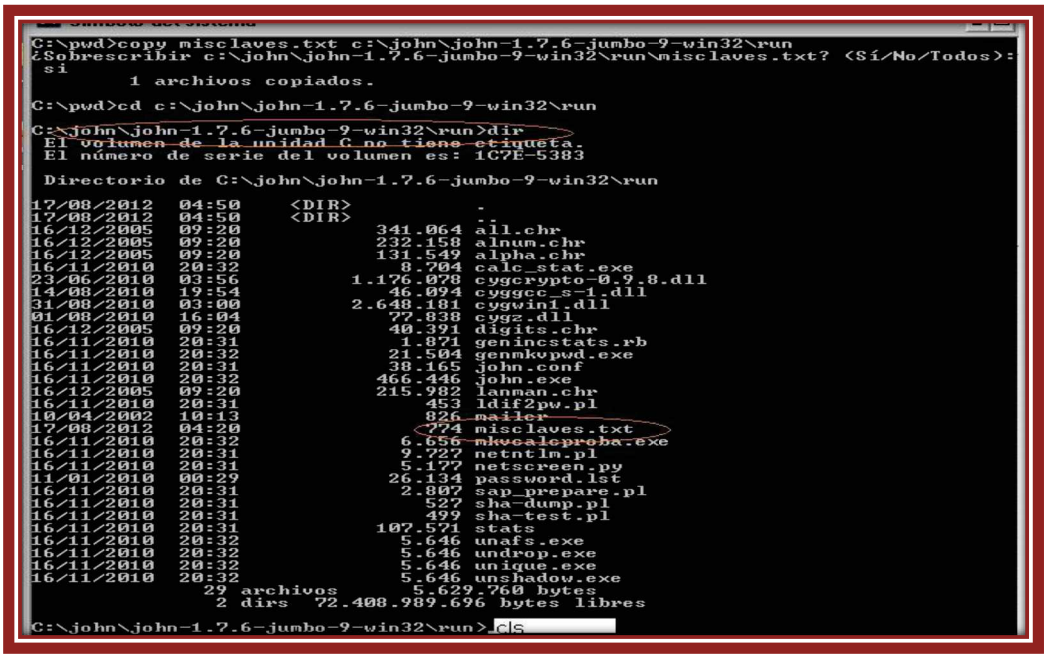


Fig.3.10. Ventana de directorio de John Ripper contraseñas.

Como se puede observar no tomó mucho tiempo el conocer las contraseñas de los usuarios. Dependiendo de qué tan robusta es la contraseña, el programa podría tardar hasta un día en resolverlo.

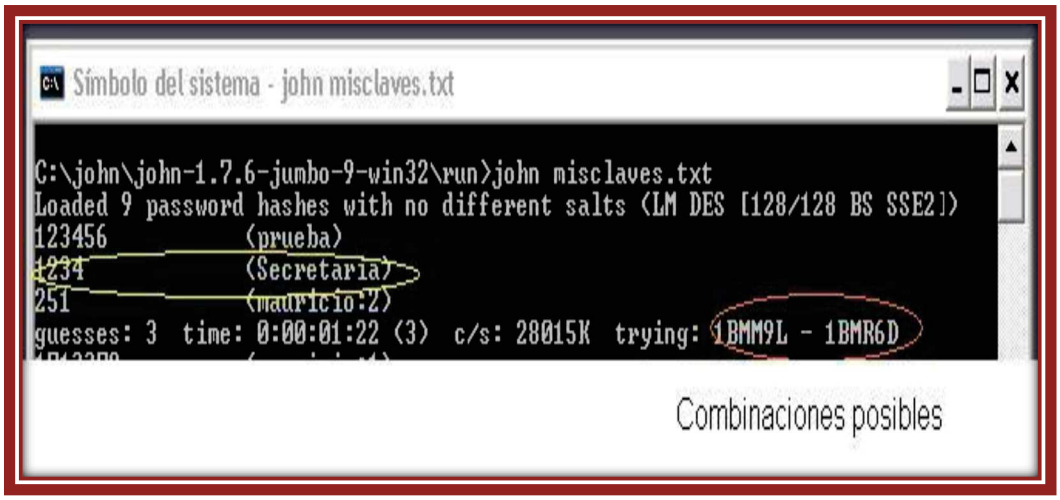


Fig.3.11. Ventana de John Ripper contraseñas encontradas.

Conclusiones:

Es necesario crear dos cuentas de usuario administrador y usuario estándar para tener una adecuada administración con sus respectivas contraseñas y evitar que terceras personas ingresen al sistema, puedan causar daño y se pierda la información.

El programa John Ripper utiliza un ataque de fuerza bruta para descubrir contraseñas, probando todas las combinaciones posibles, en nuestro caso, se ingreso fácilmente al sistema y pudimos conocer todas las contraseñas posibles debido a que no se tiene una cuenta de administrador y de esta manera se puede instalar cualquier programa y modificar el sistema sin restricción.

Recomendaciones:

La manera más eficiente para administrar las cuentas de usuario es creando al menos dos cuentas, una para el administrador cuyo acceso no tiene restricciones y puede hacer los cambios que sean necesarios en el sistema y otros para usuarios estándar. Con todas las restricciones para evitar que puedan realizar cambios en el sistema.

Fig.3.12. Ventana de usuario administrador y estándar como debería utilizarse.

Se recomienda cambiar las contraseñas, en este caso como se observará en la fig.3.13 el nivel de seguridad de esta contraseña (Admin911*Jef) es adecuada y se la utilizará para la cuenta de Administrador; así, cuando se trate de utilizar cualquier programa para descifrarla la búsqueda será más lenta y podrían tardar horas o días en darla a conocer.

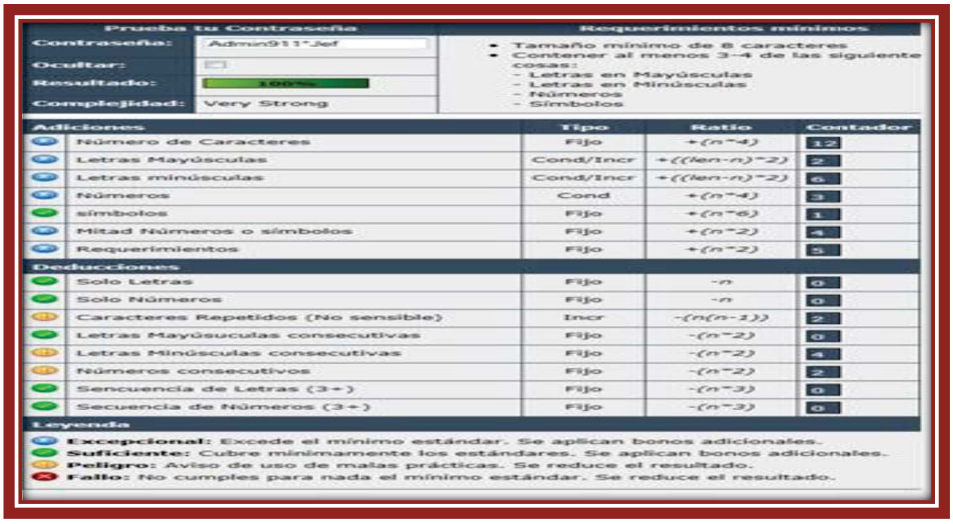


Fig.3.13. Ventana contraseña adecuada que debería utilizar el administrador.

Se utilizó para las cuentas de usuario la siguiente contraseña (User*Carolina/911) como estándar porque su nivel de seguridad es alto como muestra la fig.3.14.

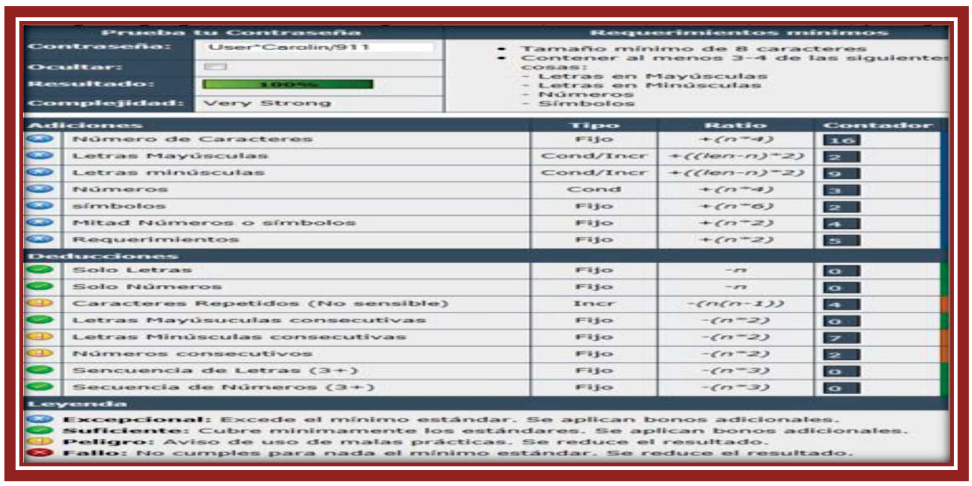


Fig.3.14. Ventana contraseña adecuada que deberían utilizar los usuarios.

3.2 Evaluación Antivirus.

Para la evaluación del Antivirus se procederá a ir a la página www.eicar.org su funcionamiento se basa en un archivo que comprueba el nivel de seguridad y hasta donde analizan los antivirus los virus y en qué circunstancias detecta los archivos infectados y si están funcionando correctamente, no existe ningún riesgo para el equipo. Se copiará la cadena de caracteres que muestra la página como se observará en la figura 3.15

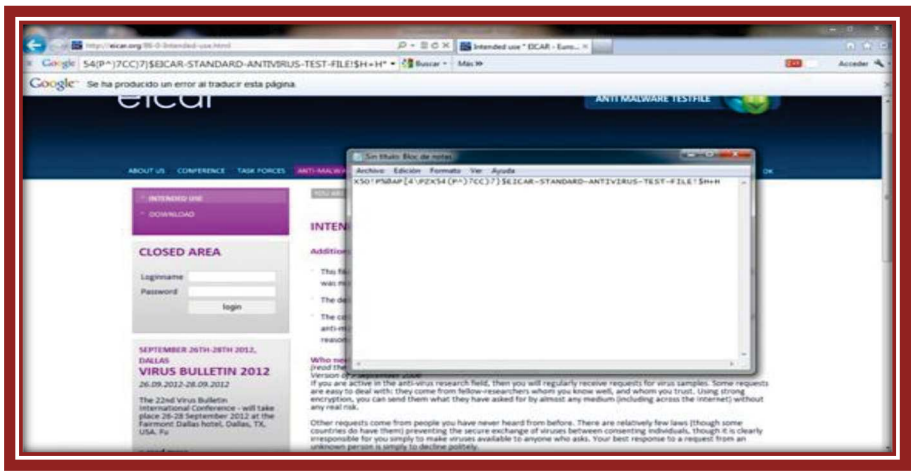


Fig.3.15. Prueba de Eicar en el antivirus Avast.

A continuación se lo guardará en el bloc de notas con la extensión.com.

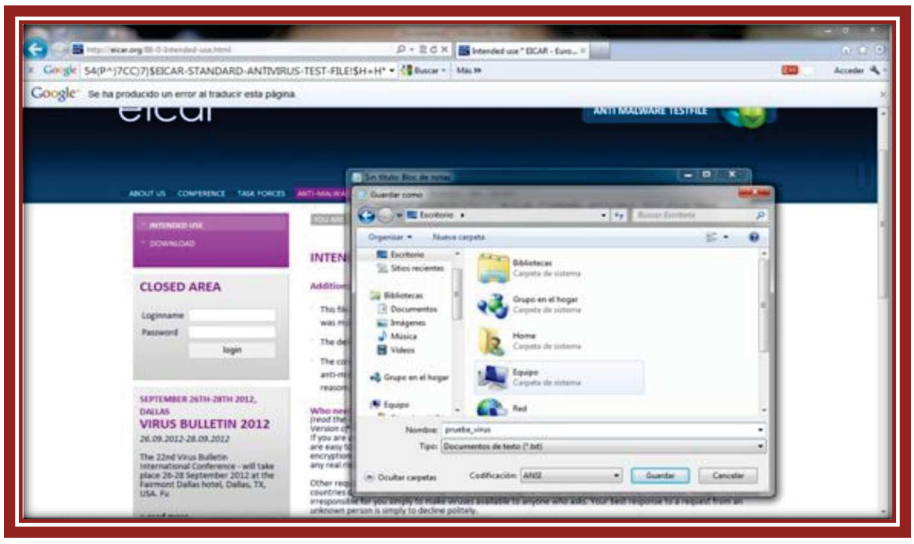


Fig.3.16. Prueba de Eicar en el antivirus Avast.

Luego se abrirá la página que se encuentra resaltada con rojo con esto se logrará examinar si el antivirus captura la descarga y la ejecuta.

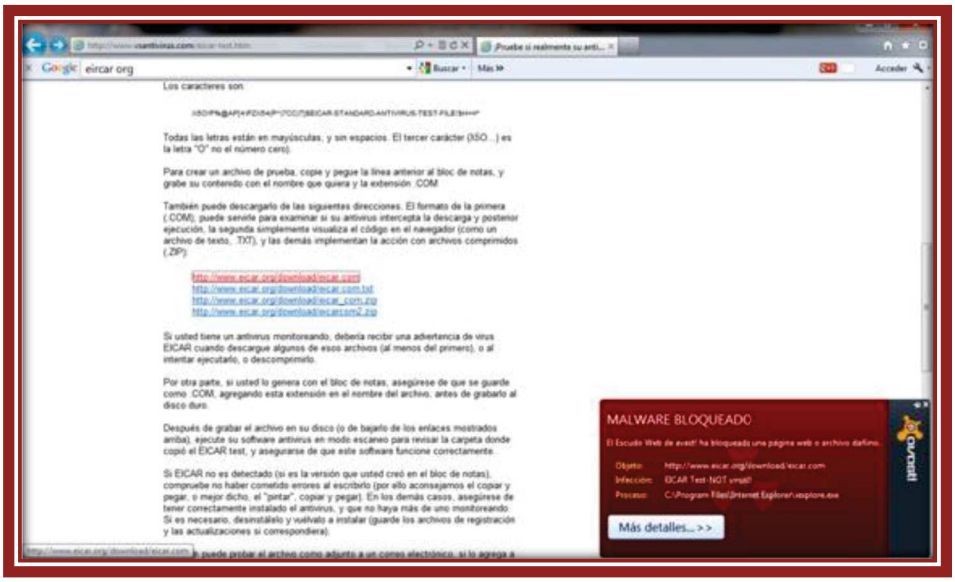


Fig.3.17. Prueba de Eicar en el antivirus Avast.

Se abrirá el siguiente archivo este visualizara el código en el navegador como archivo de texto.

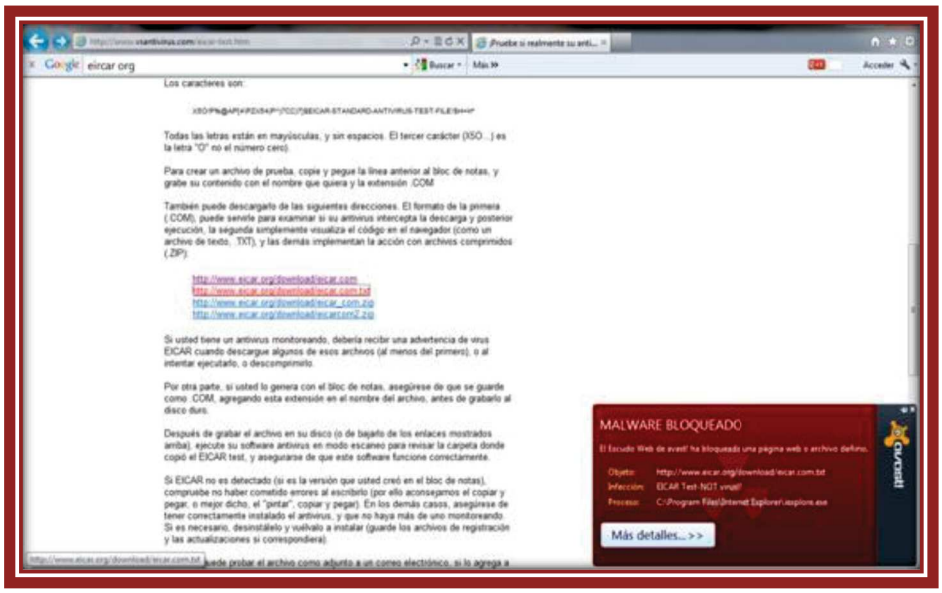


Fig.3.18. Prueba de Eicar en el antivirus Avast.

Las siguientes direcciones implementan la acción con archivos comprimidos ZIP. Como se muestra en las figuras 3.19 y 3.20.

Fig.3.19. Prueba de Eicar en el antivirus Avast.

El Antivirus está trabajando adecuadamente y en tiempo real.

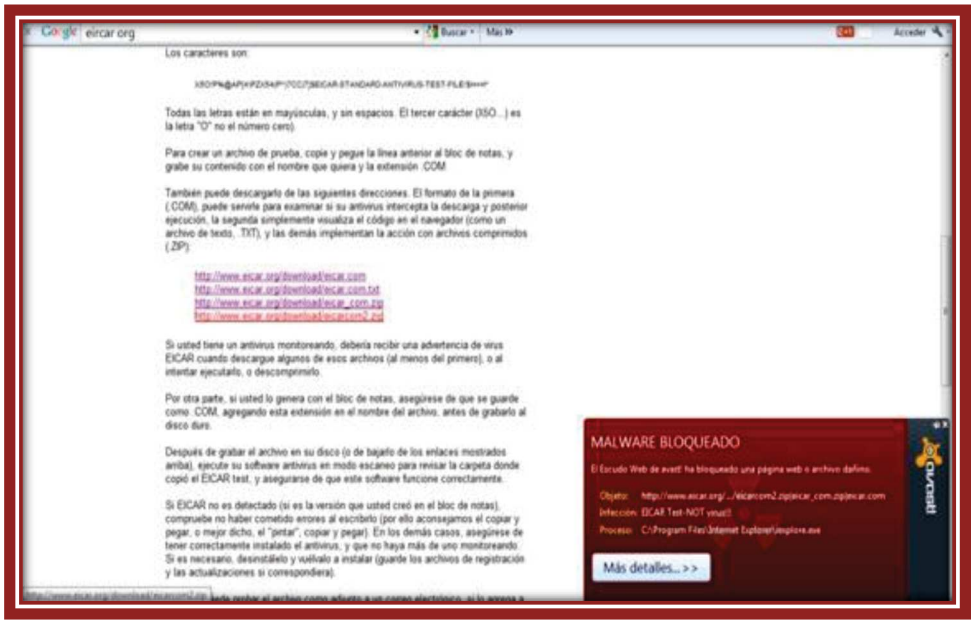


Fig.3.20. Prueba de Eicar en el antivirus Avast.

Se dirigirá a la página http://www.info-techs.com/eicar.shtml ,con esta prueba se puede comprobar la protección del sistema de correo que consiste en pasar un archivo de prueba estándar que no posee ningún código malicioso pero que actúa de manera similar a si tuviera un virus, para esto ingresamos el nombre y dirección de correo electrónico como se muestra en la fig. 3.21.

Fig.3.21. Prueba de Eicar en el antivirus Avast.

A continuación seleccionamos todas las opciones que aparecen y se escribe la palabra de seguridad que se muestra en la parte inferior.

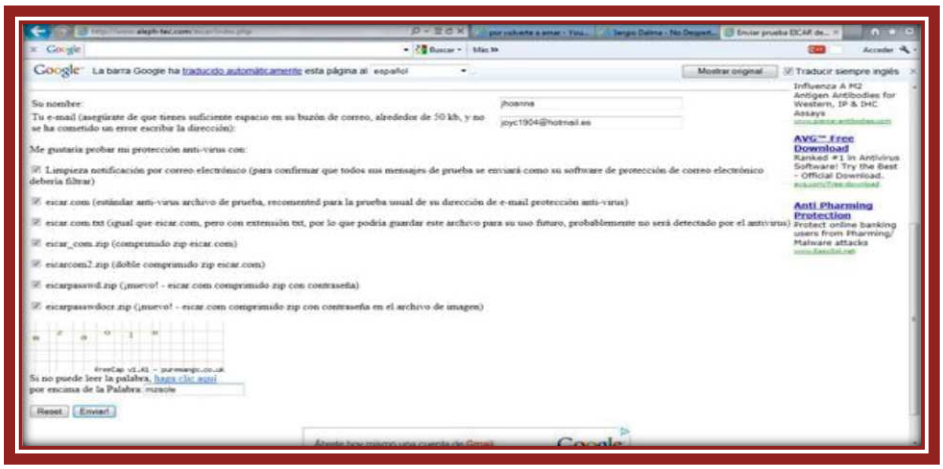


Fig.3.22. Prueba de Eicar en el antivirus Avast.

En la siguiente figura se observará la confirmación del envío de Eicar con los archivos de prueba hacia la dirección de correo electrónico que deseamos que se envié.

Fig.3.23. Prueba de Eicar en el antivirus Avast.

Luego se dirigirá al correo electrónico que se registró en la página de Eicar para abrir los archivos que nos enviaron, se lo descargará y se verificará si es posible abrirlos.

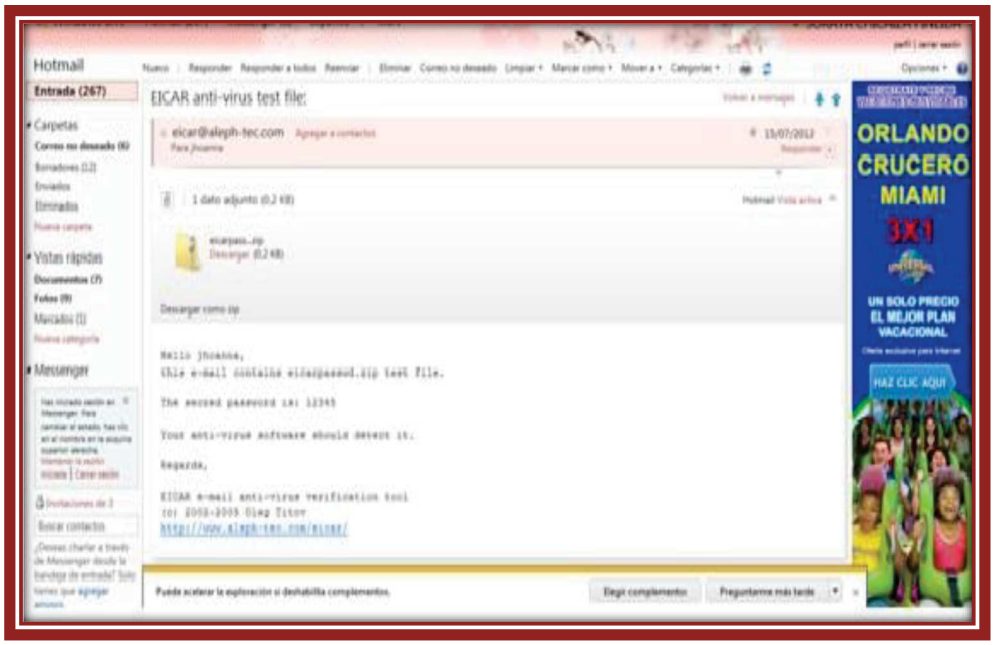


Fig.3.24. Prueba de Eicar en el antivirus Avast.

Se abrirá el archivo y pedirá una contraseña que se encuentra en el correo que envió la pagina de Eicar.

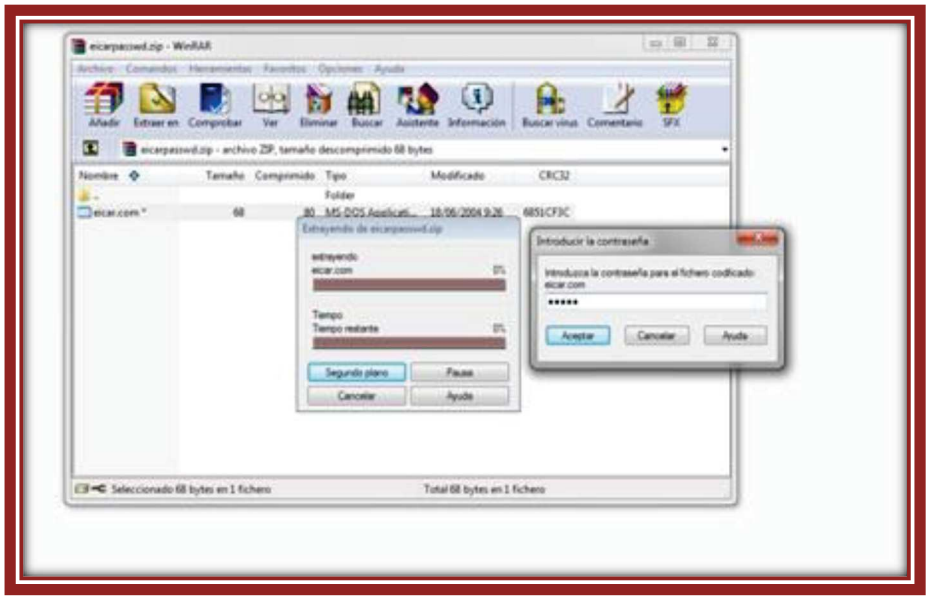


Fig.3.25. Prueba de Eicar en el antivirus Avast.

En este caso el antivirus Avast no permitió abrir el archivo y lo bloqueo.

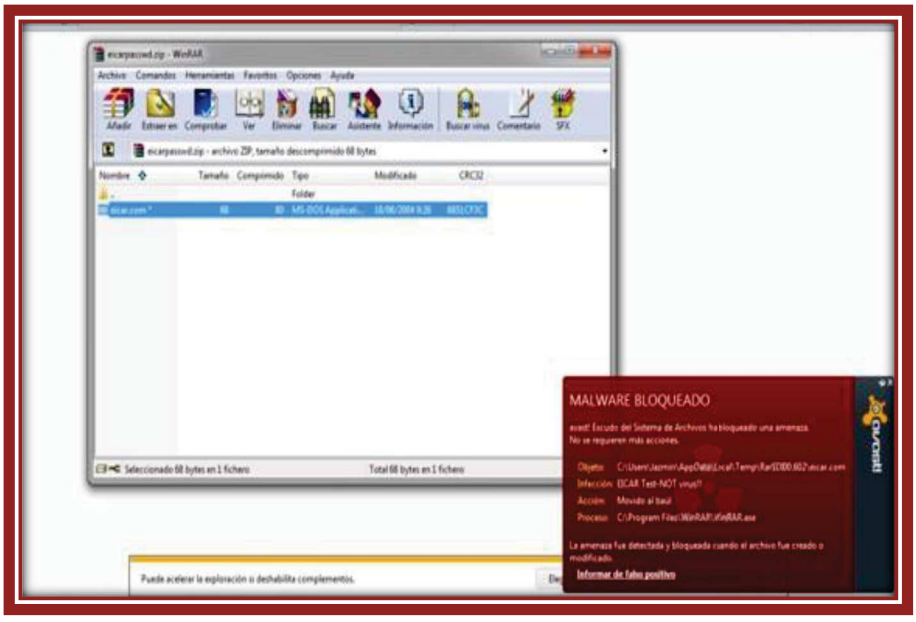


Fig.3.26. Prueba de Eicar en el antivirus Avast.

Ahora se realizarán las mismas pruebas con el antivirus Eset Nod 32 se procederá a ir a la página www.eicar.org , se copiará la cadena de caracteres que muestra la página y se guardará en un archivo de texto.

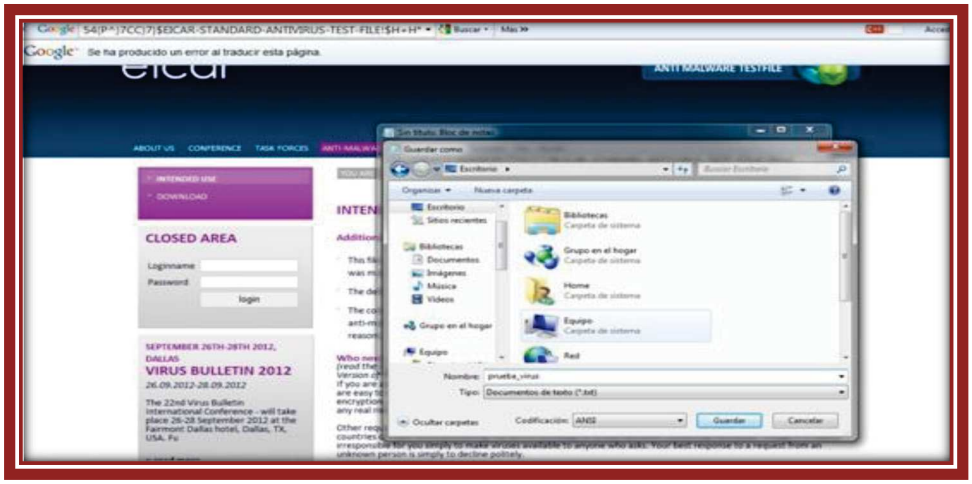


Fig.3.27. Prueba de Eicar en el antivirus Eset Nod.

Se abrirá el archivo guardado para comprobar si el antivirus funciona adecuadamente en este caso el antivirus Eset Nod 32 no permitió que se abra el archivo y lo reconoció como virus.

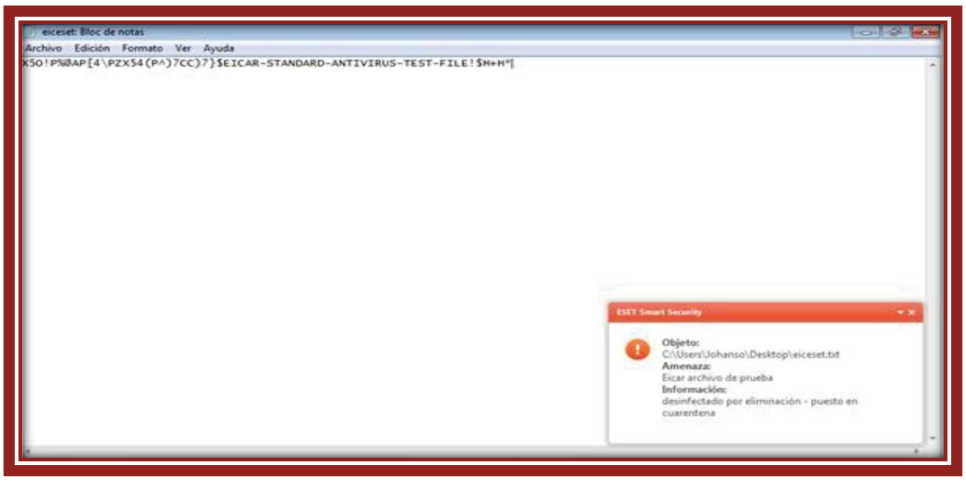


Fig.3.28. Prueba de Eicar en el antivirus Eset Nod.

Se dirigirá a la página que se encuentra al inicio y esta resaltada, con esto se logrará examinar si el antivirus captura el archivo de prueba lo descarga y lo ejecuta.

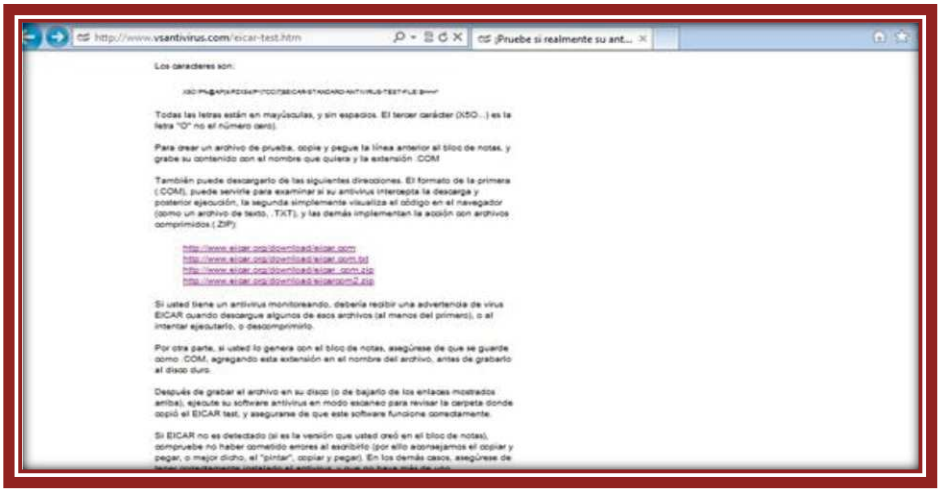


Fig.3.29. Prueba de Eicar en el antivirus Eset Nod.

Se abrirá el siguiente archivo este visualizará el código en el navegador como archivo de texto.

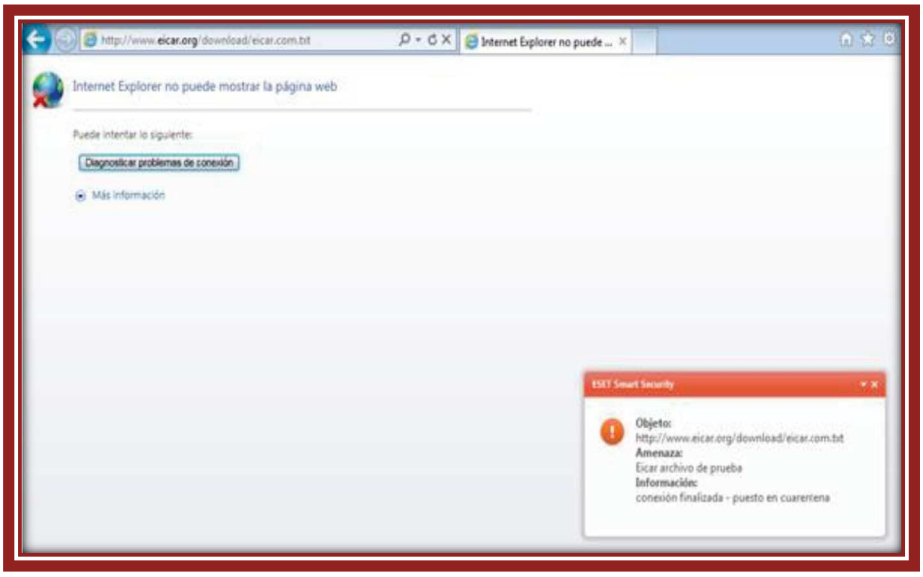


Fig.3.30. Prueba de Eicar en el antivirus Eset Not.

Las siguientes direcciones implementan la acción con archivos comprimidos ZIP. Como se muestra en las figura 3.31

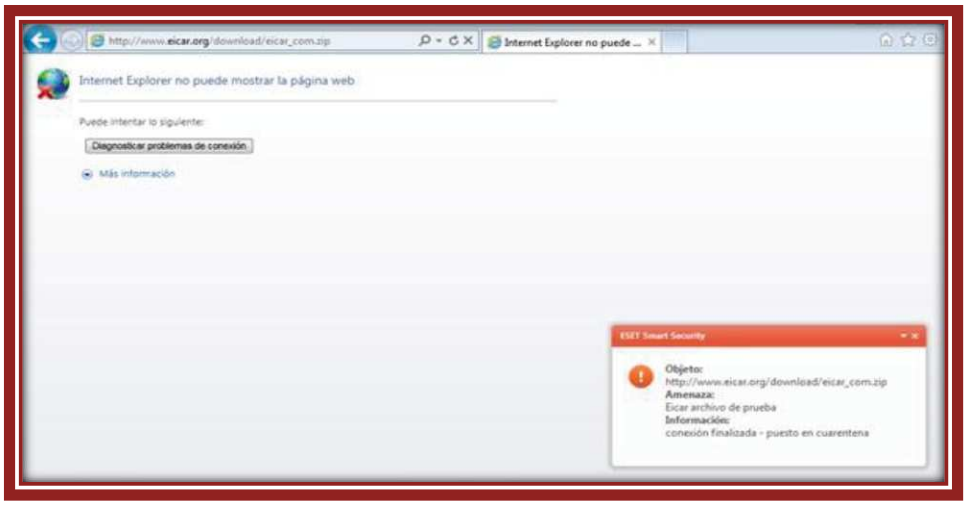


Fig.3.31. Prueba de Eicar en el antivirus Eset Nod.

El antivirus está trabajando adecuadamente y en tiempo real.

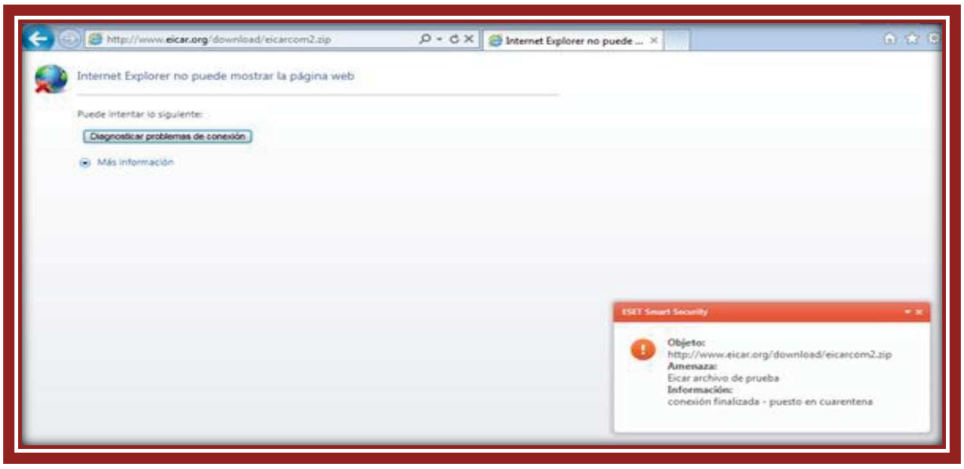


Fig.3.32. Prueba de Eicar en el antivirus Eset Nod.

Como se observó, todas las pruebas se realizaron y el antivirus no permitió que ningún archivo se abra o se ejecute.

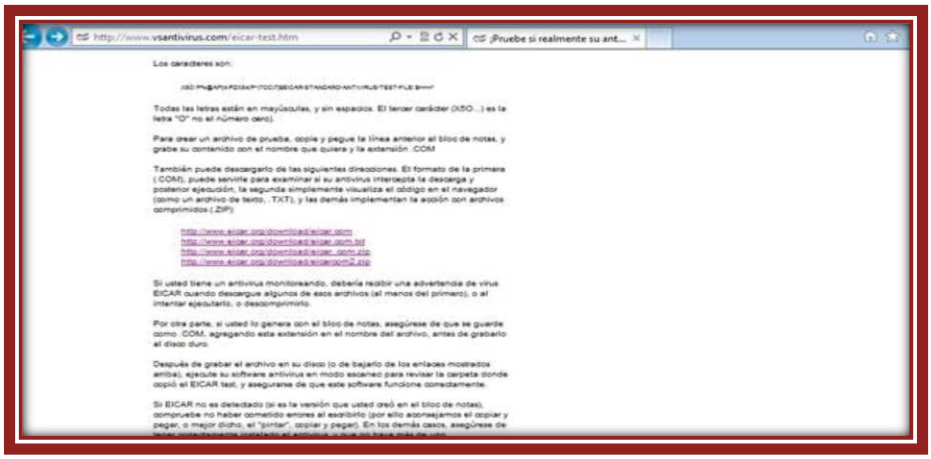


Fig.3.33. Prueba de Eicar en el antivirus Eset Nod.

Se dirigirá a la página http://www.info-techs.com/eicar.shtml

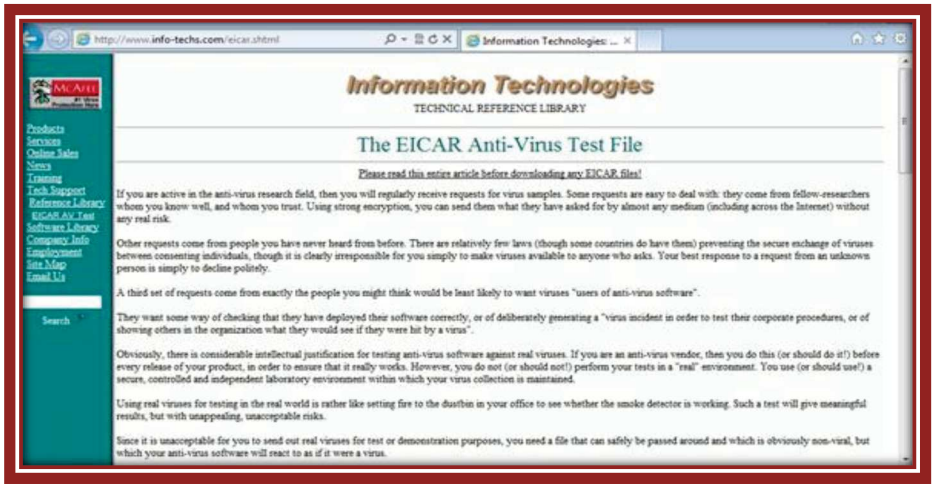


Fig.3.34. Prueba de Eicar en el antivirus Eset Nod.

Luego se enviará todas las pruebas y se añadirá la dirección de correo electrónico a la que se desea enviar las pruebas.

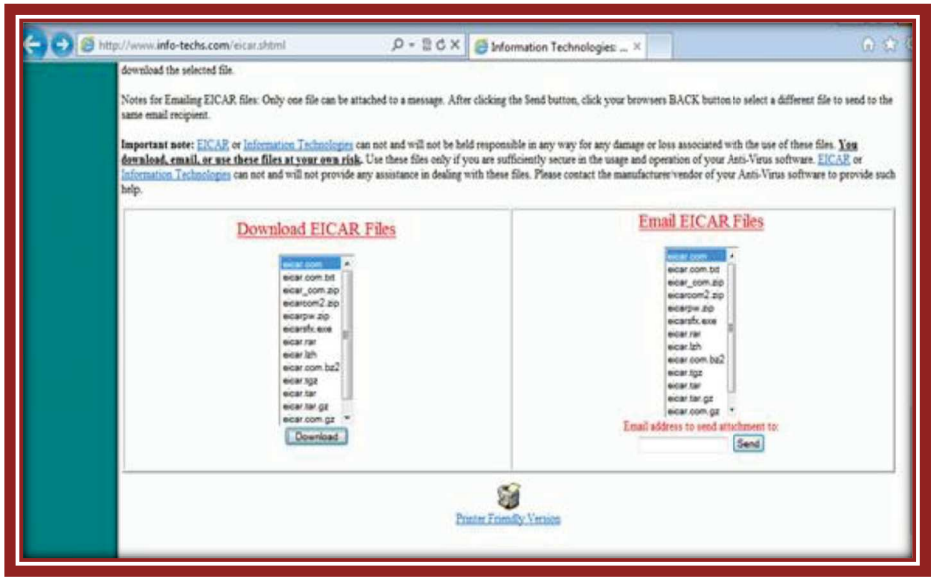


Fig.3.35. Prueba de Eicar en el antivirus Eset Nod.

Se verificará si el antivirus permite abrir los archivos de la página info-techs.com como se muestra en la fig. 3.36 y 3.37.

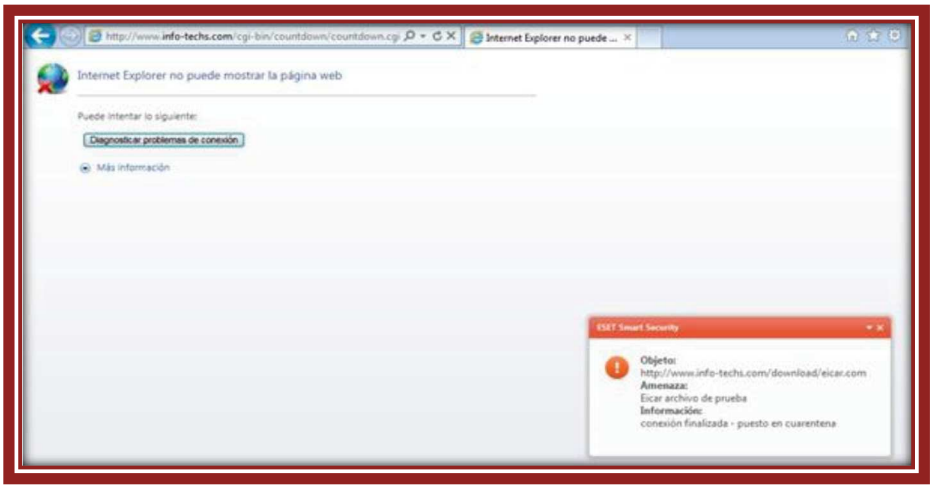


Fig.3.36. Prueba de Eicar en el antivirus Eset Nod.

Como se observó no se permitió el acceso a estos archivos.

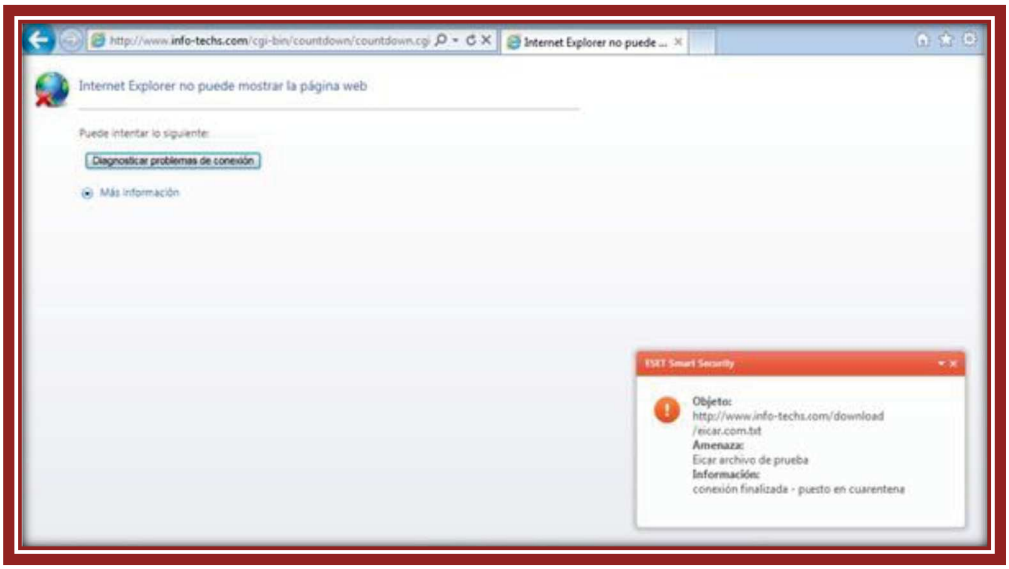


Fig.3.37. Prueba de Eicar en el antivirus Eset Nod.

A continuación seleccionamos todas las operaciones que aparecen y la dirección de correo a la que se desea que se envíe.

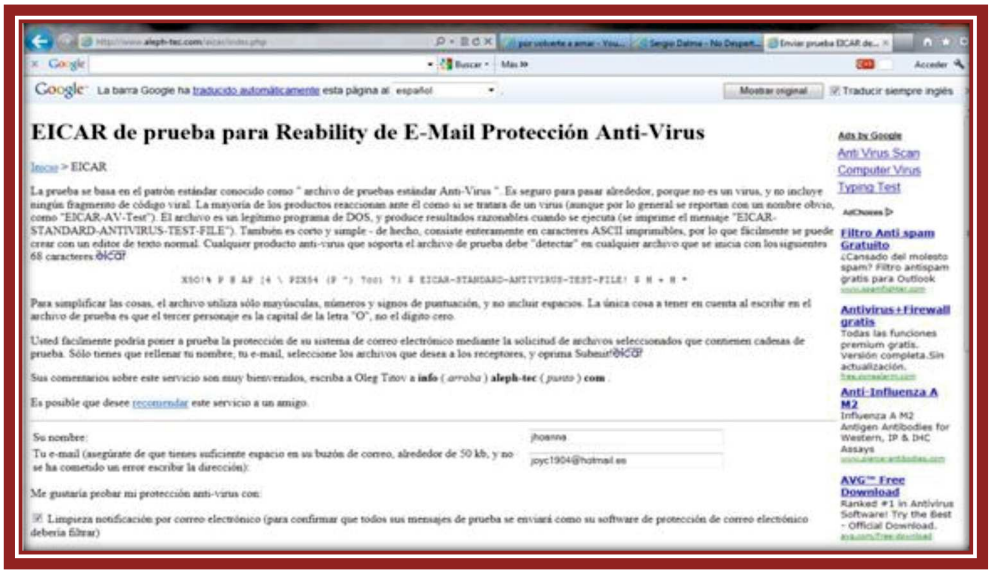


Fig.3.38. Prueba de Eicar en el antivirus Eset Nod.

A continuación se selecciona todas las opciones que aparecen y se escribirá la palabra que se muestra en la parte inferior.

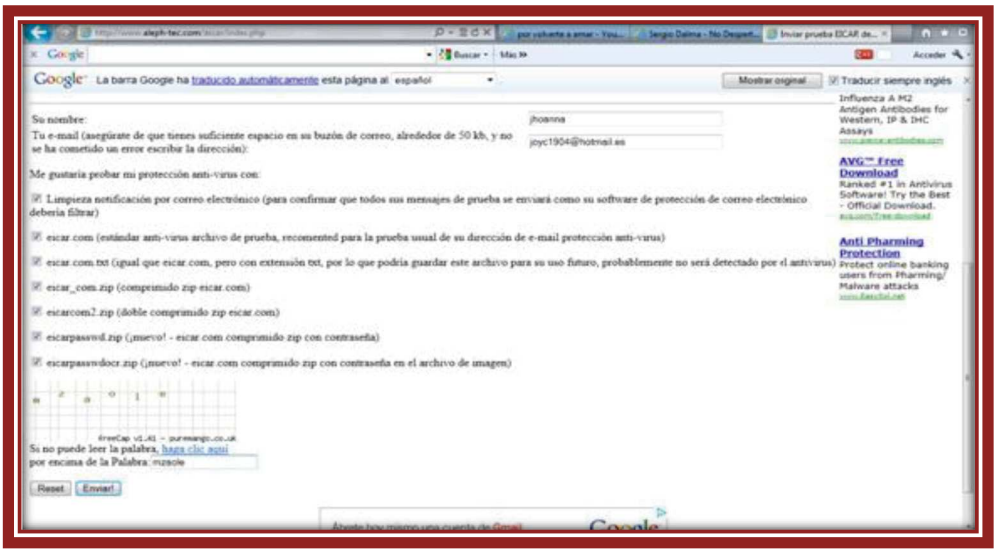


Fig.3.39. Prueba de Eicar en el antivirus Avast.

Luego se observará la confirmación del envío de Eicar con los archivos de prueba hacia la dirección de correo electrónico que se envió.

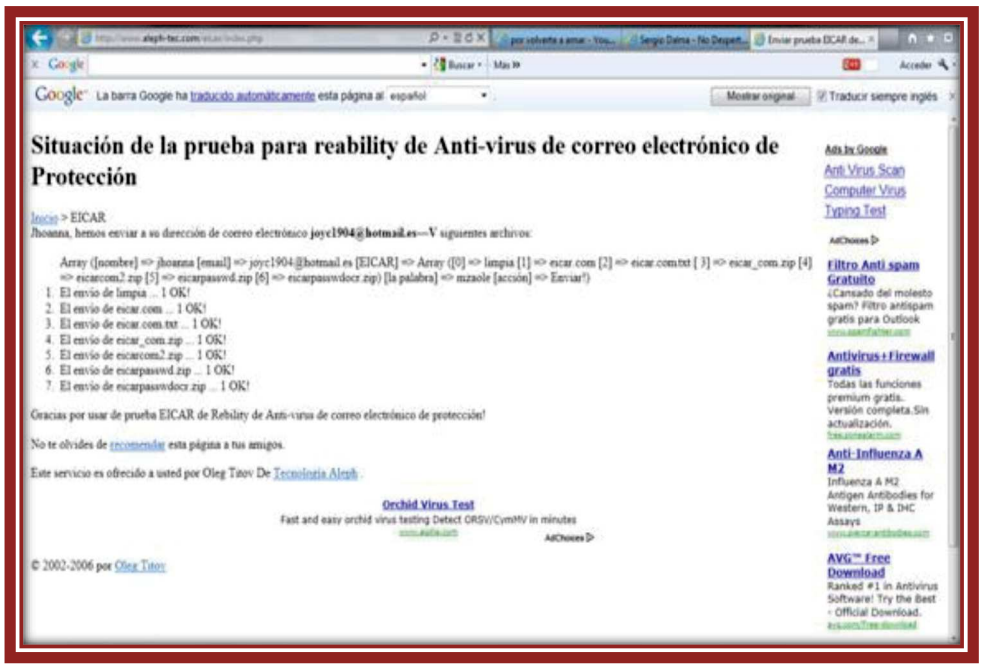


Fig.3.40. Prueba de Eicar en el antivirus Eset Nod.

Eicar enviará la confirmación de la solicitud y si el resultado fue exitoso.

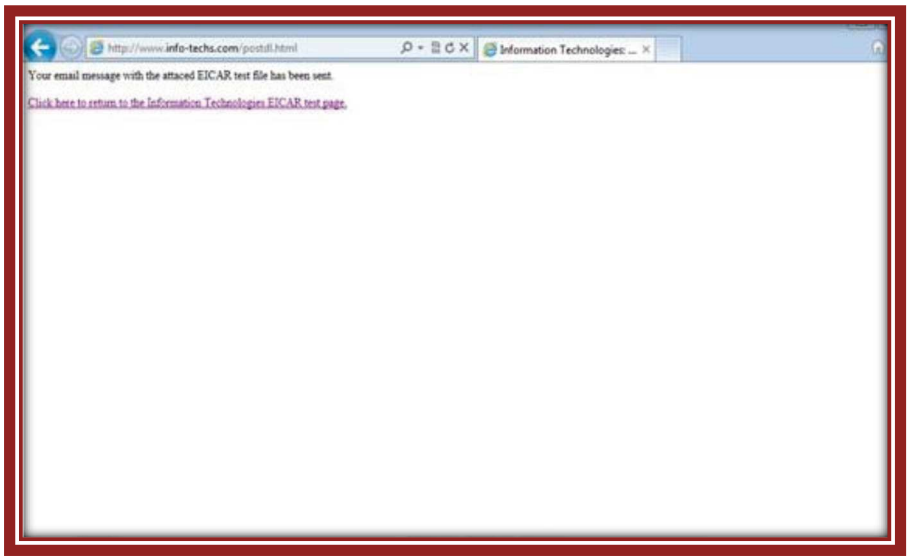


Fig.3.41. Prueba de Eicar en el antivirus Eset Not.

Luego se dirigirá al correo electrónico que se registró en la página de Eicar para abrir los archivos, se los descargará y se verificará si se permite abrirlos.

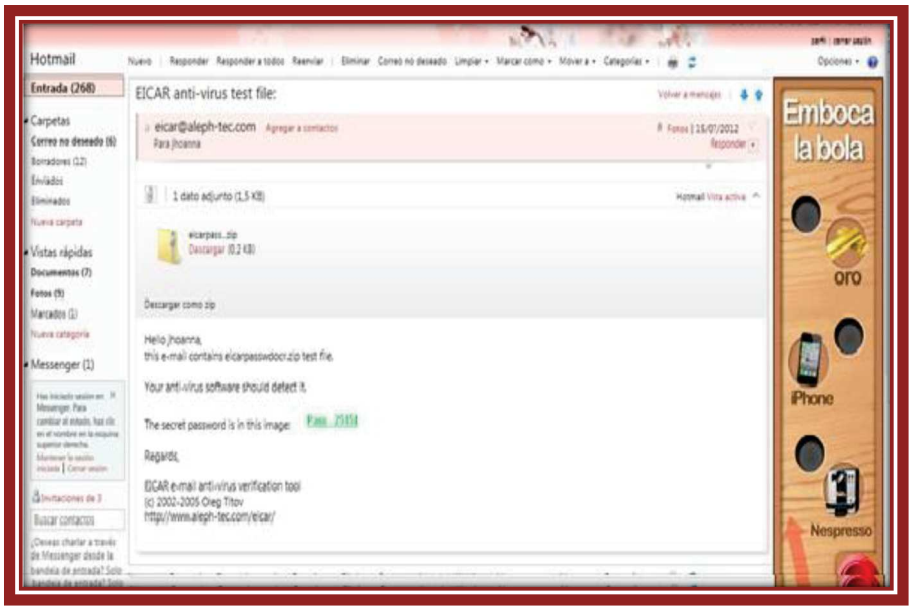


Fig.3.42. Prueba de Eicar en el antivirus Eset Not.

Se abrirá el archivo y se ejecutará.

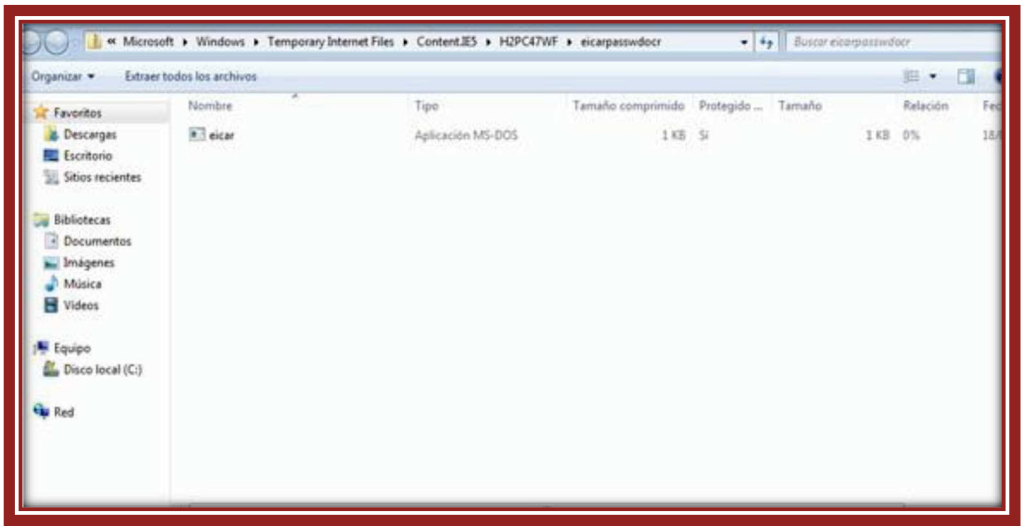


Fig.3.43. Prueba de Eicar en el antivirus Eset Nod.

Luego se digitará la contraseña que se encuentra en el correo que envió Eicar.

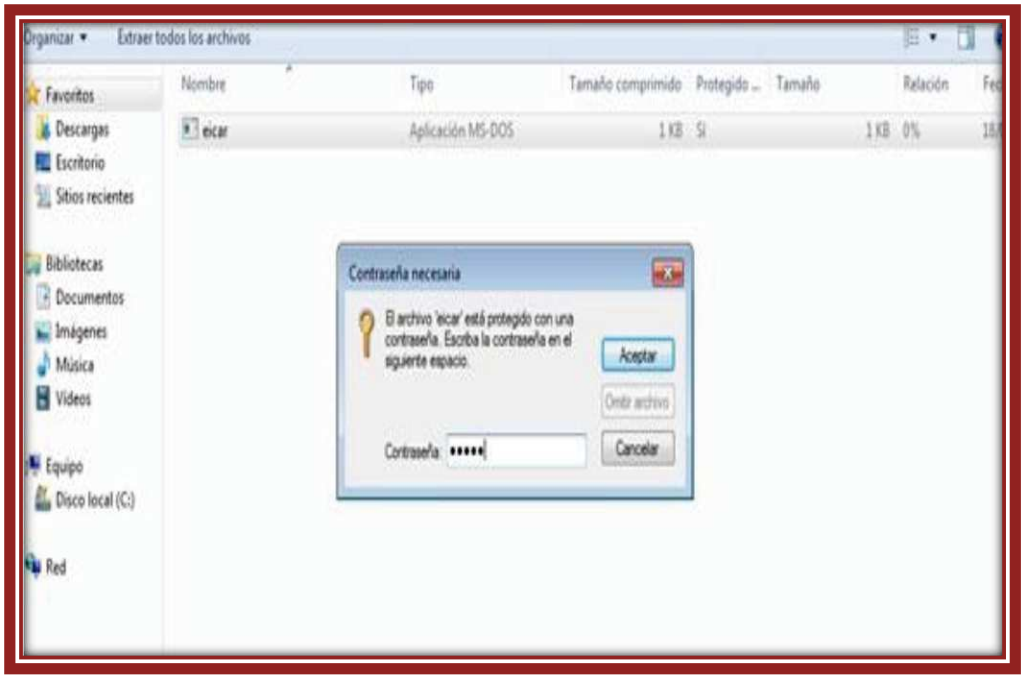


Fig.3.44. Prueba de Eicar en el antivirus Eset Nod.

En este caso el antivirus Eset Nod 32 no permitió abrir el archivo y lo bloqueo.

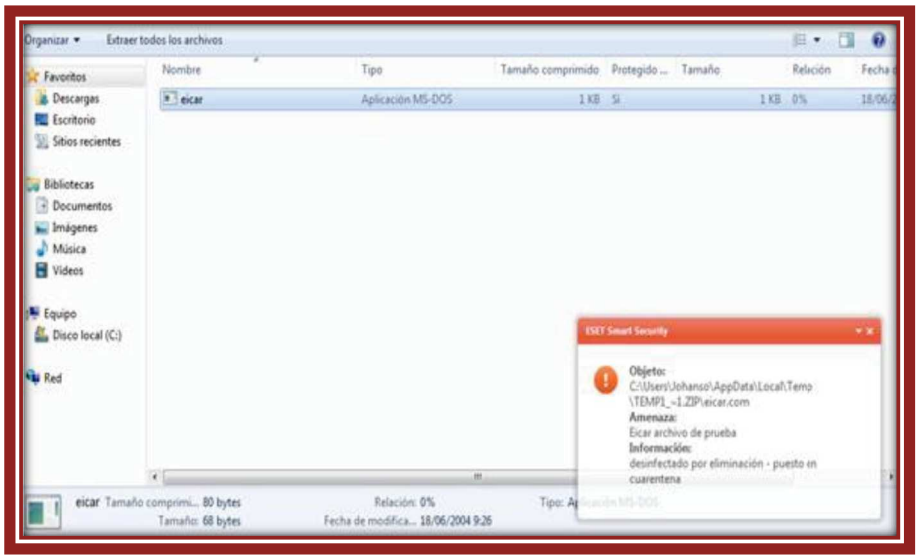


Fig.3.45. Prueba de Eicar en el antivirus Eset Nod.

A continuación se observará los archivos con su respectivo nombre posición y funcionamiento que se descargaron para realizar las pruebas de Eicar como se muestra en la fig. 3.46.

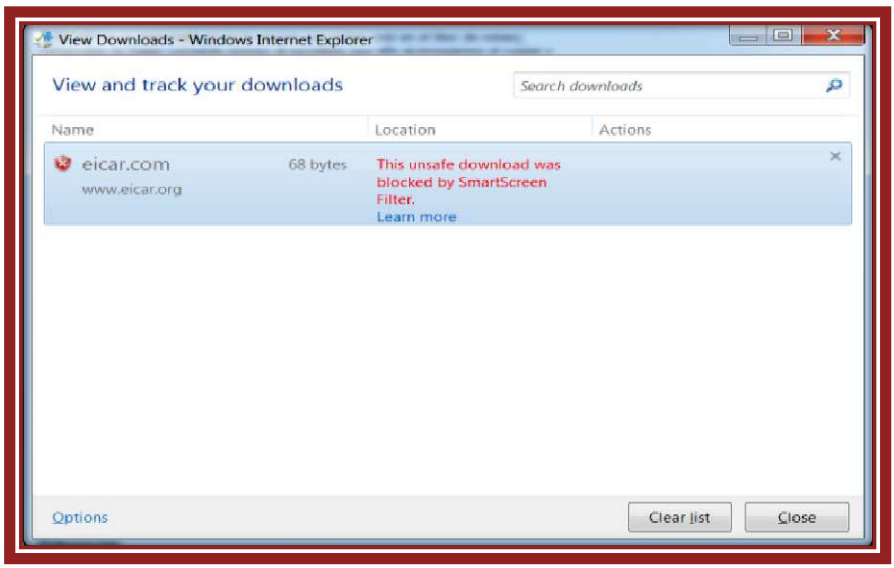


Fig.3.46. Ventana de análisis de antivirus con Eicar.

Como se observó se encuentran todos los archivos de prueba de Eicar el archivo .com.txt, com.zip, zip2.com y el eicar.com como indica la fig.3.47 y 3.48.

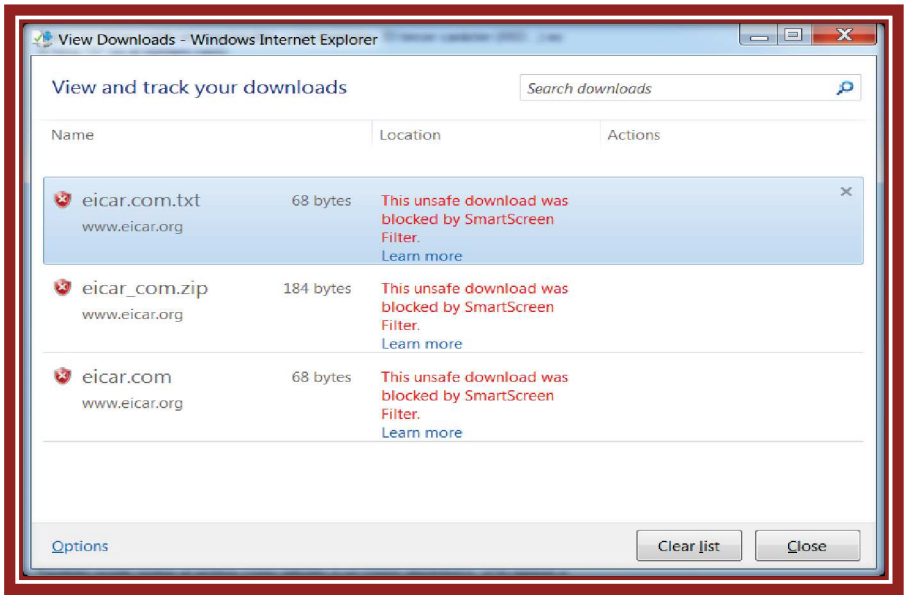


Fig.3.47. Ventana de análisis de antivirus con Eicar.

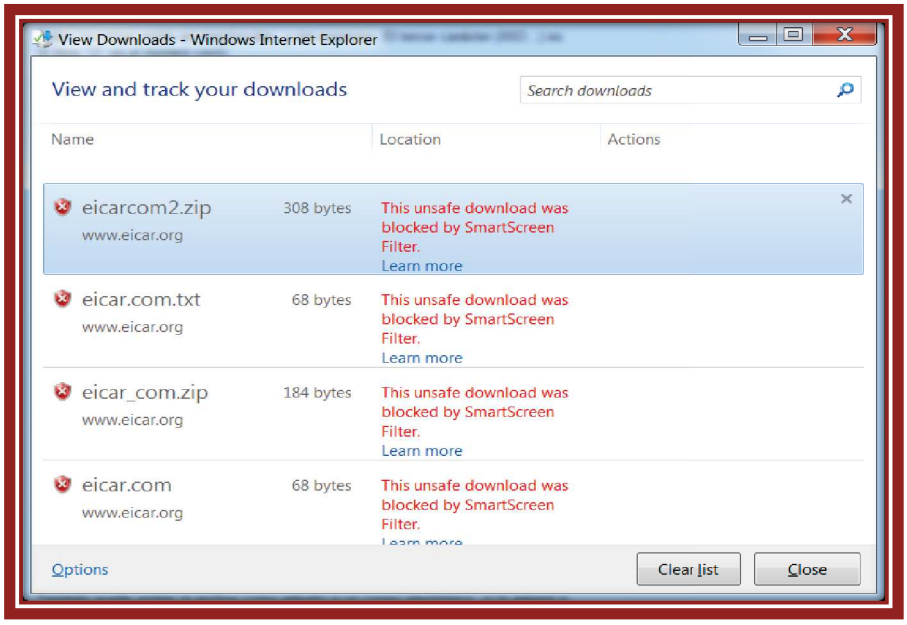


Fig.3.48. Ventana de análisis de antivirus con Eicar.

Conclusiones:

Eicar sirve para probar el funcionamiento del antivirus, no es un virus se basa en un archivo de prueba que verifica, la efectividad y capacidad de alerta del antivirus instalado.

Verifica hasta donde detecta el antivirus los archivos infectados y si restringe su descarga y ejecución. Al realizar el test el antivirus no permitió abrir los archivos y lo pusieron en cuarentena tanto el antivirus Eset Nod como el Avast.

Recomendaciones:

Revisar que la página web www.eicar.org a la que se ingresará sea la oficial ya que existen páginas que son idénticas pero son manejadas por Hackers o personas mal intencionadas para causar daño enviando software malicioso o virus.

Copiar la contraseña que se encuentra en el correo que envía Eicar para realizar la prueba debido a que si no se digita correctamente no se descomprime el archivo y no se obtiene ninguna respuesta por parte del antivirus.

Utilizar un antivirus que tenga licenciamiento ya que poseen más opciones al instante de configurarlo y así evitar la infiltración de virus que dañen el sistema operativo.

3.3 Evaluación de conectividad de los dispositivos.

La Dirección IP se usa para identificar un host o una red ya sea local o externa. Cuando se utiliza el servicio de Internet el Host se identifica con el servidor al que está conectado o viceversa.

Para saber cuál es la IP que se estará utilizando para navegar en Internet se dirigirá a la siguiente página http://whatismyipaddress.com/. La dirección IP sirve para identificar el país o región cuando un equipo se conecta a Internet como se observa en la figura 3.49.

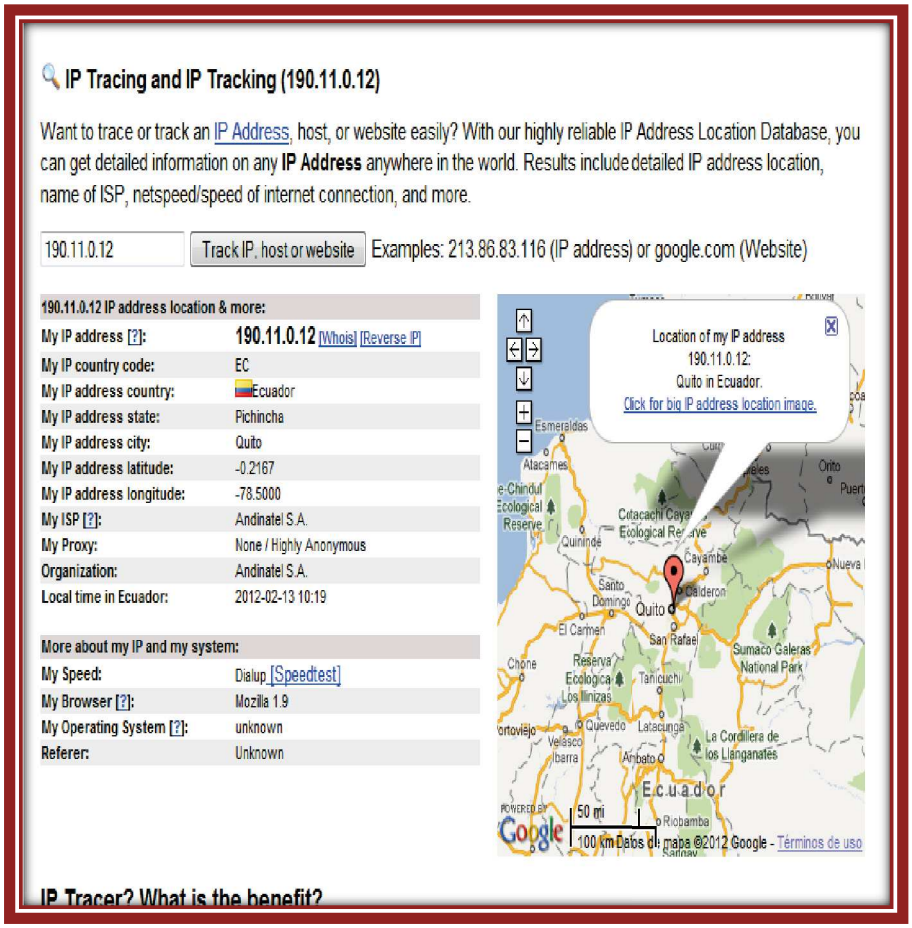


Fig.3.49. Ventana de análisis de la dirección IP púbica.

Para verificar la conexión de los equipos se dirigirá a Windows Inicio Símbolo, CMD y se digita PING más la dirección IP con la que se requerirá establecer comunicación. Con el comando Ping se realizará la comprobación del estado de conexión con uno o varios equipos remotos su utilidad se basa en diagnosticar los errores en redes o enrutadores.

En este caso se constatará que la conexión está bien y sin errores de la dirección IP 190.11.0.12 y la IP 192.168.1.1.

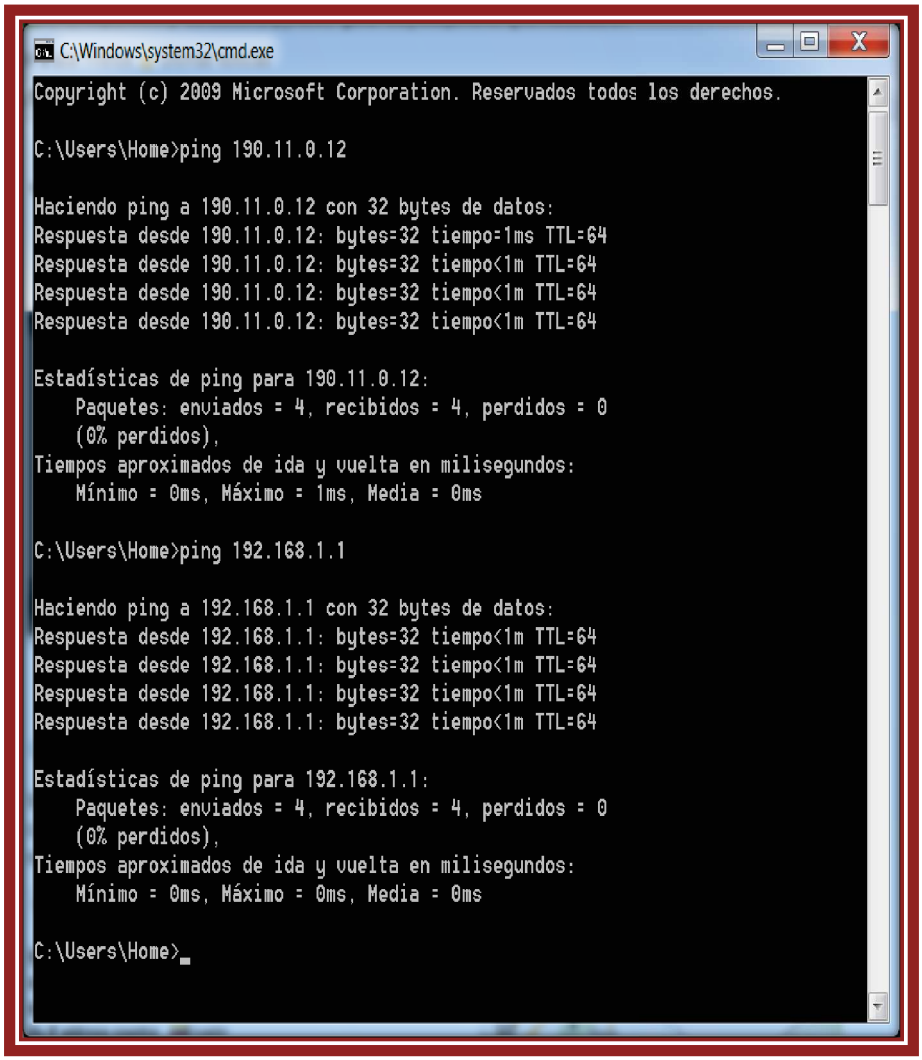


Fig.3.50. Ventana de análisis de conectividad de la IP púbica con el comando ping.

En el siguiente caso se observará que existe un conflicto de conexión con errores y que no existe respuesta con la dirección IP 192.168.1.11 y 192.168.1.12 como se observa en la figura 3.51.

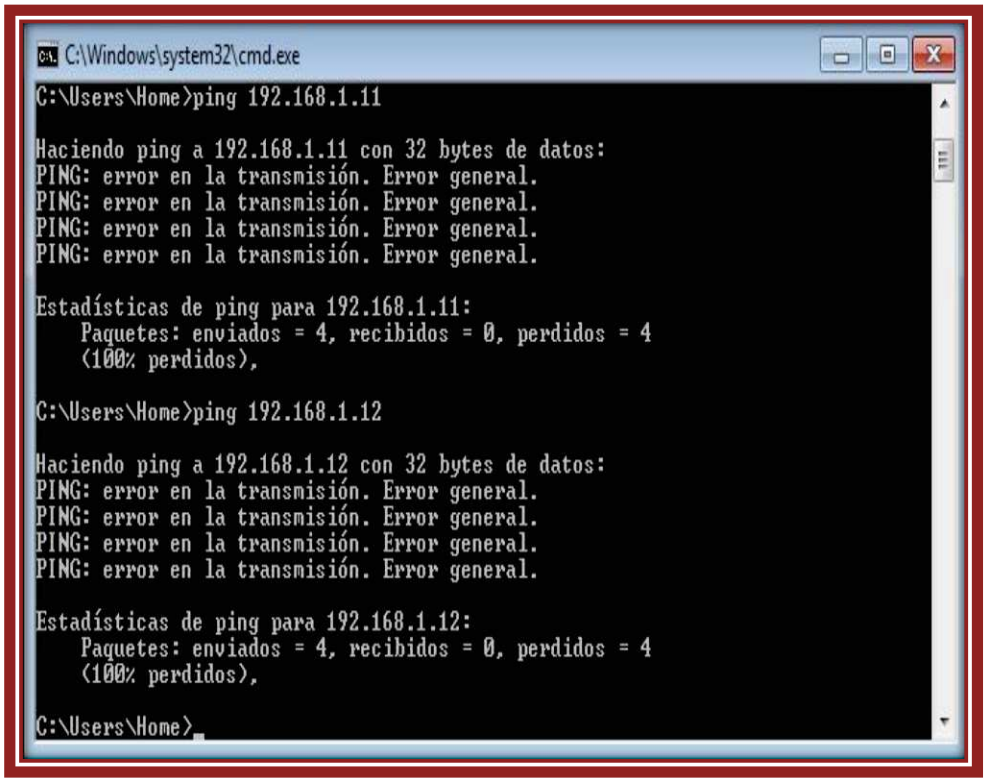


Fig.3.51. Ventana de análisis de conectividad de la IP de la red utilizando el comando ping.

Conclusiones:

La utilización del comando Ping proporciona la información necesaria en la conexión de la red con otros dispositivos, obteniendo una respuesta rápida.

Es muy importante saber la IP que se está utilizando para identificar el país o región cuando existe conexión a Internet.

Si existen conflictos de conexión y no se reconoce a otro equipo en la red puede ser debido a que el adaptador de red esta deshabilitado o porque la dirección IP y su máscara son inadecuadas y no se encuentran en el rango que le corresponde.

Recomendaciones:

Verificar si el adaptador de red esta encendido para esto se dirigirá a Windows centro de recursos compartidos luego a la opción cambiar configuración del adaptador, conexión de área local luego a activar y estará encendido.

Fig.3.52. Ventana de conectividad adaptador de red Windows .

Resolver el problema de conectividad en caso de que la dirección IP y máscara sean inadecuadas se dirigirá en Windows al centro de recursos compartidos luego a la opción cambiar configuración del adaptador, conexión de área local luego a propiedades de conexión local , protocolo de Internet versión TCP/IP 4 y a continuación la opción propiedades. Se deberá configurar la dirección IP y máscara adecuada como se observa en la fig.3.3 (5) lo que está mal configurado es la mascará de red por lo que lo óptimo es 255.255.255.240 para utilizar 14 host.

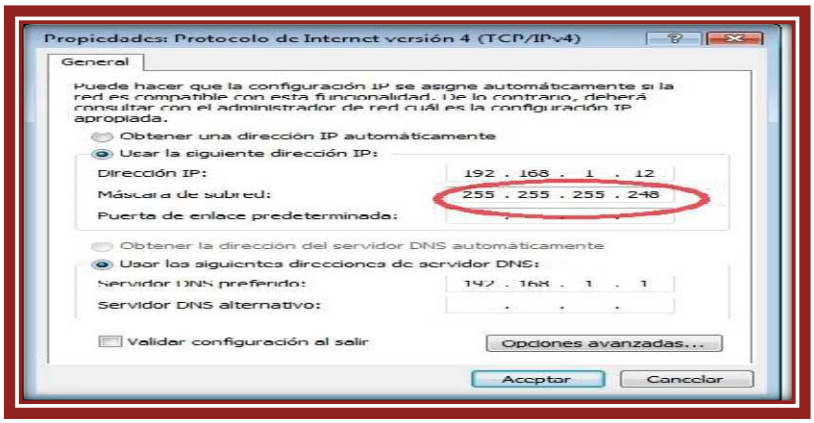


Fig.3.53. Ventana de conectividad adaptador de red Windows.

3.4 Evaluación de Proxy.

El servidor proxy en línea es un servicio utilizado para navegar vía web en forma anónima para poder acceder a varios sitios bloqueados evitando las seguridades.

Se basa en la utilización de un servidor espejo en el cual estará la IP y otros detalles ocultos. Cuando el administrador de red bloquea algunos sitios como las redes sociales evita que entren a estos sitios y se concentren solo en el área de trabajo. Para esto se utiliza el proxy anónimo y no deja rastro de las páginas que se estaba viendo y utilizando.

Se dirigirá a la siguiente página http://zend2.com/ y se digitará la pagina a la cual se desea acceder en este caso www.Ares.com.

Fig.3.54. Ventana de análisis del proxy anonymous.

Como se observará a continuación se logró ingresar a la página www.Ares.com se tomó como ejemplo esta página debido a que es una aplicación que permite la infiltración de virus, también se ingresó a las redes sociales y páginas de pornografía lo que significa que no se tiene bloqueado el acceso a estos sitios web debido a que no se cuenta con un servidor proxy.

Fig.3.55. Ventana de análisis del proxy anónimos para abrir el Programa Ares.

Conclusiones:

El proxy limita y restringe los derechos de usuario, puede negarse a responder algunas peticiones si detecta que estas están prohibidas aprovecha los recursos al máximo actúa como intermediario en la comunicación entre usuarios de una red local y el Internet.

Recomendaciones:

Lo favorable sería tener un servidor proxy ya que este intercepta las conexiones de red que un cliente hace a un servidor de destino y esto se lo puede realizar por un programa o un dispositivo.

Es adecuado utilizarlo en las empresas debido a que así los empleados solo tienen acceso a ciertas páginas que tiene relación con el trabajo que realizan.

3.5 Evaluación de la configuración IP de los host de red.

Se dirigirá a Windows, centro de recursos compartidos, cambiar configuración del adaptador, conexión de área local, propiedades, TCP IPV4 y se observará la dirección IP la máscara de red, el Gateway, y DNS en este caso el primer host tiene asignada una IP fija de manera manual. La empresa requiere una configuración para trabajar con 8 Host y 2 impresoras conectadas a la red, como se observará en la siguiente figura la IP es 192.168.1.6 y su máscara de subred es 255.255.255.192 con la cual se puede trabajar con conexión de red para 62 Host lo que excede el número de IP´S que normalmente se requiere.

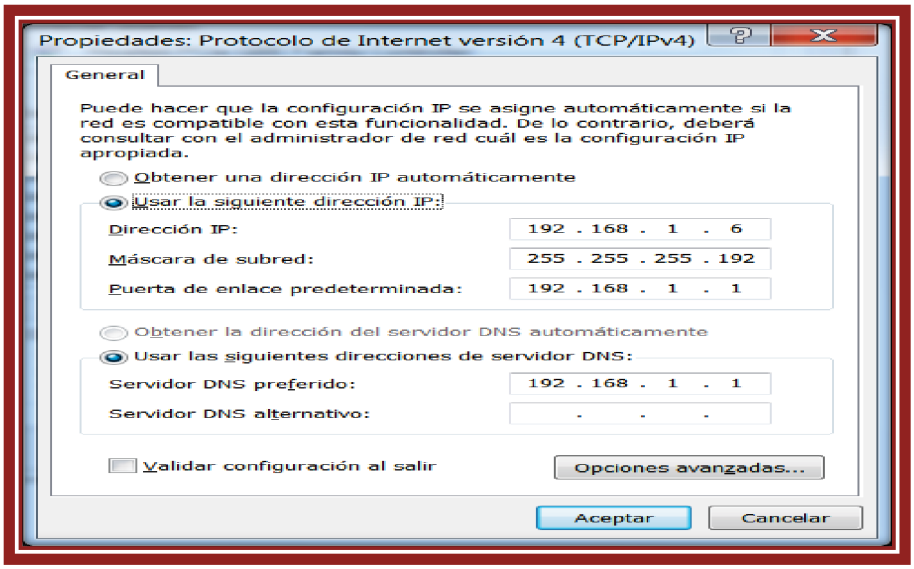


Fig.3.56. Ventana de análisis de la configuración de los host.

En el siguiente caso se observará que otro Host tiene configurado la IP 192.168.1.11 con máscara 255.255.255.248 lo que tampoco es adecuado debido a que con este rango funciona solo para trabajar con conexión de red con 6 Host y la empresa requiere trabajar con 8 Host y 2 impresoras.

Esto genera conflictos en la conexión entre dispositivos ya que no se encuentran en la subred por lo tanto no pueden comunicarse y no

pueden compartir recursos como se muestra en la fig. 3.57.

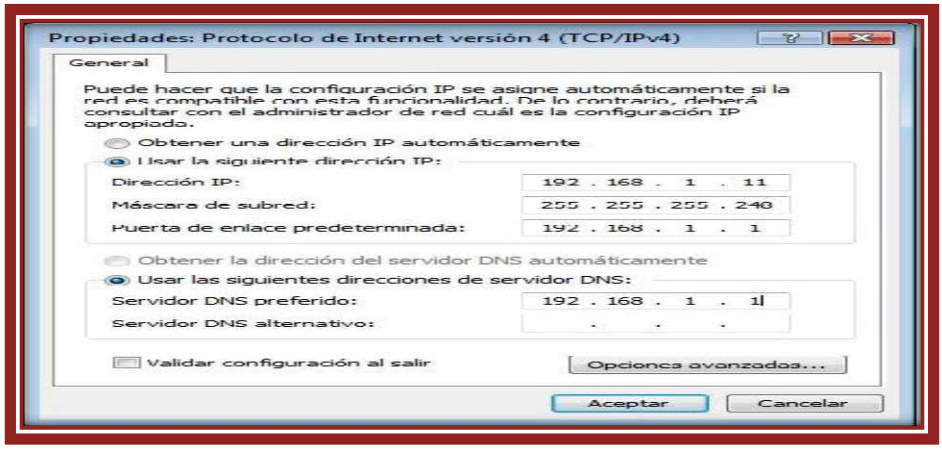


Fig.3.57. Ventana de análisis de la configuración de los host.

En el siguiente caso otro host tiene asignada su dirección IP de manera automática por medio del servidor DHCP. Cuando existen computadoras portátiles que se conectan a la red por medio del WIRELESS, el servidor DHCP asigna direcciones IP que estén libres pero no es inteligente para registrar que IP tiene los otros Host por ejemplo si un Host estaba apagado y coinciden con otra dirección IP de la red local se generan conflictos en conexión por duplicación de IP´S.

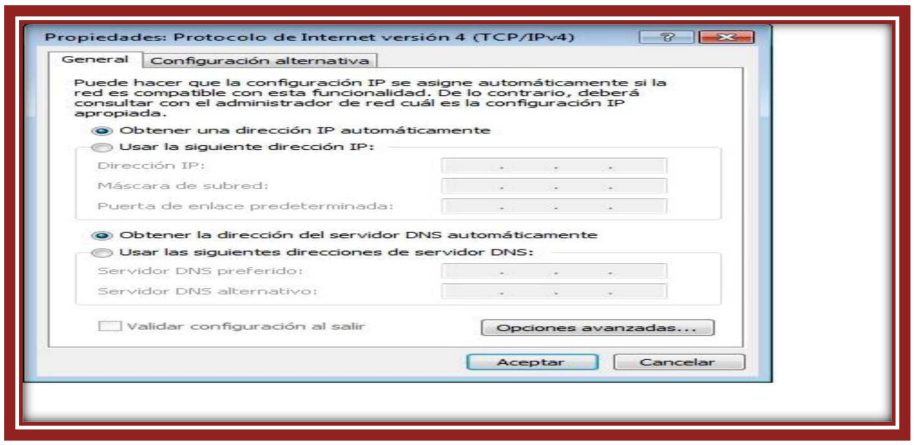


Fig.3.58. Ventana de análisis de la configuración IP con DHCP.

Como se pudo observar se encuentran asignados 2 tipos de configuraciones IP manual y dinámica por esta razón existen conflictos en la comunicación.

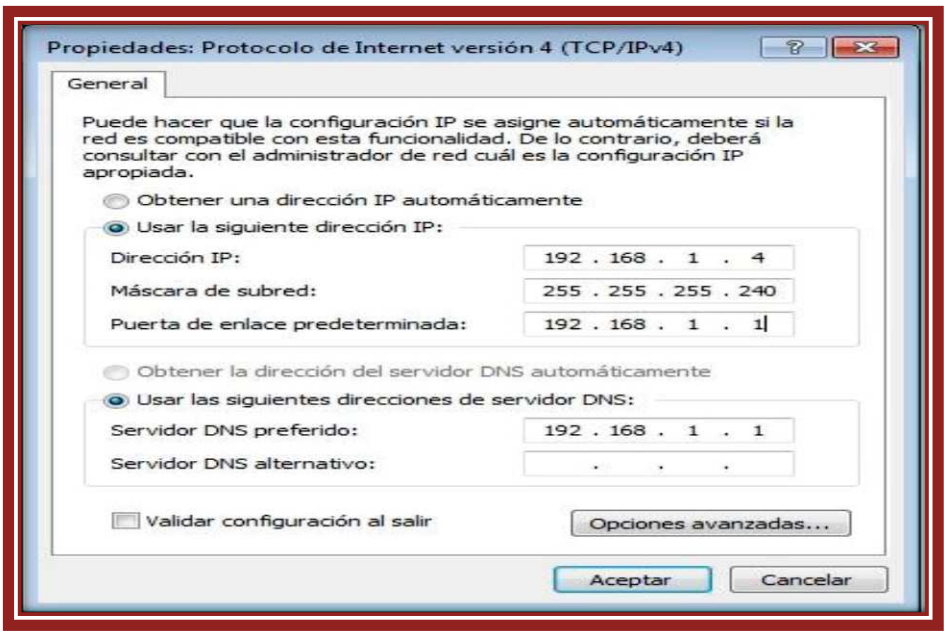


Fig.3.59. Ventana de análisis de la configuración IP con DHCP.

Conclusiones:

La configuración de las direcciones IP son muy importantes para el establecimiento de comunicación con otros Hosts. Si se encuentra mal configurado existen serios problemas ya que impide el óptimo desenvolvimiento de los sistemas. Y esto se lo puede hacer mediante la asignación de direcciones IP en forma manual o por medio de DHCP que permite a un host obtener una dirección IP en forma dinámica cuando se conecta a la red.

Recomendaciones:

Utilizar el siguiente rango de IP´S con DHCP desde 192.168.1.11 hasta 192.168.1.14.

Utilizar el siguiente rango de IP´S fijas desde 192.168.1.1 hasta 192.168.1.10.

Lo óptimo para trabajar en una red local que consta de 8 estaciones de trabajo y 2 impresoras se debería utilizar la siguiente configuración en el rango de 192.168.1.1 con máscara 255.255.255.240 que sirve para utilizar 14 Host con conexión a la red y que solo las computadoras portátiles se conecten a la red por medio del WIRELESS asignándole su dirección de manera dinámica el servidor DHCP.

3.6 Evaluación de listas negras.

Una lista negra es una base de datos donde se registran las direcciones IP que envían correo masivo no solicitado ya sea publicitario o no, son listas de fuentes conocidas como SPAM. Los filtros SPAM utilizan la lista negra como un método de bloquear el SPAM y obliga a los ISP a monitorear el correo de salida si un ISP es incluido en la lista negra los correos recibidos de el serán devueltos. Para verificar si la dirección IP se encuentra en la lista negra se dirigirá a la página http://www.anti-abuse.org/multi-rbl-check/ y se digitará la dirección IP que va a ser evaluada en este caso la IP pública 190.11.0.12 no se encuentra en lista negra.

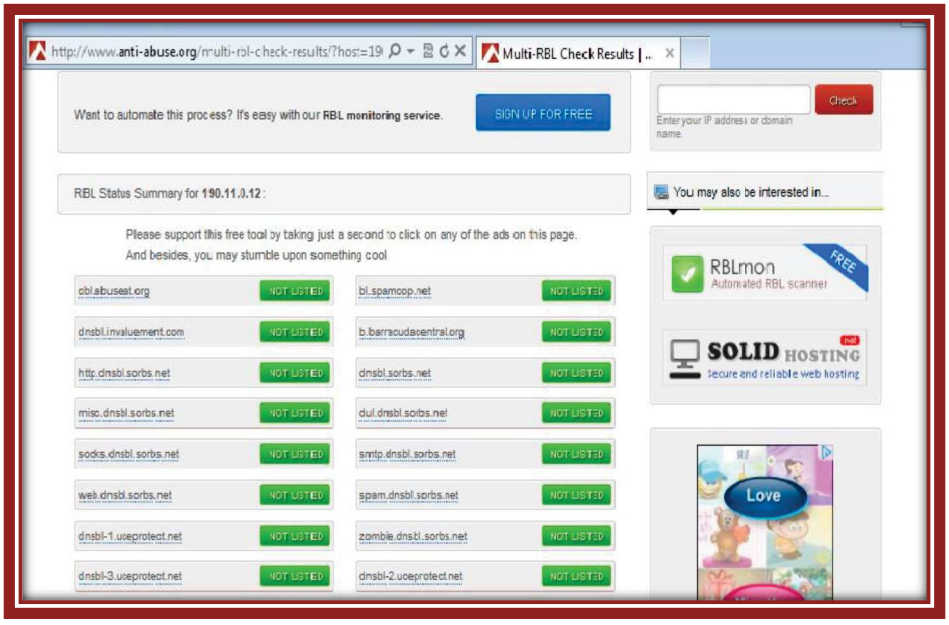


Fig.3.60. Ventana de análisis de Listas negras.

Conclusiones:

Las listas negras registran a las IP´S que envían correo SPAM que es correo basura y es enviado a gran escala, no es solicitado por el usuario y lo perjudica. Para las empresas el SPAM es un gran problema ya que pierden gran parte de su tiempo abriendo archivos publicitarios basura o cuando envían correos a sus clientes estos son catalogados como SPAM y no llegan a su destinatario.

Recomendaciones:

Cuando no se desea recibir o aceptar correo de una dirección IP que le pertenece a una institución de dudosa procedencia se debe realizar una denuncia de SPAM a RBL (Listas Negras Públicas Internacionales).

• Evitar abrir correo basura publicitario y no renviarlo.

• Elegir el ISP de su servidor de correo cuidadosamente en caso de que sea denunciado en la lista negra.

• Eliminar de la base de datos E-Mails incorrectos.

• Poseer un servicio de list higiene que es una aplicación que corrige errores de la base de datos ejemplo johngmail.com cuando debería ser John@gmail.com.

• Tener un servicio en el que el cliente pueda actualizar sus correos.

• Eliminar de la base de datos direcciones de correo SPAM FLAG (Direcciones que se han añadido de manera mal intencionada) y puede hacer que la empresa se auto denuncie en las listas negras ejemplo abuse@somedomain.

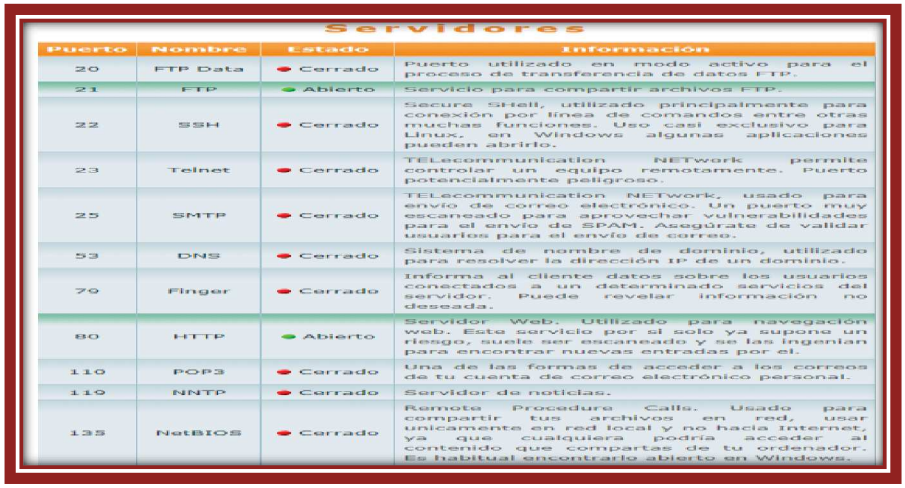
• Evitar crear direcciones de correo con estilos comerciales, con palabras agresivas ejemplo GANE YA, FREE y signos de admiración o símbolos.

3.7 Evaluación de puertos abiertos.

Un puerto es una interfaz física o de software por la cual los datos pueden ser enviados o recibidos. Con el escaneo de puertos se comprobará la seguridad del equipo y que puertos se encuentran abiertos y cerrados para esto se utilizará la página http://www.puertosabiertos.com/

Fig.3.61. Ventana de análisis de la evaluación de puertos.

Existen dos puertos abiertos el 21 que es FTP y EL 80 HTTP.

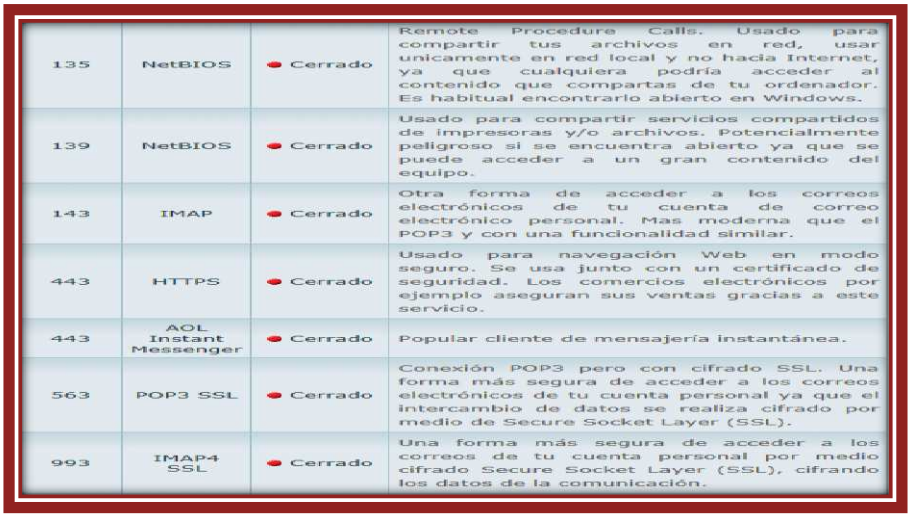


Servidores

Puerto	Nombre	Estado	Información
20	FTP Data	Cerrado	Puerto utilizado en modo activo para el proceso de transferencia de datos FTP.
21	FTP	Abierto	Servicio para compartir archivos FTP.
22	SSH	Cerrado	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	TELecommunication 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 podria acceder al contenido que compartas de tu ordenador. Es habitual encontrarlo abierto en Windows.

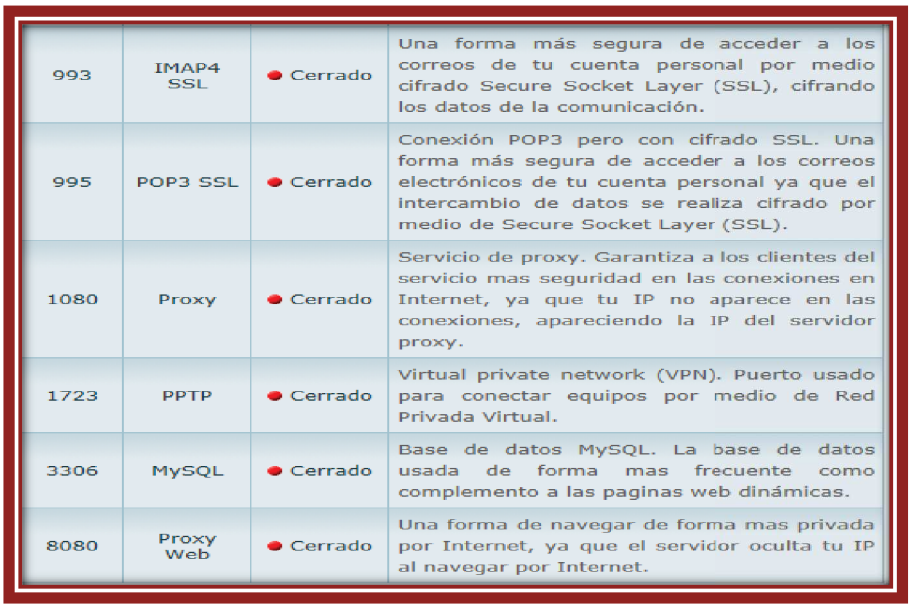
Fig.3.62. Ventana de análisis de los puertos abiertos.

Como se observará en la siguiente figura los puertos están cerrados y no representa ningún peligro como se muestra en la fig.3.63 y 3.64.



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.

Fig.3.63. Ventana de análisis de los puertos abiertos.



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	Cerrado	Base de datos MySQL. La base de datos usada de forma mas frecuente como complemento a las paginas web dinámicas.
8080	Proxy Web	Cerrado	Una forma de navegar de forma mas privada por Internet, ya que el servidor oculta tu IP al navegar por Internet.

Fig.3.64. Ventana de análisis de los puertos abiertos.

Existen puertos que se usan en la comunicación cotidiana que no representan ningún peligro para la comunicación. Windows posee una herramienta llamada Netstat, funciona mediante línea de comandos, con esto se puede conocer exactamente que puertos están abiertos y cuales incluso están recibiendo o transmitiendo información. Para saber que puertos están abiertos se dirigirá al Símbolo de Windows y se digitará: NETSTAT –A o también digitar CMD /K NETSTAT -AN|FINDSTR /C:LISTENING.

Se observará una lista de puertos que se encuentran abiertos y a la espera de alguna conexión.

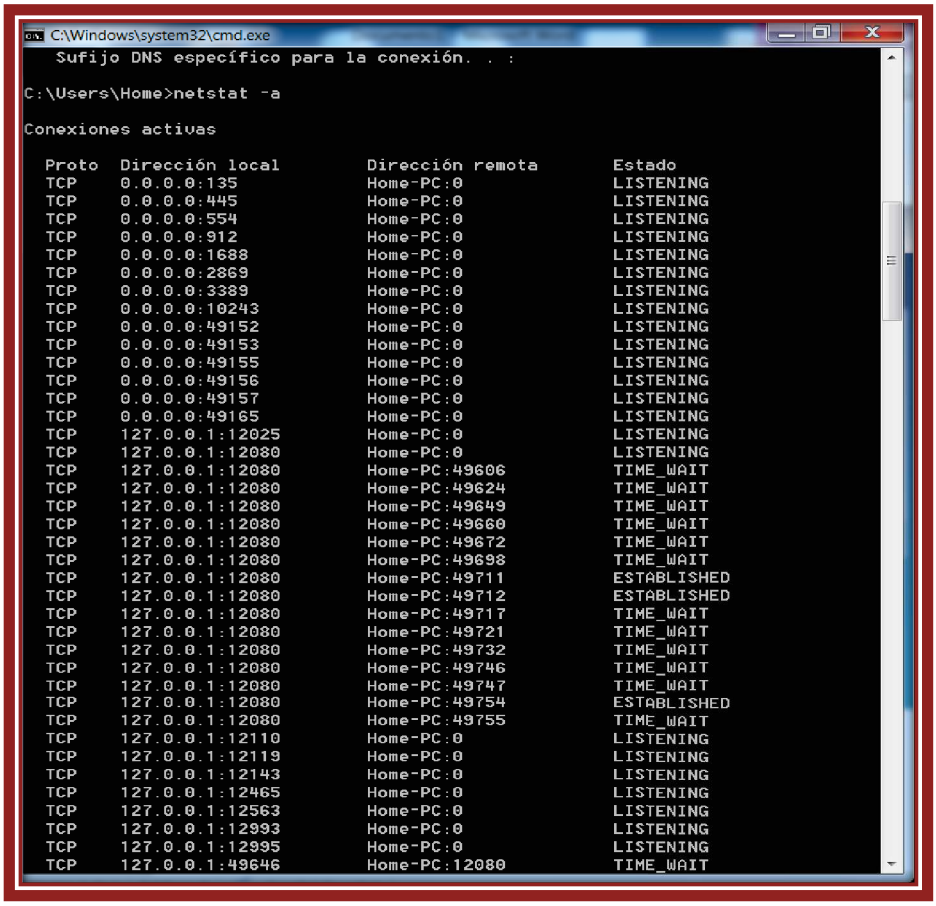


Fig.3.65. Ventana de análisis de los puertos abiertos con el comando Netstad.

Puertos que se encuentran abiertos.

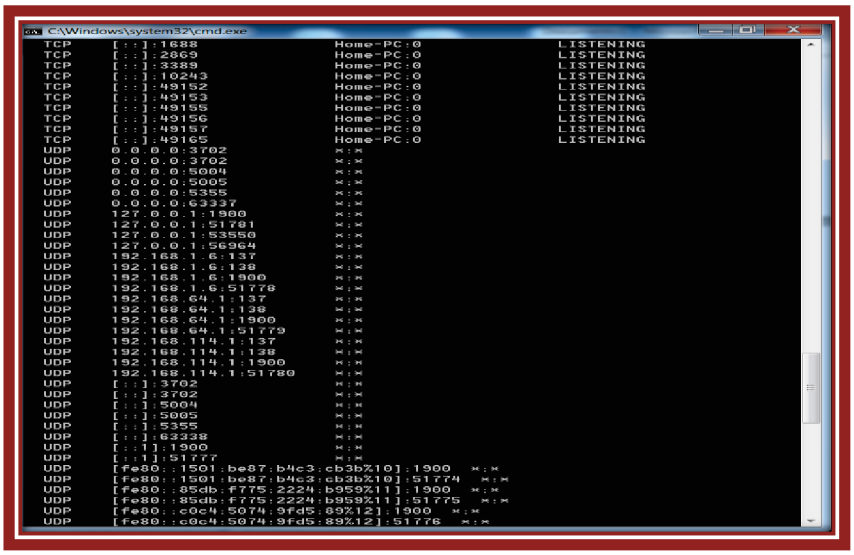


Fig.3.66. Ventana de análisis de los puertos abiertos con el comando Netstad.

Conclusiones:

Existen puertos que son considerados como peligrosos para el sistema si se encuentran abiertos. Un puerto no es abierto por el sistema operativo, sino por un programa específico que quiere usarlo.

Recomendaciones:

Si existen puertos abiertos y se necesita cerrar un puerto se requiere cerrar el servicio o programa que mantiene abierto dicho puerto, no es necesario cerrar todos los puertos manualmente en el sistema ya que si todos los puertos están cerrados no se podrá utilizar el Internet.

Utilizar un Firewall ya que este permite o deniega el trafico protegiendo adecuadamente al host o a la red contra posibles atacantes que se encuentran en el Internet.

3.8 Evaluación del ancho de banda.

El ancho de Banda es la cantidad de información que se envía cuando existe conexión de una red con el Internet, es la cantidad de datos que pueden ser transportados por un medio en un período de tiempo.

Para evaluar el rendimiento se dirigirá a la página http://speedtest.cnt-grms.com.ec/ de acuerdo al plan contratado con el proveedor de Internet es 1.5 Mbps por 256Kb/s de subida y el resultado obtenido es que la velocidad de descarga es 1.63 Mbps y la velocidad de subida es 0.26 Mbps.

Fig.3.67.Análisis del Ancho de Banda utilizando el software de aplicación Cnt.

Fig.3.68. Ventana de análisis del Ancho de Banda utilizando el software de aplicación Speed testnet.

Conclusiones:

El ancho de banda asignado por el proveedor es correcto. El ancho de banda es la transmisión de datos que se envían simultáneamente por una unidad de tiempo. En donde dos o más señales comparten un medio de transmisión. La velocidad, conexión capacidad de acceso son indispensables.

Recomendaciones:

Es recomendable utilizar el test de medidor de ancho de banda para verificar si el proveedor de servicio de Internet cumple con el contrato estipulado y brinda la cantidad de velocidad necesaria de ancho de Banda.

3.9 Evaluación del servidor de correo.

El servidor de correo electrónico tiene clientes de correo que la mayoría de veces reciben correo basura por eso se debe configurar de una manera adecuada el servidor de correo, existen servidores de correos internos y externos en este caso se utilizará el correo de los usuarios que es de correo externo Hotmail para esto se verifica si está abierto el Open Relay o no. Para evaluar el servidor de correo se dirigirá al CMD de Windows y se verificará si está bien configurado el servidor de correo y no existe Open Relay.

Se digitará (telnet www.hotmail.com 25) y enter como se muestra en la fig.3.69 telnet no se reconoce como un comando ejecutable esto sucede porque el cliente telnet no viene instalado por defecto.

Fig.3.69. Ventana del uso del comando telnet.

Se ingresará al Panel de Control de Windows, programas, programas y características y saldrá una ventana donde le indicará activar o desactivar el cliente telnet como muestra la fig. 3.70.

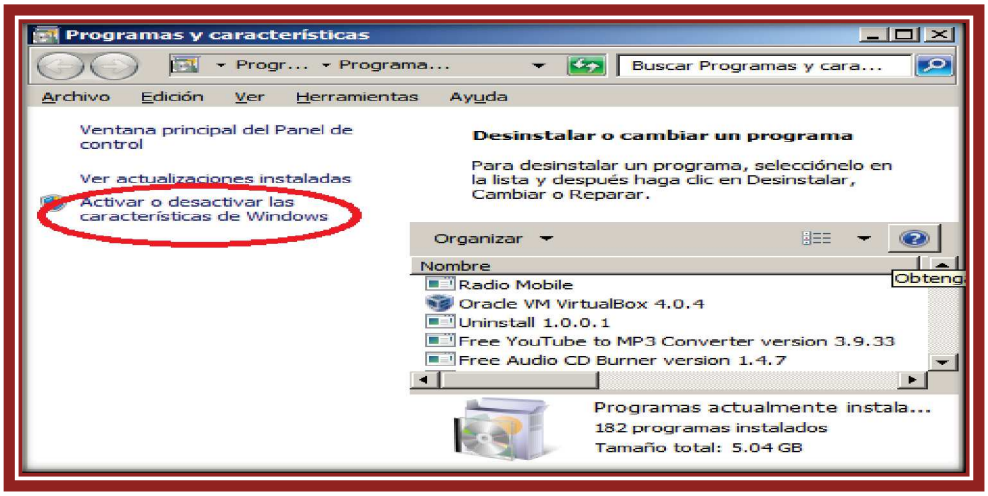


Fig.3.70. Ventana activación de cliente telnet.

Luego aparecerá la siguiente ventana, se pondrá un visto en cliente telnet y luego aceptar.

Fig.3.71. Ventana activación de cliente telnet.

Una vez que está habilitado el cliente telnel se procederá a verificar si el servidor de correo está bien configurado se digitará (telnet www.hotmail.com 25) como se observa en la fig.3.72 no permite la conexión lo que significa que el puerto 25 está cerrado y no existe ningún problema de seguridad.

Fig.3.72. Ventana activación de cliente telnet.

Pero en el caso de que se ingresará y la respuesta de telnet sea favorable se digitará lo siguiente:

helo client.server.com

mail from: bancopichincha@domain.com

rcpt to: jofre-carolinaconstrucciones@hotmail.com

$ telnet www.hotmail.com 25

Salida:

Trying 200.50.x.xxx…

Connected to www.hotmail.com

Escape character is '^]'.

220 www.hotmail.com ESMTP Postfix

helo client.server.com

250 www.hotmail.com

mail from: bancopichincha@domain.com

250 Ok

rcpt to: jofre-carolinaconstrucciones@hotmail.com

554: Relay access denied

Como se puede mostrar la transmisión de correo es denegada y el servidor de correo no tiene Open Relay.

Conclusiones:

Cuando el servidor de correo procesa un mensaje donde ni el remitente ni el destinatario es un usuario local, es decir tanto el destinatario como el remitente están fuera del área local (rango de IP local). Se está apoyando en un correo válido para mandarlo a un tercero esto significa que existe Open Relay en el servidor y no posee las suficientes seguridades que impidan que exista un hueco de seguridad en la red.

Recomendaciones:

• Verificar si la seguridad del servidor de correo externo es adecuado utilizando el test open relay.

• Utilizar un servidor de correo interno ejemplo: Zimbra.

• Usar la consola de comandos con el comando Telnet para verificar si el puerto está abierto y si existen vulnerabilidades al utilizarlo.

3.10 Evaluación de la estética y etiquetado del cableado.

Como se observará a continuación el cableado y etiquetado en los faceplace son inadecuados ya que el punto de red 16 no existe, razón por la cual existían conflictos cuando terceras personas configuraban la red asignado este punto como válido y la manera en la que está escrita su nomenclatura es incorrecta lo adecuado es utilizar una rotuladora la misma que posee una cinta adhesiva e imprime la información necesaria P3-DO2 lo que significa que en el piso 3 existe el punto de datos número 2 como se muestra en la fig.3.73

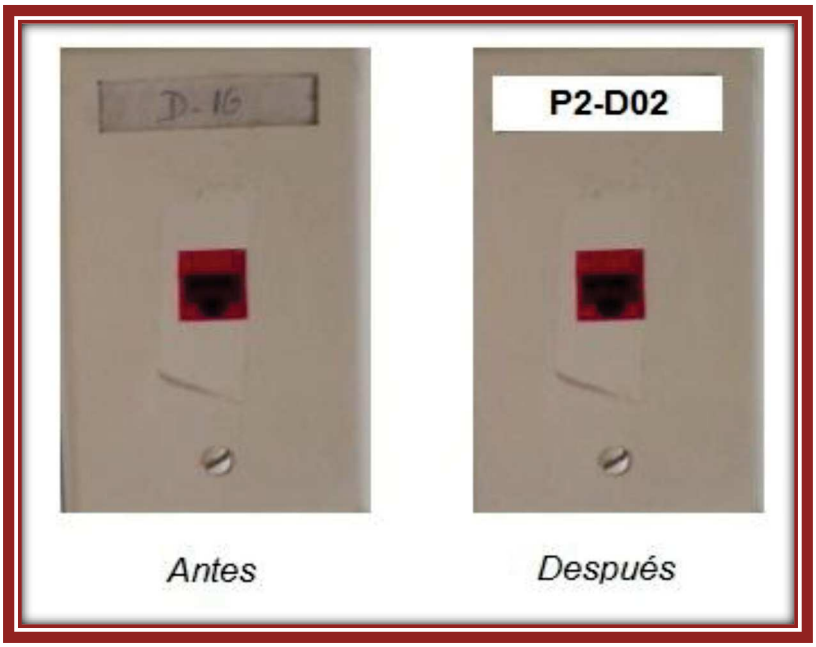


Fig.3.73. Etiquetado en los face place antes y después.

En la siguiente fig.3.74 se muestra como en el pach panel se utilizan cables de Ethernet categoría 5E que son demasiado grandes esto no es óptimo ya que existen cables de hasta 3 metros sobre pasan el tamaño que se necesita, esto hace que la estética sea pésima por lo que lo es recomendable utilizar pachcords de un metro y colocar una tapa plástica para cubrir el pach panel.

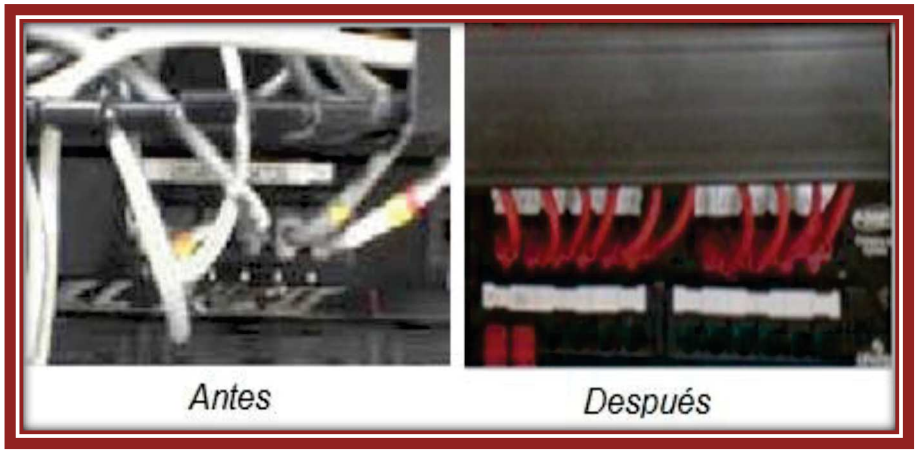


Fig.3.74. Estética de los pachcords en el pach panel.

Conclusiones:

Es primordial mantener un orden adecuado con los cables de red, con su respectiva nomenclatura, utilizar accesorios como canaletas Dexon para el paso de los cables no solo por la estética sino también porque de esa forma se cumple con las normas de seguridad y optima eficiencia en la red.

Tener un entorno agradable de trabajo facilita la administración de la red y permite corregir de manera eficiente y rápida posibles errores que se presenten en el futuro.

Recomendaciones:

• Siempre utilizar cajas y canaleta Dexon para el paso de los cables de red.

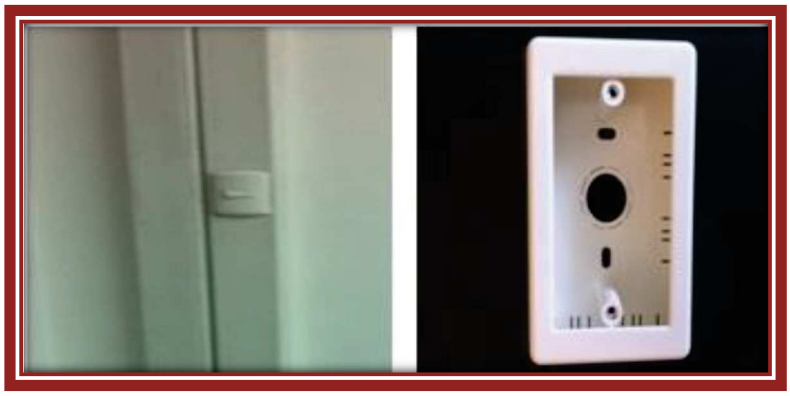


Figura .3.75. Canaleta y cajas Dexon.

- Utilizar pach cords adecuados en tamaño en el pach panel.

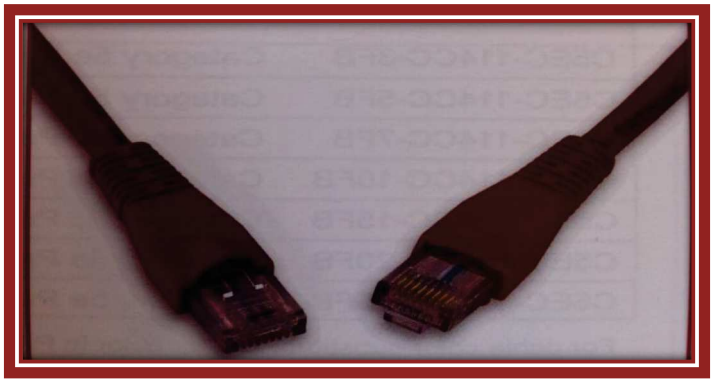


Fig. 3.76. Pachcords

• Utilizar en el pach panel y organizador de rack para mantener ordenados los cables de red en el cuarto de equipos.

Fig.3.77. Pach panel y organizador de rack

• Etiquetar los cables y los faceplace con el número de red al que pertenecen.

4. Capítulo IV Análisis de Resultados de la Auditoria de red.

4.1 Resultado del análisis y elaboración del plano de red.

La siguiente estructura de red es la adecuada para la empresa debido al mal Subneteo e inadecuada asignación de Direcciones IP que existen y se tienen conflicto con las direcciones IP que posee.

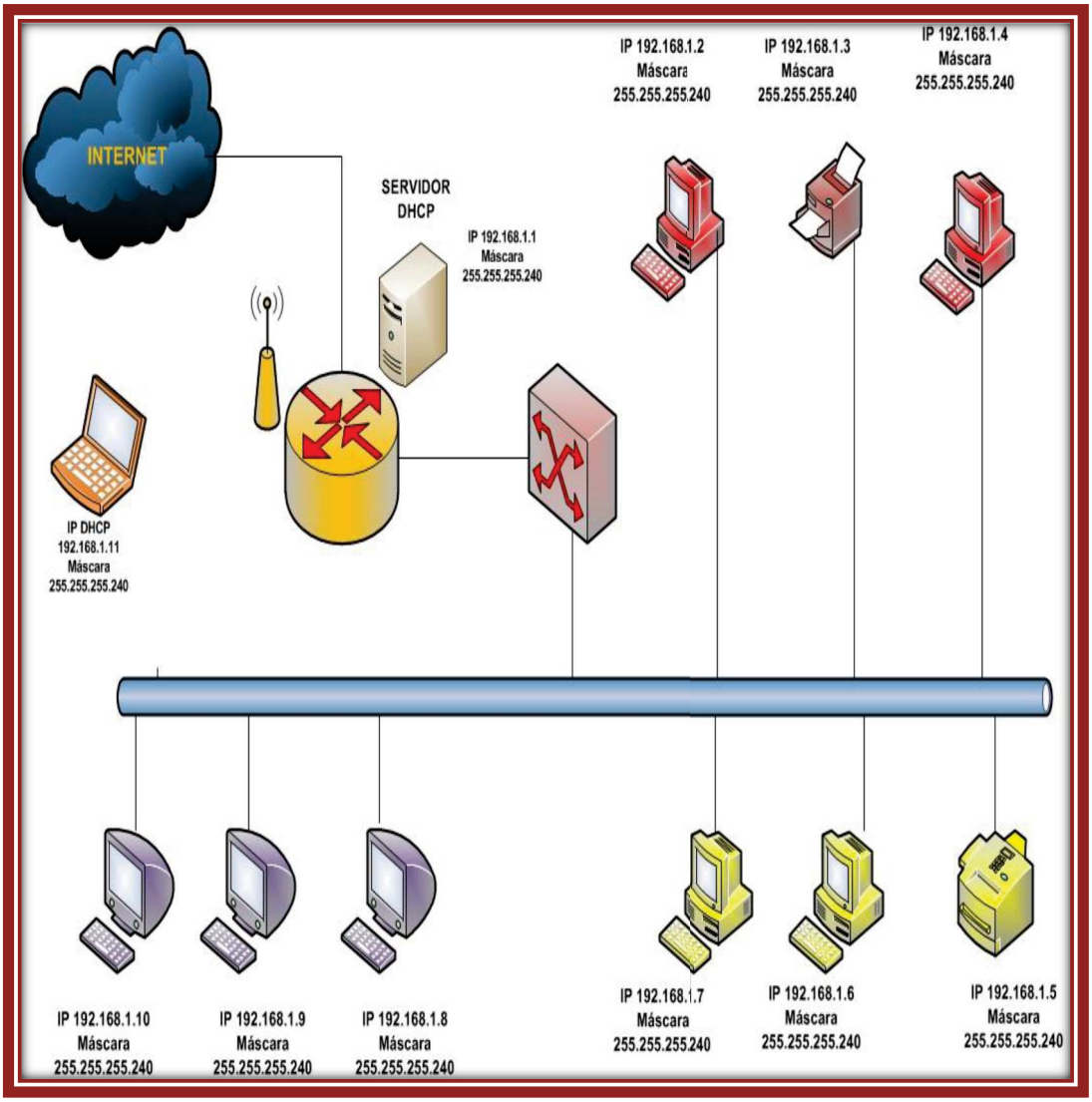


Fig.4.1 Diseño de estructura adecuada de la red.

Autor: Johanna S. Chicaiza Pineida. 08/07/2012

Existen 8 estaciones de trabajo más 2 puntos de datos para las impresoras por lo que en total se necesitan 10 puntos de datos, pero se encontró este direccionamiento IP 192.168.1.2/29 con máscara 255.255.255.248 que es óptimo solo para 6 estaciones de trabajo motivo por el cual no se pueden comunicar los Host entre sí. Realizando el debido cálculo para 10 estaciones de trabajo se tiene el rango adecuado que es 192.128.1.2/28 con máscara 255.255.255.240. y sirve para 14 estaciones de trabajo.

El cálculo se realiza de la siguiente manera utilizando la siguiente fórmula:

M= máscara de subred # IP´S= Número de IP´S

256 =constante

Se requiere trabajar con 10 estaciones de trabajo por lo que se tiene que utilizar la siguiente tabla:

Tabla.4.1 Diseño de estructura adecuada de la red.

Se debe utilizar el número 16 para 10 puntos de red por lo que se tiene el número de la subred que es 16 por lo tanto.

La fórmula para calcular el número de subredes es:

Subredes = 256 / # IP´S entonces:

16 = 256 / # IP´S

IP´S = 256 / 16 entonces: # IP´S = 16

Máscara = 256 - # IP´S

Máscara = 256 – 16

Máscara = 240

Entonces el direccionamiento IP es:

0 - 15

El rango de IP´S utilizables son:

1 – 14 porque la # 0 es de red y la 16 es de Broadcast.

Con este adecuado rango de IP´S se solucionó el problema de conectividad en la red y los conflictos que existían por duplicación de IP´S debido a las inadecuadas direcciones IP y máscaras que existían.

4.2 Resultados del análisis del servidor DHCP.

Resultado del análisis del servidor DHCP, en el Router viene por defecto habilitado el servidor DHCP este se encarga de asignar IP´S de manera automática a las nuevas computadoras que se conectan a la red ya sea vía inalámbrica o por conexión fija.

Se detectaron los siguientes problemas el servidor DHCP ,asigna direcciones IP en forma dinámica a los Hosts, pero existen otros que tienen configurado su dirección IP de manera manual. Esto no es recomendable ya que si el servidor DHCP se conecta con otros Hosts, que se integran a la red local a través del WIRELESS y existen IP´S duplicadas se pierde la comunicación. Debido a que DHCP no es inteligente y no asigna direcciones IP a los Hosts de manera permanente ya que tiene un tiempo de vida, que dura mientras exista comunicación con la red local en el instante en que el Hosts se desconecta de la red o se apaga la dirección IP regresa al servidor DHCP y esta estará lista para dársela a otro Hosts que solicite una IP. Pero al momento en que la PC comience a trabajar no podrá estar en red con las demás debido a que su IP ya está utilizada por otra PC. Se resolvió este problema utilizando IP fijas en los Host y en las portátiles se utilizó IP´s con DHCP.

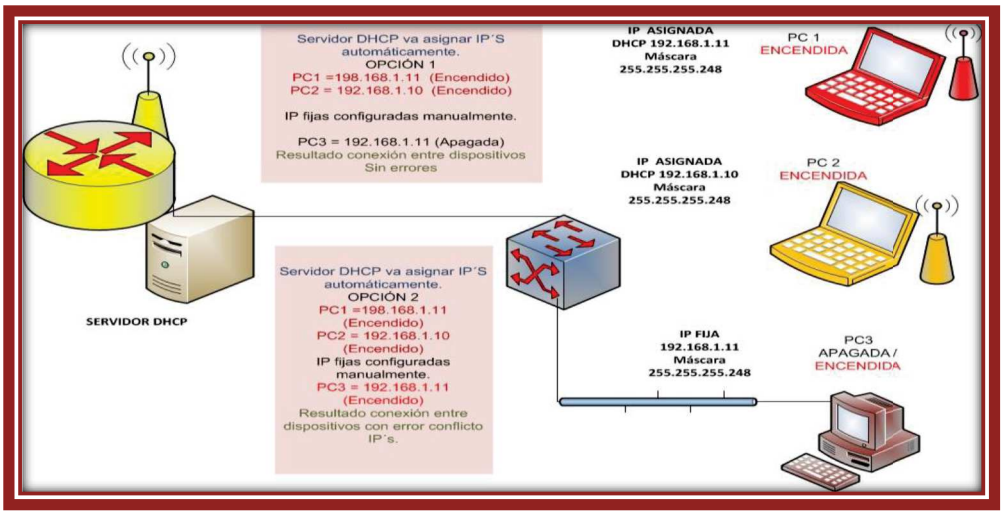


Fig.4.2 Conflictos servidor DHCP.1

Autor: Johanna S. Chicaiza Pineida. 23/07/2012

4.3 Resultado del análisis del servidor de correo.

Existen muchas vulnerabilidades, al no poseer una cuenta de correo interno y esto se debe a que pueden ingresar software mal intencionado a través del correo y causar daño al sistema. También por la gran cantidad de correo basura que día a día llegan al usuario por correo y es una pérdida de tiempo para el usuario abrirlo y chequearlo.

Se realizó el TEST OPEN RELAY y la utilización del comando Telnet que sirven para detectar si el servidor de correo está bien configurado o no y si evita los correos Spam. Se constato que no existen problemas con el servidor de correo externo de Hotmail y no representa un peligro para la administración, por lo que no se realizó ningún cambio.

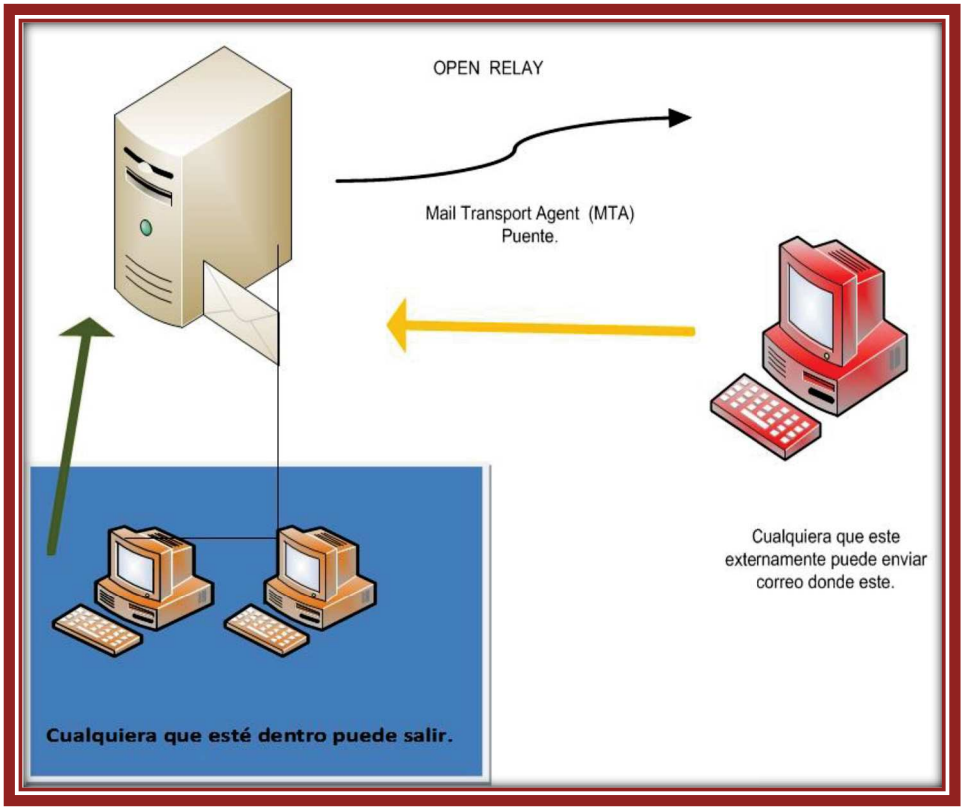


Fig.4.3 Open Relay.

Autor: Johanna S. Chicaiza Pineida. 23/07/2012

4.4 Resultado del análisis del sistema operativo.

En los siguientes diagramas se constatará la cantidad de máquinas que utilizan los diferentes sistemas operativos.

Fig.4.4 Análisis del sistema operativo.

Autor: Johanna S. Chicaiza Pineida. 08/08/2012

Se analizó el porcentaje total del Licenciamiento de Windows XP y Windows 7.

Fig.4.5 Licenciamiento de los sistemas operativos.

Autor: Johanna S. Chicaiza Pineida. 08/08/2012

A continuación se observará que para el sistema operativo XP el 33% de los quipos no tienen licenciamiento y el 67% tiene licenciamiento.

Fig.4.6 Licenciamiento del Sistema Operativo XP.3

Autor: Johanna S. Chicaiza Pineida. 12/09/2012

Como se muestra en la fig.4.7 en el sistema operativo Windows 7 el 40 % no es licenciado y el 60% si es licenciado.

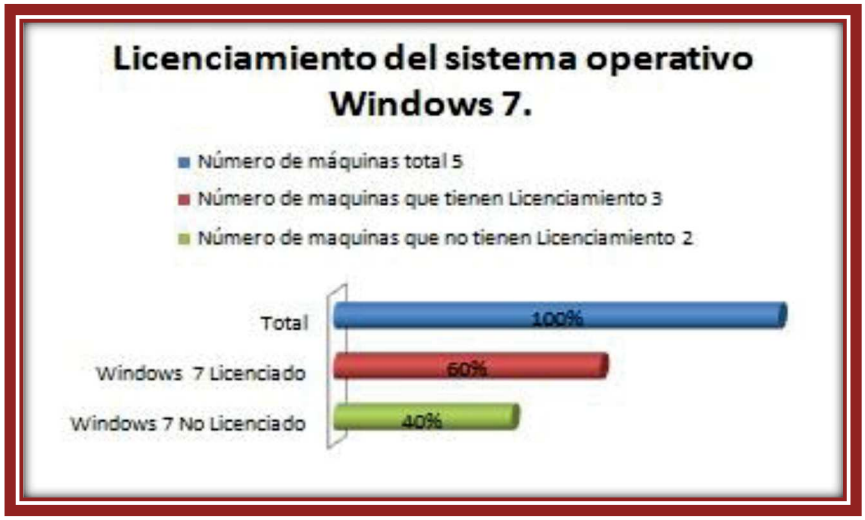


Fig.4.7 Licenciamiento del sistema operativo Windows7.

Autor: Johanna S. Chicaiza Pineida. 12/09/2012

4.5 Resultado del análisis el software de Aplicación.

Se observará que existe un porcentaje de software Licenciado, Libre y No Licenciado.

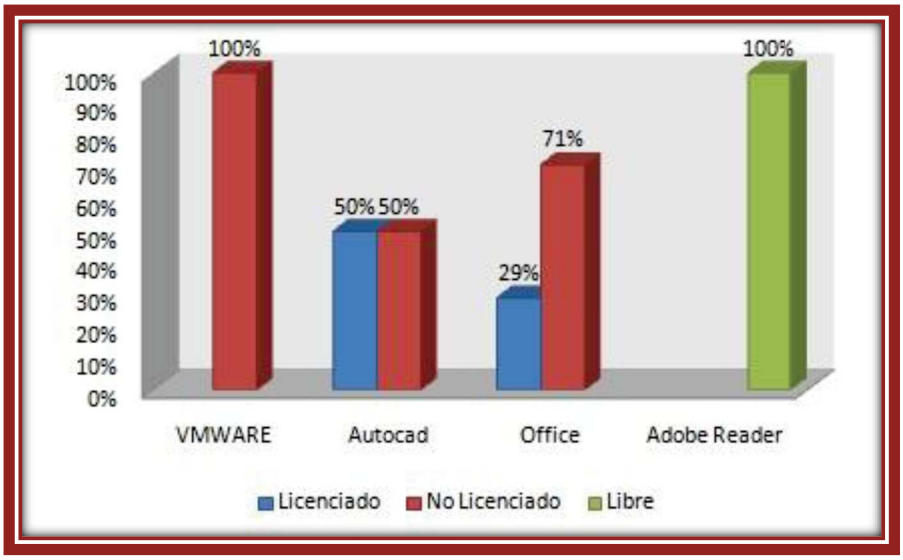


Fig.4.8 Software de Application.

Autor: Johanna S. Chicaiza Pineida. 12/09/2012

4.6 Resultado del análisis del antivirus.

La siguiente ilustración indicará el porcentaje total de cada una de las marcas de antivirus instalado, el porcentaje del licenciamiento del antivirus Eset Nod32.

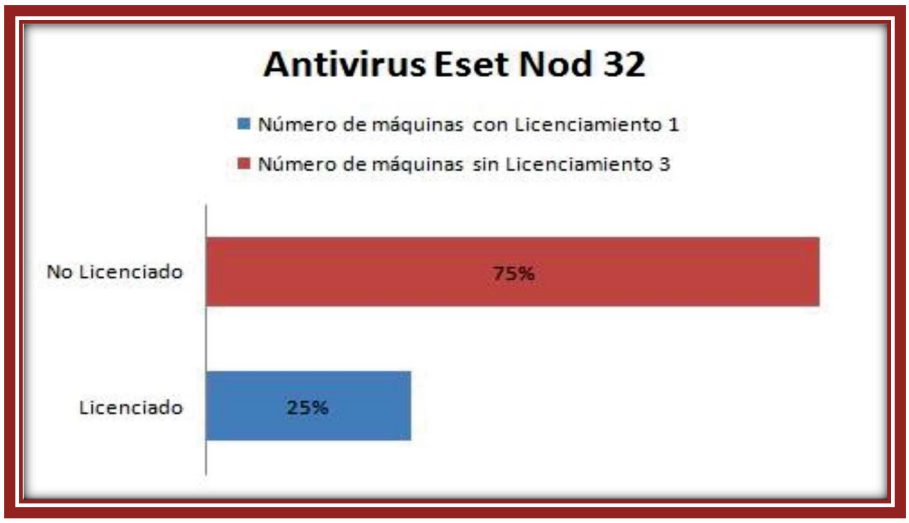


Fig.4.9 Antivirus ESET Nod. 1

Autor: Johanna S. Chicaiza Pineida. 12/09/2012

El porcentaje del antivirus AVAST es en un 100% libre.

Fig. 4.10 Antivirus Avast.

Autor: Johanna S. Chicaiza Pineida. 15/10/2012

4.7 Resultado de la Prueba de Eicar.

Al realizar las pruebas de Eicar con los antivirus Avast y Eset Nod 32, se comprobó que los antivirus pasaron las pruebas y ratificaron que tan robustos son ante la posible presencia de software malicioso y virus en este caso ninguno permitió abrir archivos dañinos ya que ambos impidieron su ejecución y los pusieron en cuarentena cumpliendo con todas las pruebas como se muestra en la fig.4.11.

Fig. 4.11. Pruebas del Eicar.

Autor: Johanna S. Chicaiza Pineida. 15/10/2012

4.7.1 Resultado del análisis de la certificación del cableado.

El cableado de la red cumplen ciertos parámetros que son correctos como en el uso de FACEPLACE conectores RJ45 Cat. 5E, canaletas para el paso del cable, pero en cuanto la estética y orden del rack no se respetan ciertas normas de etiquetado y adecuada ubicación de los cables y dispositivos.

No se cuenta con una certificación de Red del cableado estructurado debido a la falta de información por el personal.

Se mejoró la estética de los cables y se cambió los patch cords así como se mejoró el etiquetado de la nomenclatura en los face place, no se realizaron otros cambios debido a que no existía presupuesto y por el posible cambio de domicilio de la empresa.

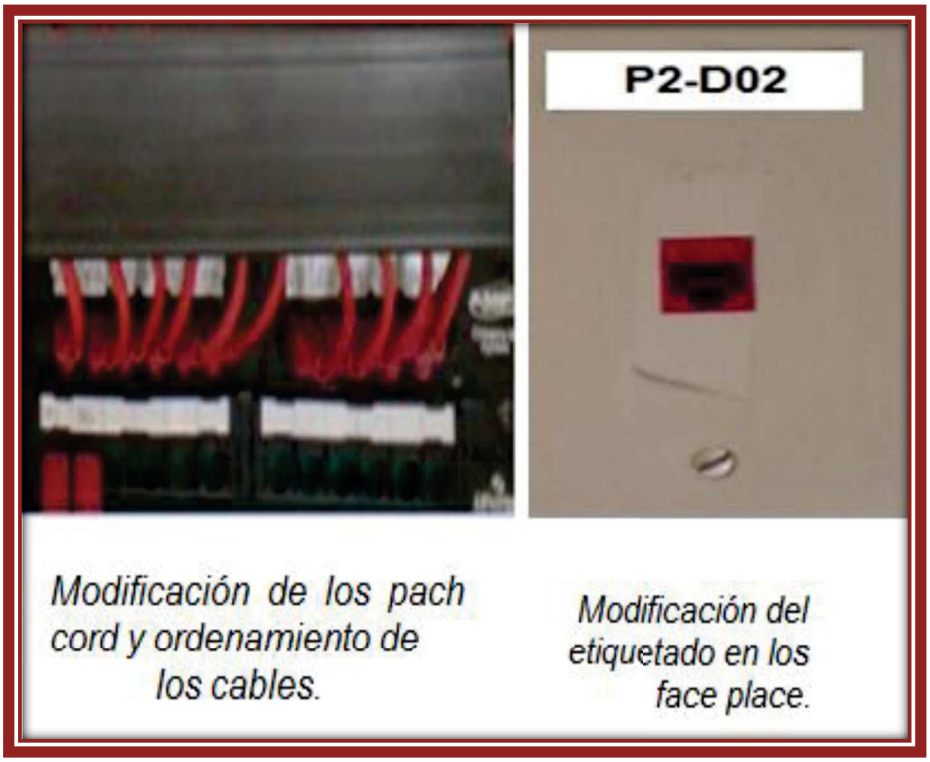


Fig. 4.12. Modificación de los cables y etiquetado de los cables.

Autor: Johanna S. Chicaiza Pineida. 15/10/2012

4.8 Resultado del análisis de la Administración de red.

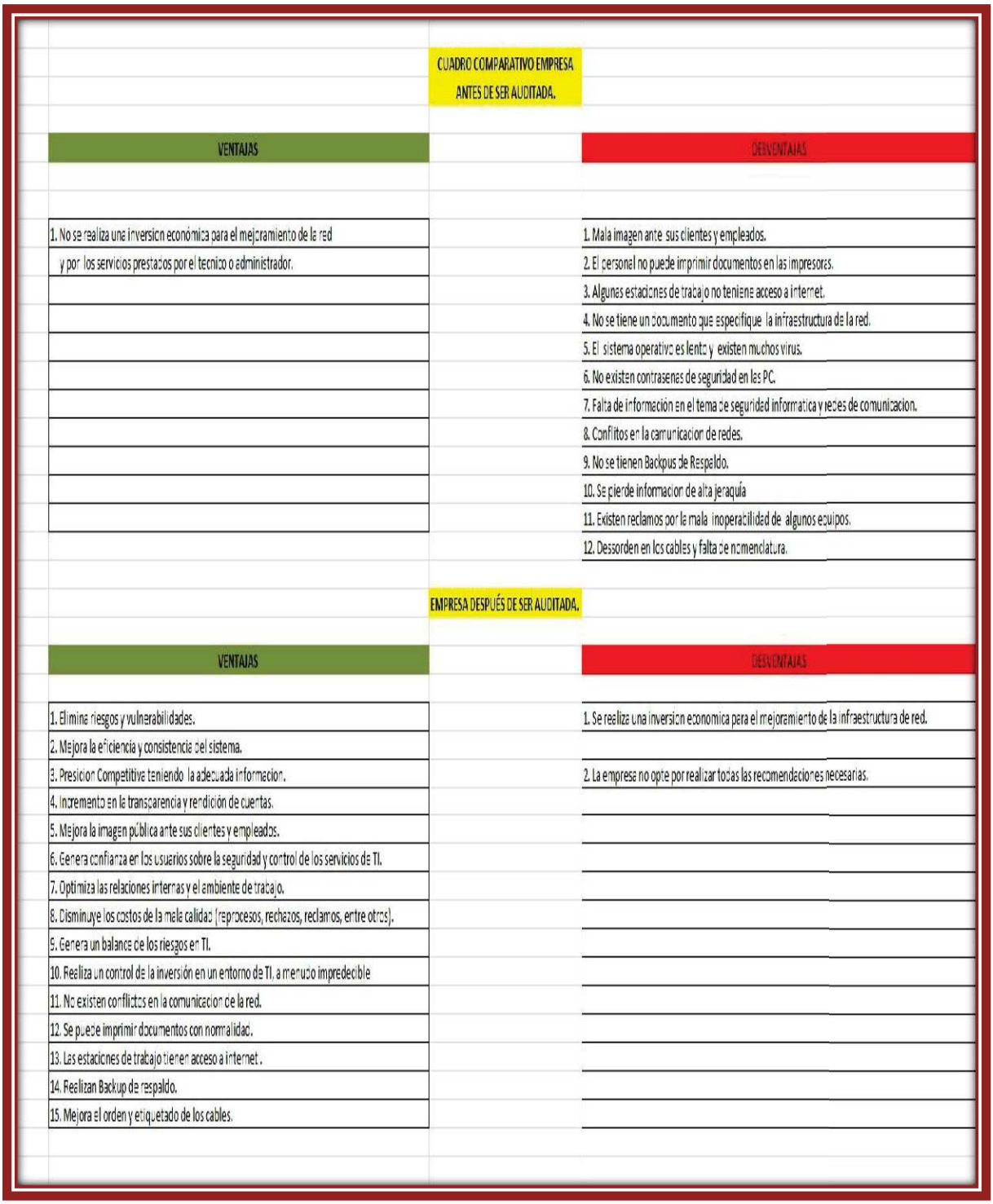
Se tiene una difícil Administración de la Red ya que se utiliza servicios tercerizados por diversas empresas que proveen del servicio de Internet. Generalmente no se realiza una adecuada configuración y constantes actualizaciones de software, debido a esto se cambiaron las contraseñas y se crearon cuentas de usuarios seguras para las máquinas, no se instaló ni se desinstaló ningún programa a petición de la empresa.

4.9 Documento Informativo de la actual estructura de la red.

EQUIPOS	CARACTERISTICAS	
	Nombre de Usuario	Nomenclatura de los puntos de red.
PC 1 Gerencia	Gerencia (usuario Administrador)	P3 - 02
PC 2 Secretária	Secretária (usuario estandar)	P3 - 04
PC 3 Departamento Diseño	Departamento Diseño (usuario estandar)	P3 - 06
PC 4 Departamento Diseño	Departamento Diseño (usuario estandar)	P3 - 07
PC 5 Departamento Técnico	Departamento Técnico (usuario estandar)	P3 - 08
PC 6 Departamento Técnico	Departamento Técnico (usuario estandar)	P3 - 09
PC 7 Departamento Técnico	Departamento Técnico (usuario estandar)	P3 - 10
PC 8 Invitados	Invitados (usuario estandar)	P3 - 11
Impresora IP 1		P3 - 03
Impresora IP 2		P3 - 05

Fig. 4.13. Tabla de usuarios y nomenclatura de red. 1

Autor: Johanna S. Chicaiza Pineida. 25/10/2012



CUADRO COMPARATIVO EMPRESA ANTES DE SER AUDITADA.

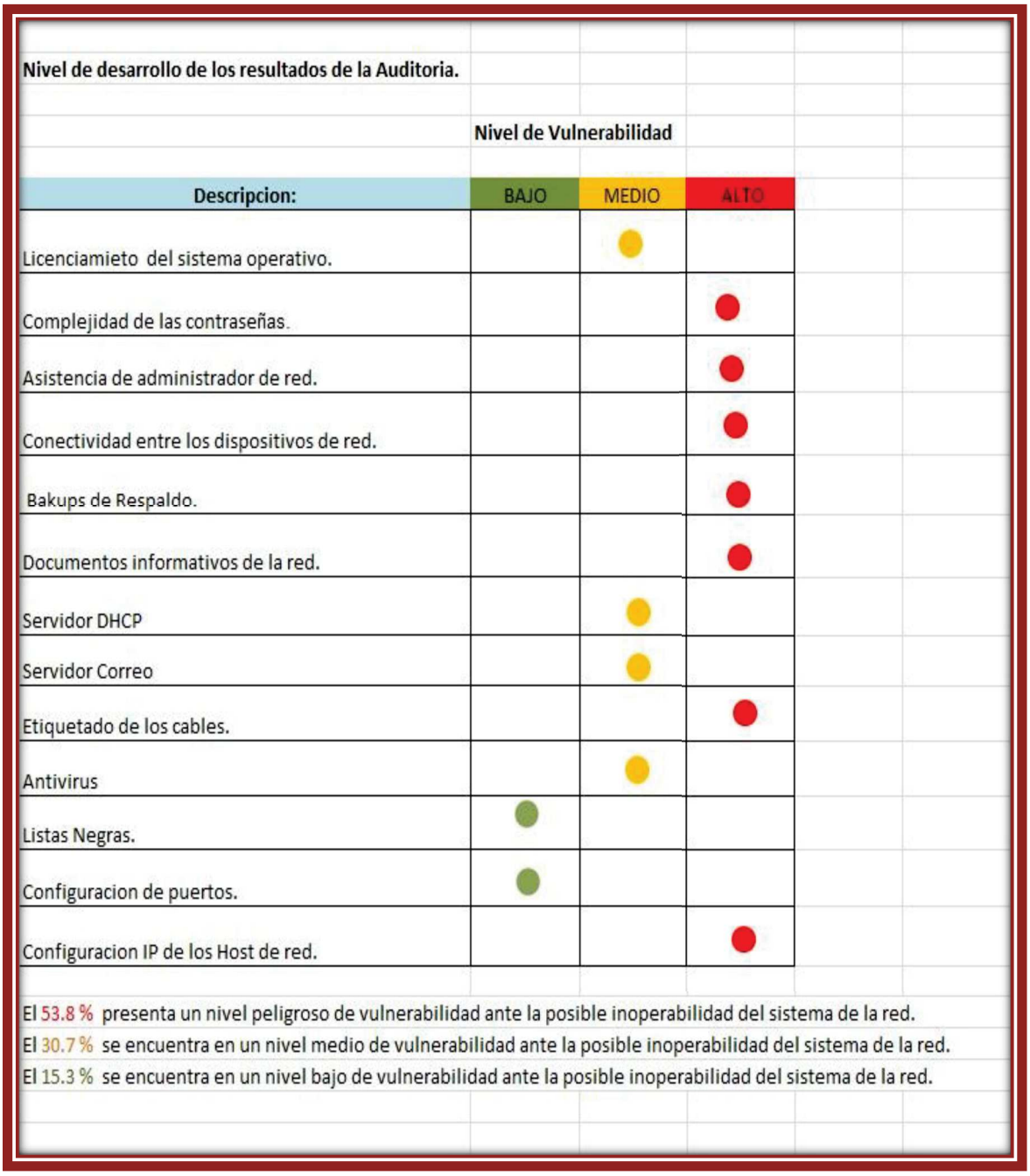
VENTAJAS	DESVENTAJAS
1. No se realiza una inversion económica para el mejoramiento de la red y por los servicios prestados por el tecnico o administrador.	1. Mala imagen ante sus clientes y empleados.
	2. El personal no puede imprimir documentos en las impresoras.
	3. Algunas estaciones de trabajo no tienen acceso a internet.
	4. No se tiene un documento que especifique la infraestructura de la red.
	5. El sistema operativo es lento y existen muchos virus.
	6. No existen contrasenas de seguridad en las PC.
	7. Falta de información en el tema de seguridad informatica y redes de comunicacion.
	8. Conflitos en la camunicacion de redes.
	9. No se tienen Backpus de Respaldo.
	10. Se pierde informacion de alta jeraquía
	11. Existen reclamos por la mala inoperacilidad de algunos equipos.
	12. Dessorden en los cables y falta de nomenclatura.

EMPRESA DESPUÉS DE SER AUDITADA.

VENTAJAS	DESVENTAJAS
1. Elimina riesgos y vulnerabilidades.	1. Se realiza una inversion economica para el mejoremiento de la infraestructura de red.
2. Mejora la eficiencia y consistencia del sistema.	
3. Presicion Competitiva teniendo la adecuada informacion.	2. La empresa no opte por realizar todas las recomendaciones necesarias.
4. Incremento en la transparencia y rendición de cuentas.	
5. Mejora la imagen pública ante sus clientes y empleados.	
6. Genera confianza en los usuarios sobre la seguridad y control de los servicios de TI.	
7. Optimiza las relaciones internas y el ambiente de trabajo.	
8. Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, entre otros).	
9. Genera un balance de los riesgos en TI.	
10. Realiza un control de la inversión en un entorno de TI, a menudo impredecible	
11. No existen conflictos en la comunicacion de la red.	
12. Se puede imprimir documentos con normalidad.	
13. Las estaciones de trabajo tienen acceso a internet.	
14. Realizan Backup de respaldo.	
15. Mejora el orden y etiquetado de los cables.	

Fig. 4.14. Cuadro Comparativo antes y después de la auditoria. 1

Autor: Johanna S. Chicaiza Pineida. 22/11/2012



Nivel de desarrollo de los resultados de la Auditoria.

Descripcion:	Nivel de Vulnerabilidad BAJO	MEDIO	ALTO
Licenciamieto del sistema operativo.		●	
Complejidad de las contraseñas.			●
Asistencia de administrador de red.			●
Conectividad entre los dispositivos de red.			●
Bakups de Respaldo.			●
Documentos informativos de la red.			●
Servidor DHCP		●	
Servidor Correo		●	
Etiquetado de los cables.			●
Antivirus		●	
Listas Negras.	●		
Configuracion de puertos.	●		
Configuracion IP de los Host de red.			●

El 53.8 % presenta un nivel peligroso de vulnerabilidad ante la posible inoperabilidad del sistema de la red.
El 30.7 % se encuentra en un nivel medio de vulnerabilidad ante la posible inoperabilidad del sistema de la red.
El 15.3 % se encuentra en un nivel bajo de vulnerabilidad ante la posible inoperabilidad del sistema de la red.

Fig. 4.14. Cuadro Nivel de Vulnerabilidades. 1

Autor: Johanna S. Chicaiza Pineida. 25/11/2012

CONTROLES	SI	NO	N/A
Existen planes a largo plazo para el departamento de informática.		7	
Valore la conexión de estos planes con planes generales de la empresa.			*
Cubren los planes del D.I. los objetivos a largo plazo de la empresa, valórelo.		7	
Existen un comité de planificación o dirección del departamento de informática.		*	
Dicho comité está compuesto por directivos de departamento de usuario.		*	
Existe en dicho comité algún miembro con conocimientos informáticos exhaustivos.		*	
El comité realiza algún tipo de estudio para analizar la coherencia de su departamento de información con los avances tecnológicos.		*	
Qué importancia le asigna la dirección de la empresa al comité/dirección de informática.		*	
Existe una adecuada vía de comunicación y control de cumplimiento de objetivos a corto y largo plazo por parte de la dirección.		*	
Existen políticas para la planificación, control y evaluación del D.I.		*	
Existen estándares que regulen la explotación de recursos del D.I.		*	
Existen procedimientos sobre las responsabilidades, peticiones de servicio y relaciones entre los diferentes departamentos y el D.I.	*		
Dichos procedimientos están adecuadamente distribuidos en los diferentes departamentos.		*	
Evalué el cumplimiento de dichos procedimientos por parte de los diferentes departamentos. (ponga el resultado en no) 1 -10		4	
El D.I está separado orgánicamente en la estructura orgánica de la empresa.		*	
Es independiente la ubicación del D.I. de los otros departamentos de la empresa.	*		
Están separadas las unidades de desarrollo de sistemas y explotación.			*
Están separadas las unidades de explotación y control de datos.		*	
Están separadas las unidades de administración de bases de datos y desarrollo de sistemas.		*	
Evalué la independencia de las funciones del personal entre las diferentes unidades. (ponga el resultado en no)1 -10		7	
¿Existe una descripción por escrito(manual de operaciones y			

procedimientos)de cada puesto de trabajo en las diferentes unidades de D.I.		*	
¿La descripción del puesto de trabajo incluye definiciones de conocimientos y pericia técnicos?		*	
¿Los manuales de operaciones y procedimientos pasan una revisión mínima anual?		*	
¿Existe un método de evaluación para cubrir las vacantes del D.I.?		*	
Evalué la adecuación del método y políticas de selección para cubrir las antedichas vacantes. (ponga el resultado en n/a)			*
Evalué la conformidad del personal del D.I. con las políticas y el sistema de selección.			*
¿Existe algún método de control y evaluación de consecución de objetivos de cada puesto de trabajo?		*	
¿Existe una lista de aplicaciones de tratamiento de datos cuya explotación está programada regularmente?		*	
¿Se especifica en dicha lista tiempos de preparación y tratamiento?		*	
¿Existe algún sistema de control para la carga de trabajo de D.I.?		*	
¿Ha establecido el D.I. prioridades de tratamiento de los diferentes trabajos?		*	
Evalúe la carga de trabajo del D. I. en época baja de proceso (ponga el resultado en no)		4	
Evalúe la carga de trabajo del D.I en época alta de proceso (ponga el resultado en si).	7		
Evalúe la capacidad de los equipos disponibles para satisfacer la demanda en la época alta de proceso (resultado en sí).	7		
Evalúe el exceso de capacidad de los equipos disponibles para la satisfacer la demanda en la época baja de proceso(resultado en no)		4	
¿Qué valoración le dan los trabajadores del área de explotación a la disponibilidad de equipo en época alta de trabajo (resultado positivo en si y resultado negativo en no)?	14	8	
Evalúe la capacidad de los recursos humanos para satisfacer la demanda en la época alta de proceso(resultado en si)	7		
Evalúe el exceso de capacidad de los recursos humanos disponibles para satisfacer la demanda en la época baja de proceso(resultado en no).		7	
¿Qué valoración le dan los trabajadores del área de explotación a la disponibilidad de recursos humanos en época altas de trabajo(resultado positivo en si y resultado negativo en no)?	7	7	

¿Existe un calendario de mantenimiento preventivo a las PCS?		*	
¿Se verifica que dicho calendario no incluya revisiones en periodos de carga alta de trabajo?		*	
¿Realizar la dirección del D.I. un control y seguimiento del flujo de trabajo y de las variaciones del calendario de explotación?		*	
¿Se registran las variaciones del calendario de explotación?		*	
¿Existe un procedimiento para evaluar las causas de los problemas de tratamientos de datos?		*	
¿Existe un registro de problemas de tratamiento de datos?		*	
¿Se toman acciones directas para evitar la recurrencia de los problemas de tratamiento de datos?		7	
¿existe una preasignacion para la solución de problemas específicos de tratamiento de datos?	4		
¿Se ha determinado una prioridad en la resolución de problemas de tratamiento de datos?		7	
¿Existe un inventario de contenido de la biblioteca de soportes?		*	
¿Identifican las etiquetas de los soportes: nombre de archivo, fecha de creación, programa que lo creo y periodo de retención de soporte?		*	
¿Existe algún sistema de control de entrada y salida de la biblioteca de soporte?			
Evalúe la satisfacción de los usuarios de software respecto a la última adquisición?.			*
¿Existe algún procedimiento de prueba antes de efectuar cambios de logical de sistemas?		*	
¿Existe alguna persona especializada en implementación de logical de sistemas?		*	
¿Existe algún registro sobre los cambios realizados sobre el logical de sistemas?		*	
¿Existe algún registro de problemas de logical de sistemas?		*	
¿Se identifican y registran exhaustivamente la gravedad de los problemas de logical de sistema, la causa y su resolución?		*	
¿Existen procedimientos de control generales de la red de informática distribuida?		*	
¿Se realizan dichos procedimientos de control con una periodicidad mínima mensual?		*	
¿Ha establecido el departamento de informática, desde la implantación de la red, un mecanismo para asegurar la compatibilidad de conjunto de datos entre aplicaciones al crecer la misma?		*	

¿Están adecuadamente canalizadas las peticiones de cambios de procedimientos operativos de la red de I.D.?		*	
¿Existe algún control sobre cambios autorizados o no en los procedimientos operativos de la red?		*	
¿Son analizados los cambios de los procedimientos operativos para ver si responden a necesidades reales de los usuarios?		*	
¿Ha establecido el departamento de informática controles sobre utilización de los contenidos de las bases de datos de la red?		*	
¿Está asegurado el control del cambio de definición de datos comunes de las bases?		*	
¿Existe un sistema eficaz para evitar que los usuarios cambien la definición de datos comunes de las bases?		*	
¿Existe una comunicación regular sobre cambios efectuados en las bases de datos comunes?		*	
¿Existe algún sistema de control que asegure la compatibilidad de los contenidos de las bases de datos de la red?		*	
¿Existen controles establecidos por el departamento de informática sobre utilización de contenido de las bases de datos de la red?		*	
¿Existe algún control que asegure que los cambios introducidos en los contenidos de la base de datos mantienen la compatibilidad de dichas bases?		*	
¿Existe algún procedimiento establecido que asegure en todos los puntos de la red que los cambios críticos en los contenidos de las bases se lleven a cabo con puntualidad?		*	
¿Se ha establecido una política para identificación y clasificación de datos sensibles de la red?		*	
¿Existen mecanismos de seguridad que impidan introducciones o modificaciones erróneas de daños sensibles?		*	
¿Existe algún mecanismo de control que asegure una adecuada carga de la red especialmente en los periodos de trabajo crítico?	*		
¿Se han establecido y comunicado a los usuarios procedimientos efectivos para coordinar la operación de los programas de aplicación y la utilización de los contenidos de las B.D?		*	
¿Poseen todos los usuarios de la red especificaciones sobre disponibilidades, horarios, tiempo de respuesta, almacenamiento, respaldo y control operativo?		*	
¿Se realizan reuniones periódicas entre los usuarios para coordinar calendarios de explotación, especificaciones de tratamiento y procedimientos operativos?		*	
¿Establecen todas las instalaciones de departamentos usuarios de la red previsiones sobre necesidades de material fungible?	*		

¿Existe siempre un remanente de material fungible que asegure la continuación de los procesos, en los departamentos usuarios?	*		
¿Existen procedimientos establecidos por el departamento de informática para la gestión y control del logical de comunicaciones?		*	
¿Estan incluidos en dicho procedimiento estándares sobre la utilización de dicho logical?		*	
¿Se han remitido descripciones escritas sobre los citados procedimientos a todos los departamentos usuarios?		*	
¿Se han establecido prioridades de transmisión asignadas a los mensajes enviados por la red?	4		
Evalué la satisfacción de los usuarios sobre las transmisiones a través de la red, sobre todo en periodos críticos.		7	
¿Existen planes de formacion para usuarios de la red?		*	
¿Existen responsables que evalúen el correo uso de la red por parte de los usuarios?		*	
¿Están perfectamente identificados todos los elementos físicos de la red(unidades de control, modem, cables etc) mediante etiquetas externas adecuadas?		*	
¿Está asegurando en un tiempo prudencial la reparación o cambio de elementos físicos de la red?		*	
¿Se realiza por parte de personal especializado una revisión periódica de todos los elementos de la red?		*	
¿Existe algún sistema para controlar y medir el funcionamiento del sistema de informática distribuida en la red?		*	
¿Existe una estructura que asegure que la explotación de máxima prioridad se lleva a cabo y se transmite e primer lugar?		7	
¿Se han desarrollado o adquirido procedimientos automáticos para resolver o evitar cierres del sistema (abrazos mortales)?		*	
¿Existe una rutina que asegure que ningún proceso o dato de baja prioridad va a estar sin procesar indefinidamente en la red?		*	
¿Existen mecanismos que controlen los tiempos de respuesta de la red y la duración de los fallos de operación de la misma?		*	
¿Se controlan regularmente todos los procesadores de la red?		*	

4.10. Conclusión General.

De acuerdo a la auditoría realizada se evidencia la manera en como la seguridad informática es necesaria para comprobar la fiabilidad y el nivel de cumplimiento de las normas y hacer frente a los problemas de seguridad descubiertos por la auditoría, implementando acciones correctivas que optimicen los recursos y reduzcan los problemas que se presentan en la administración de la red.

Se puede concluir que ningún sistema es 100 % confiable. Se debe tener conocimiento general del sector en el que se desenvuelve la empresa para tener una administración correcta

Referencias.

Libro:

- Piattini, M. G. (2005). Auditoria Informática un enfoque practico 2da edicion. Mexico,D.F.: ALFA OMEGA GRUPO EDITOR S.A. DE C.V.
- Santos, J. C. (2010). Seguridad Informática. España: RA-MA.
- Villalón, A. H. (2001). Seguridad Unix Redes. México: Open Publication Licence v.10.

Documento de Internet:

- http://www.redesyseguridad.es/clasificacion-del-software-malicioso/
- http://www.consultec.es/sistemas/pdf/cableado_estructurado.pdf
- http://www.consultec.es/sistemas/pdf/cableado_estructurado.pdf
- http://noemagico.blogia.com/2006/091301-la-investigacion-descriptiva.php
- http://es.wikipedia.org/wiki/Telecomunicaciones
- https://learningnetwork.cisco.com/community/certifications/ccna
- http://www.senavirtual.edu.co/
- http://biblioteca.universia.net/html_bura/verColeccion/params/id/43857.html
- http://www.justanswer.com/sip/microsoft?r=ppc|ga|1|Rest+of+World|
- http://www5.us.freebsd.org/doc/handbook/network-dhcp.html
- http://www.webopedia.com/TERM/F/firewall.html
- http://escreveassim.com.br/2012/04/17/redes-lan-man-wan-pan-san-can-wman-wwan-e-ran-qual-a-diferenca/
- http://en.wikipedia.org/w/index.php?title=Firewall_(computing)&action=edit