ESCUELA DE TECNOLOGÍA EN REDES Y TELECOMUNICACIONES

AUDITORIA DE SEGURIDAD INFORMÁTICA INTERNA Y PERIMETRAL PARA LA EMPRESA CONFECCIONES PAZMIÑO CASTILLO CIA. LTDA.

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

Profesor Guía

Ingeniero Henry Burbano

Autor

María Jazmín Mendoza Rivera.

Año

2012

DECLARACIÓN DEL PROFESOR GUÍA

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

……

Henry Burbano

Ingeniero

Número Cédula

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”

…….

María Jazmín Mendoza Rivera.

1310011026

AGRADECIMIENTO

Agradezco a cada una de las personas que aportaron con un granito de arena en mi vida. A mis ilustrados profesores quienes impartieron con sabiduría su conocimiento y paciencia para mi formación forjándome de esta manera un futuro competitivo como persona de bien, a mis padres que son el motor de mi vida y siempre me han brindado el apoyo incondicional, creyendo en mí y mis capacidades.

DEDICATORIA

Este proyecto lo dedico a Dios por guiarme en el camino del bien y fortalecerme ante las adversidades de la vida y culminar esta etapa; a mis padres por ser mis pilares fundamentales en esta lucha, en especial a mi madre por su trabajo incansable y espíritu de mujer luchadora para que cada uno de sus hijos forjen un mejor futuro. Ella es mi gran ejemplo a seguir, dedico este escalón de mi vida con mucho cariño y amor.

RESUMEN

En esta auditoría de seguridad informática interna y perimetral, se ha realizado la evaluación de las vulnerabilidades, errores y fallas que tiene la red; con el fin de documentar todas las anomalías e informar a las personas responsables sobre los resultados obtenidos para que tomen las medidas correctivas y preventivas, evitando riegos en el futuro.

Para este proyecto se necesitó obtener información de la teoría básica para la conceptualización de la seguridad informática y auditoría; ya que por medio de ellas se tendrá el entendimiento y conocimiento para definir las bases sólidas y lograr desarrollar habilidades que se apliquen en la duración de este proyecto; es lo que hace referencia el capítulo I.

El capítulo II se enfoca en el levantamiento de la información de la empresa, aquí se obtendrá la información total de la infraestructura de la red, la misma que permitirá encontrar las vulnerabilidades para tomar las medidas preventivas y llevar a cabo el desarrollo de la auditoria que es el tema que abarca el capítulo III. En este capítulo se harán las respectivas pruebas y evaluaciones para ver las falencias de cada uno de los equipos de comunicación, equipos terminales (sistema operativo, antivirus, contraseñas) y servidores.

Una vez realizada la auditoría; en el capítulo IV se hablará de los resultados obtenidos, con los cuales se elaborará un documento con las respectivas conclusiones y recomendaciones; de igual manera se realizarán los cuadros con los porcentajes de la auditoría realizada; los mismos que determinarán los correctivos necesarios para el mejoramiento de la red y evitar cualquier daño en el futuro.

ABSTRACT

This internal audit and information security perimeter has made the assessment of vulnerabilities, errors and failures that have the network in order to document and report all anomalies to those responsible for the results to take measures corrective and preventive actions to avoid risks in the future.

For this project we needed to obtain information from the basic theory for the conceptualization of computer security and auditing, because through them we will have the understanding and knowledge to define and achieve a solid foundation to develop skills that apply to the duration of this project is as referred to in chapter I.

Chapter II focuses on lifting the corporate information, here you will get the total information network infrastructure, which will find the same vulnerabilities to take preventive measures and carry out the development of the audit is the topic covered by chapter III. This chapter will make the respective tests and evaluations to see the shortcomings of each of the communications equipment, terminal equipment (operating system, antivirus, password) and servers.

After the audit, in Chapter IV will discuss the results obtained, which will produce a document with the relevant conclusions and recommendations will be made just as the pictures with the percentages of audit, which we will determine the necessary corrective measures to improve the network and prevent any future damage.

ÍNDICE

Introducción

Debido a la constante evolución de las tecnologías de la información, ha surgido la necesidad de implementar en diversas instituciones sistemas que brinden seguridad, confiabilidad y escalabilidad en las diferentes redes de información y comunicación; esto debido a que se transfiere información de vital importancia para la empresa, por lo que se debe considerar un mejor control y protección para el procesamiento de sus datos.

En sí, la seguridad de una red va ligada a las políticas de seguridad de la organización que la utiliza; por lo que debe tener frentes como: la red LAN, WAN, Wireless, Servidores y PCs; los cuales no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados.

“El desarrollo de los procesos apegados a las normas y procedimientos bajo eficientes medidas de CONTROL y PRODUCTIVIDAD, son en los actuales momentos dos de los principales objetivos que persigue una empresa moderna de carácter mundial. Así como la Auditoria financiera controla los sistemas y registros de su contabilidad, la Auditoria Informática es la encargada de verificar que sus sistemas y procesos informáticos funcionen adecuadamente para el objetivo que han sido programados, y sus activos fijos tangibles se encuentren debidamente protegidos, para garantizar la confiabilidad de los registros que en ellos se almacenan. Hoy en día las organizaciones modernas destinan muchos recursos financieros para desarrollar sistemas de controles que le permitan manejar de una manera más eficiente los datos, permitiendo de esta forma disponer de ellos en los momentos precisos y poder tomar decisiones muy acertadas y de alto impacto. Todas estas tareas se cumplen siempre y cuando se cuente con una revisión y evaluación de los sistemas informáticos, conociendo los equipos detalladamente para desglosar el tipo de utilización, eficiencia y algo muy importante que es la seguridad, y por último no debemos descartar la rotación del personal que opera en todos los procesos informáticos a efectos de recomendar las mejoras necesarias para una

utilización más correcta y segura de los sistemas, esto nos permitirá confiar en la información que los mismos brindan. El término de Auditoria se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "Tiene Auditoria" como sinónimo de que, en dicha entidad, antes de realizarse la auditoria, ya se habían detectado fallas.” (Bertucci, 2011)

1 Capítulo I Marco Teórico

1.1 Definición del proyecto

1.1.1 Antecedentes

Confecciones Pazmiño Castillo Cía. Ltda. ubicada en el sector el Condado, posee una infraestructura de red con seguridad poca robusta en los sistemas de información, cuenta con un cableado estructurado categoría 6 y con equipos terminales que conforman la red.

En la infraestructura implementada se desconoce el estado de los equipos de comunicaciones como modem, firewall, router, switch.

Se desconoce el estado de licenciamiento del sistema operativo, antivirus, aplicaciones.

Existe acceso libre a la información difundida en la red LAN sin importar el nivel jerárquico.

No existe un respaldo en la información generada, ni un cronograma de mantenimiento para los equipos terminales.

1.1.2 Formulación del problema

Debido al constante cambio de los sistemas informáticos, se debe considerar medidas necesarias para el buen funcionamiento de la red en la empresa.

Al no existir políticas de seguridad, hace que la infraestructura de la red no sea eficiente.

Los equipos informáticos al no contar con una configuración de contraseñas seguras, se ven vulnerados a robos, hurtos, pérdidas de información, e inclusive se ve vulnerable a posibles catástrofes naturales, debido a que no cuenta con un mecanismo de Backus, para respaldar todo la información que genera la empresa.

No hay documentación de la red; lo que dificulta la administración y solución a los problemas de una manera efectiva al momento de realizar algún tipo de reparación.

En la configuración del antivirus no existe documentación por lo que dificulta el acceso de las aplicaciones en los equipos.

1.1.3 Objetivo General

Realizar la auditoría de seguridad informática interna y perimetral en la empresa Confecciones Pazmiño Castillo Cía. Ltda. para asegurar un mejor control de la información y efectuar las debidas recomendaciones de seguridad para corregir las vulnerabilidades en caso de existir.

1.1.4 Objetivos específicos

Efectuar un estudio general sobre la situación actual de la empresa, en especial el área informática, para identificar las debilidades en los sistemas de información.

Evaluar el software y aplicaciones instaladas en los dispositivos.

Evaluar las contraseñas en los equipos de cómputos y perfiles de usuarios.

1.1.5 Alcance

Con la realización de este proyecto la empresa tendrá un análisis minucioso de las debilidades que afronta la red tanto interna como externa.

Se elaborará un documento donde se proporcionará las recomendaciones y sugerencias de la información general de la infraestructura de la red.

Los usuarios podrán gozar de privilegios y servicios en cada una de sus máquinas obteniendo eficiencia en el trabajo.

Se garantizará que la información esté protegida por contraseñas seguras tanto en equipos fronterizos como servidores.

1.1.6 Justificación del proyecto

Ante los inconvenientes previamente mencionados es necesario tomar un apropiado control en la organización de los planes de contingencia y sistemas que operan la empresa; debido a esto se considera de mucha importancia la realización de una auditoría de seguridad informática, con el objeto de evaluar y prevenir fallas en un momento oportuno.

1.2 La Seguridad Informática

1.2.1 Aspectos básicos de la seguridad en informática

En los orígenes de los sistemas informáticos, la seguridad ha sido un tema de preocupación para dichos sistemas; ya que está enfocada a la prevención de la vida y todas las posesiones.

En las raíces modernas se tiene la necesidad de desencriptar mensajes de preguerra y guerra entre las potencias de época en los años 40. El primer ordenador Collosus construido por Tuning, tenía la tarea de vulnerar los mensajes encriptados por la famosa maquina Enigma, utilizada por los alemanes para codificar los mensajes de guerra.

El problema de seguridad en los sistemas de computación, se restringe al acceso de las personas en los sistemas con el fin de garantizar que no se divulguen sus claves de acceso.

En el año 1982 Rich Skrenta crea el primer virus informático llamado “Elk Cloner” el mismo que consistía en copiar un pequeño programa en las unidades de disquete sin permiso de los usuarios en los diferentes equipos en general, su objetivo era distribuir un pequeño poema indicando que se había infectado el ordenador; ya para el año de 1983 se lo cataloga por primera vez con el término de virus informático.

A través de la difusión del internet y el uso de éste como plataforma de negocio, hizo que todos los ordenadores del mundo se conecten entre sí lo cual ocasionó el aumento de códigos maliciosos que son muy destructivos y que pueden vulnerar los sistemas de seguridad de un país; causando grandes pérdidas económicas.

Sin embargo estas plataformas tecnológicas evolucionan y la inseguridad se transforma, ocasionando un enfrentamiento de aprendizaje ante los profesionales de la seguridad. Es por esto que la seguridad hoy en día es compleja y con funciones especializadas que se dividen en: seguridad física, ambiental, nuclear, lógica etc.

Hoy por hoy la conectividad es indispensable para el progreso y a pesar que existen diferentes tipos de amenazas; es necesario utilizar políticas, metodologías y técnicas de protección de la información.

1.2.2 Definición

“La seguridad informática representa el conjunto de medios y técnicas implementados para asegurar la integridad y que no se difundan involuntariamente los datos que recorren el sistema de información, entendiendo como tal al conjunto de datos y recursos (físicos, lógicos y humanos) que permiten almacenar y que circule la información que contiene. También representa la red de actores que intervienen sobre éste, que intercambian datos, acceden a ellos y lo usan.” (ACISSI, 2011)

1.2.3 Principios de la seguridad informática

La seguridad informática, en general, está teniendo una importancia cada vez mayor. Los usuarios particulares y trabajadores de las empresas, deben ser conscientes de que el funcionamiento correcto de sus sistemas depende en gran medida, de protegerlos como el mayor de sus tesoros.

“La seguridad informática consiste en asegurar que los recursos del sistema de información (material informática o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación, solo sea posible a las personas que se encuentre acreditadas y dentro de los límites de su autorización.

Fiabilidad, confidencialidad, integridad y disponibilidad

Si bien es cierto que todos los componentes de un sistema informático están expuestos a un ataque (hardware, software y datos) son los datos y la información los sujetos principales de protección de las técnicas de seguridad. La seguridad informática se dedica principalmente a proteger la confidencialidad, la integridad y disponibilidad de la información. Por tanto, actualmente se considera generalmente aceptado que la seguridad de los datos y la información comprende tres aspectos fundamentales.

Confidencialidad, es decir, no desvelar datos usuarios no autorizados que comprende también la privacidad (la protección de datos personales).

Integridad, permite asegurar que los datos no se han falseado.

Disponibilidad, esto es, que la información se encuentre accesible en todo momento a los distintos usuarios autorizados.

Hay que tener en cuenta que tanto las amenazas como los mecanismos para contrarrestarlas, suelen afectar a estas tres características de forma conjunta. Así por ejemplo, fallos del sistema que hacen que la información no sea accesible pueden llevar consigo una pérdida de integridad.

Generalmente tiene que existir los tres aspectos descritos para que haya inseguridad. Dependiendo del entorno en que un sistema trabaje, a sus responsables les interesará dar prioridad a un cierto aspecto de la seguridad.

Los conceptos confidencialidad, integridad o disponibilidad son muy comunes en el ámbito de la seguridad y aparecen como fundamentales en toda

arquitectura de seguridad de la información, ya sea en el ámbito de la protección de datos, normativa vigente relacionada con la protección de datos de carácter personal, como de códigos de buenas prácticas o recomendaciones sobre la gestión de la seguridad de la información y de prestigiosas certificaciones internacionales, éstas últimas, relacionadas con la auditoría de los sistemas de información.

Juntos a estos tres conceptos fundamentales se suelen estudiar conjuntamente la autenticación y el no repudio en los sistemas de información. Por lo que suele referirse al grupo de estas características como CIDAN sacado de casa característica.

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticación
- No repudio

Por estos motivos es importante tener una idea clara de estos conceptos

Confidencialidad

Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado.

De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de éste y que pueda ser leído por una persona no autorizada.

Integridad

La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos sería la correspondencia entre los datos y los hechos que refleja.

Disponibilidad

Se trata de la capacidad de un servicio, de unos datos o de un sistema, a ser accesible y utilizable por los usuarios(o procesos) autorizados cuando éstos lo requieran.

También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor:

Autenticación

La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado(o pertenece) a quien el documento dice.

Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. La autenticación en los sistemas informáticos habitualmente se realiza mediante un usuario o login y una contraseña o password.

No repudio

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el

servicio de no repudio se produce frente a un tercero, de este modo, existirán dos posibilidades.

No repudio en origen: el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario

No repudio en destino: el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor

Si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el “no repudio” prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino).

Figura 1.1: Relación de los servicios de seguridad:

En la imagen superior se ilustra cómo se relacionan los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así si no existe el de más abajo, no puede aplicarse el superior. De esta manera, la disponibilidad se

convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de confidencialidad, que es imprescindible para conseguir integridad, para poder obtener autenticación es imprescindible la integridad y por último el no repudio sólo se obtiene si se produce previamente la autenticación". (Santos, 2010)

1.2.4 Clasificación de la seguridad informática.

1.2.4.1 Seguridad activa y pasiva

Seguridad Activa

"Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseña; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes.

Seguridad Pasiva

Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema, por ejemplo, teniendo siempre al día copias de seguridad de los datos". (López, 2010)

1.2.4.2 Seguridad física y lógica

A partir del medio natural de la amenaza, se puede hablar de seguridad en los niveles tanto físico como lógico.

Seguridad Física

Es la que salvaguarda físicamente el sistema informático utilizando barreras físicas y mecanismos de control.

La seguridad física puede verse sometida por desastres naturales o por personas de manera accidental o voluntariamente

Dentro de las amenazas inducidas por el ser humano existen las siguientes. Accidentales, como borrado y olvido de clave y deliberadas, como sustracción de la clave, eliminación de la información y hurto de datos confidenciales.

Seguridad Lógica

“La seguridad lógica se encarga de asegurar las partes software de un sistema informático, que se compone de todo lo que no es físico, es decir, los programas y datos.

La seguridad lógica se encarga de controlar que el acceso al sistema informático, desde el punto de vista software, se realice correctamente y por usuarios autorizados, ya sea desde dentro del sistema informático, como desde fuera, es decir, desde una red externa, usando VPN(protocolos PPP, PPTP), la web(protocolos http, https), transmisión de ficheros(ftp).”

En la seguridad lógica existen programas como el sistema operativo que restringe el acceso de los procesos o usuarios a los recursos del sistema

“Para ello debe tomar distintas medidas de seguridad. Cada vez los sistemas operativos controlan más la seguridad del equipo informático ya sea por parte de un error, por un uso incorrecto del sistema operativo o del usuario, o bien por un acceso no controlado físicamente o a través de la red, o por un programa malicioso como los virus, espías, troyanos, gusanos, phising.

Es casi imposible que sea totalmente seguro, pero se pueden tomar ciertas medidas para evitar daños a la información o a la privacidad de esta. Uno de los principales peligros de un sistema informático le puede venir por internet, también por compartir información con otro equipo por la red o a través de un archivo infectado que entre en el sistema mediante una memoria secundaria,

como un dispositivo de almacenamiento USB, DVD, disco duro externo". (Hurtado, 2011)

1.3 La Auditoria Informática

1.3.1 Introducción

"La informática ha experimentado un desarrollo espectacular desde que comenzara a implementarse en las empresas, allá por los años sesenta. Este crecimiento ha influido, en la mayoría de las organizaciones, de un modo notable tanto en su estructura como en sus funciones, alterando los tradicionales métodos de verificación y control de los procedimientos y de los datos de la organización.

Fueron pocas las empresas que supieron adaptarse a las formas de control requeridas en este nuevo entorno, y los profesionales informáticos conquistaron importantes parcelas, con unos notables presupuestos que, en la mayoría de los casos, eran difíciles de gobernar y que, aparentemente, las Direcciones no tenían más remedio que aceptar, de mejor o peor grado.

Pero aplicando la máxima de que "todo lo que sube tiene que bajar", estas Direcciones comenzaron a querer gobernar lo aparentemente ingobernable, conscientes de que una aplicación de la informática y controlada en la empresa, abarataría los disparatados costes en que se estaba incurriendo.

Estos planteamientos dieron lugar a la aparición de todos aquellos procedimientos que venían a verificar y controlar la función informática: la auditoría informática". (Rivas, 1989)

1.3.2 Definición

"Una auditoria de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistema 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.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsable quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus archivos de información en cuanto a protección, control y medidas de seguridad.” (Santos, 2010)

1.3.3 Objetivos de la auditoria informática

“La definición de los objetivos de la auditoría informática es un tema difícil y complejo. No existe un total acuerdo en la definición de tales objetivos y en consecuencia, en el establecimiento de las funciones que debe desarrollar un auditor informático. Para precisar esta situación sería necesario:

- Definir el campo de actuación del auditor informático.
- Definir los objetivos de la auditoría informática.

Para el campo de actuación del auditor, sería preciso reflexionar sobre los siguientes aspectos:

- Organización en la que se desenvolverá el auditor.
- Estructura.
- Tipo de actividad de la empresa.
- Departamento de informática objeto de la auditoría.
- Grado de sofisticación.
- Tamaño.
- Recursos del departamento
- Relaciones con la auditoría financiera.

- las propias limitaciones técnicas del auditor.

De un modo general los objetivos de la auditoría informática podrían ser:

- Elaborar un informe sobre los aspectos que afecten al alcance de una auditoría y señalar riesgos de errores o fraudes de un sistema informático.
- Evaluar la fiabilidad de los sistemas informáticos, en cuanto a la exactitud de los datos y a las informaciones tratadas.
- Verificar el cumplimiento de la normativa general de la empresa.
- Comprobar la eficacia de los sistemas implantados.
- Comprobar si se ha estudiado el coste / beneficio.
- Garantizar la seguridad física y lógica.
- Evaluar la dependencia de una organización respecto a sus sistemas informáticos, revisando las medidas tomadas en el caso de que se produzca un fallo y que permitan asegurar la continuidad de las actividades normales.
- Emisión de informes con la evaluación independiente de los sistemas informáticos. sintetizando riesgos, deficiencias, sugerencias y recomendaciones.
- Análisis de la calidad y eficacia del servicio de atención a los usuarios. Participación y seguimiento de proyectos de investigación.” (Aguilar, 2012)

1.3.4 Fases de una auditoría

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

1.3.5 Tipos de auditoria

“Los servicios de auditoría pueden ser de distinto índole:

- **Auditoría se seguridad interna**. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
- **Auditoria 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.** El 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 auditoria perimetral.
- **Análisis forense.** El 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 *postmorten*.
- **Auditoría de página 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 (XSS), etc.
- **Auditoria de código de aplicaciones.** Análisis del código tanto de aplicaciones de páginas web como de cualquier tipo de aplicación, independiente del lenguaje empleado.

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoria”.

1.3.6 Metodología de Auditoria de seguridad

“Una auditoria se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorias de informática.

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

Adicional a este estándar se puede encontrar el estándar ISO27002, 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.

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

En la auditoria 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 la auditoría de sistemas de información establece su ejecución por fases:

1. **Definir el alcance de la auditoría:** análisis inicial y plan de auditoría.

2. **Recopilación de información, identificación y realización** de pruebas de auditoría, incluyendo, si se acuerda, acciones de *hacking* ético o análisis de vulnerabilidades de aplicaciones.
3. **Análisis de las evidencias,** documentación de los resultados obtenidos y conclusiones.
4. **Informe de auditoría** en el que recogen las acciones realizadas a lo largo de la auditoría y las deficiencias detectadas. El informe contiene un resumen ejecutivo en el que resaltan los apartados más importantes de la auditoria.
5. **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". (Santos, 2010)

1.3.7 Auditoría Informática en las PYMES.

1.3.7.1 Las PYMES y las tecnologías de la información.

"La importancia de las PYMES viene dada ante todo por su número más de dos millones de empresas que conforman el tejido empresarial así como por su potencialidad, ya que constituyen la base de desarrollo empresarial.

Asumida por todos los estamentos públicos y privados de la sociedad actual la necesidad de reformar la competitividad y rentabilidad de las PYMES favoreciendo su estabilidad y la que estas aportan a la economía.

Para contribuir a ello, el primer paso es abortar su problemática interna; su propio funcionamiento; y dentro del mismo, los sistemas de información que han de permitir la gestión y seguimiento de las principales variables del negocio, facilitando la correcta toma de decisiones, minimizando riesgos, y consiguiendo de este modo ampliar su competitividad en un mercado cada vez más abierto y liberalizado". (Piattini, 2005)

Se demuestra que el Control Interno Informático y su auditoria aprueban gestionar y rentabilizar los sistemas de información de la forma más eficiente, optimizando, en suma y resultados. El método de Auditoría Informática, logrará que los Sistemas de Información sean fiables, exactos, y ante todo, den el fruto que los empresarios esperan de ellos.

1.3.7.2 Introducción

El estudio que se realizará, será sencillo y fiable para conocer la situación general del sistema de información de una empresa, así como definir el estado del control de dichos sistemas tomando como control la definición de la ISACA (Information System, Audit and Control Association).

“Los métodos que abarquen las políticas, procedimientos, practicas, estándares y estructuras organizativas que aseguren la adecuación de la gestión de los activos informáticos y la fiabilidad de las actividades de los sistemas de información.”

No se pretende con la misma eliminar las funciones del auditor (Interno o externo) informático, sino que el responsable de los sistemas de información, el Gerente o Director de un departamento o de la misma empresa pueda hacerse una idea suficientemente aproximada del estado de sus sistemas, pudiendo abordar, en caso necesario, un estudio mas interno o especializado de los mismos. Resulta, pues, un enfoque de Auditoría Interna tomando como base que la información es un activo más de la empresa y como Auditoría Informática:

“Proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva eficazmente los fines de las organización y utiliza eficientemente los recursos de este modo, así como sustenta y confirma la consecución de los objetivos tradicionales del auditor.”

El usuario o el Auditor pueden comprobar por sí mismo la fiabilidad y consistencia de los sistemas mediante una metodología que no le obligue a tener amplios conocimientos de informática ni de Auditoria propiamente dichos.

1.3.7.3 Conocimientos necesarios

No es preciso poseer conocimientos informáticos para realizar una auditoría informática mediante la técnica CHECKLIST. Pero si se requiere, un mínimo de formación específica para saber, qué es lo que se desea analizar así como algunos conceptos de conocimientos relevantes como:

- Minicomputador, red local, PC, periféricos, software de base, eficacia de un servicio informática, seguridad lógica, seguridad física, etc.

Asimismo será necesario conocer en profundidad el organismo o área a evaluar; su organización, composición y características principales, así como los medios de que se disponen: plantilla, datos técnicos, etc.

1.3.7.4 Metodología de la Auditoria Informática

En la actualidad existen tres tipos de metodología de Auditoria Informática:

- R.O.A. (RISK ORIENTED APPROACH), diseñada por Arthur Andersen.
- CHECLIST o cuestionarios.
- AUDITORIA DE PRODUCTOS (por ejemplo, Red Local Windows NT; sistemas de Gestión de base de Datos DB2; Paquete de seguridad RACF, etc.).

Las tres metodologías están basadas en la minimización de los riesgos, que se conseguirá en función de que existan los controles y que estos funcionen.

La más adecuada a la Auditoría de las PYMES es la CHECKLIST.

1.3.7.4.1 Metodología Utilizada

La metodología utilizada es la Evaluación de Riesgo (ROA Risk Oriented Approach) recomendada por ISACA (Information System, Audit and Control Association, Asociacion Internacional de Auditores de Sistemas de Información).

Esta evaluación de Riesgo se desarrolla sobre determinada áreas de aplicación y bajo técnicas de Checklist (Cuestionarios) adaptados a cada entorno específico; deberá tenerse en cuenta que determinados controles se repetirán en diversas áreas de riesgo. Esto debido a que dichos controles tienen incidencia independiente en cada una.

1.3.7.5 Utilización de la Guía

La auto guía está dividida en varias áreas de riesgo, concretamente seis, que son:

1. Riesgo en la continuidad del proceso.
2. Riesgo en la eficacia del servicio.
3. Riesgo en la eficiencia del servicio.
4. Riesgos económicos directos.
5. Riesgos de la seguridad lógica.
6. Riesgos de la seguridad física.

1.3.7.5.1 Fases de la autoevaluación

Se explicará superficialmente el significado de cada uno, tomando en cuenta que no existe una separación absoluta entre los mismos, sino que frecuentemente se solapan e incluso determinados riesgos conllevan otros que se han evaluado en diferentes áreas.

Riesgo en la continuidad del proceso

Son aquellos riesgos de situaciones que pudieran afectar a la realización del trabajo informático o incluso que pudieran llegar a paralizarlo, y, por ende, llegar a perjudicar gravemente a la empresa o incluso también a paralizarla. Se deberá hacer especial hincapié en el análisis estricto de estos riesgos puesto que, si bien otros podrían afectar relativamente a la empresa o bien causarle perjuicio de diverso tipo, éstos podrían ocasionar un verdadero desastre.

Riesgo en la eficacia del servicio informática

Se entiende como eficacia del servicio la realización de los trabajos encomendados. Así pues, los riesgos en la eficacia serán aquellos que alteren dicha realización o que afecten a la exactitud de los resultados ofrecidos por el servicio informático.

Riesgo en la eficiencia del servicio informático

Eficiencia del servicio es 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. Hay que matizar en este aspecto que determinados controles podría resultar una mejora considerable de la eficiencia del servicio pero igualmente podrían resultar económicamente poco rentables sobre todo para pequeñas empresas. La valoración de dichos controles deberá ser analizada por los responsables de la empresa en cuya mano estará la decisión de aplicación de los mismos.

Riesgos económicos directos

En cuanto a estos riesgos se analizará 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 que pudieran transgredir la normativa de la empresa o las leyes vigentes (LORTAD).

Riesgos de la seguridad física

Los riegos en cuanto a la seguridad física comprenderán todos aquellos que actúen sobre el deterioro o apropiación de elementos de información de una forma meramente física.

Dadas estas áreas de riesgo, el usuario podrá valorar cada una independientemente según sus necesidades. Aun así, se consideran como más importantes, y casi se puede asegurar que imprescindibles, las dos primeras

- Riesgo en la continuidad del proceso
- Riesgo en la eficacia del servicio

Por lo que cualquier análisis debería ser comenzado con las mismas.

1.3.7.6 Valoración de resultados

La auto guía se compone de una serie de cuestionarios de control. Dichos cuestionarios podrán ser contestados mediante dos sistemas indicados en los mismos:

En el primer sistema se responderá con SI NO o N/A (NO APLICABLE si la repuesta no lo fuera por cualquier causa). Estos cuestionarios de respuesta directa tendrán un valor numérico de 1 a 10 anexos a la pregunta que habrá que poner en el lugar de la respuesta

CONTROLES	SI	NO	N/A
¿Posee la instalación equipos de continuidad en caso de cortes de energía como puede ser los sistemas de alineación ininterrumpido?	7	4	

En el caso de que se dispusiera de UPS, se pondrían en la casilla del SI el valor 7, en caso contrario pondrían el valor 4 en la casilla del NO. La diferencia de valoración puede estar determinada porque la existencia se considera una mejora sustancial, sin embargo, la no existencia podría ser de escasa importancia.

En el segundo sistema no existirá un número de ponderación y será el propio usuario quien deberá dar una valoración a la respuesta. Generalmente en estos casos los controles comenzaran con la propuesta EVALUE. y la valoración que habrá que dar estará anexada a la pregunta con los valores mínimos y máximo, por ejemplo:

CONTROLES	SI	NO	N/A
¿Evalúe la carga de trabajo en época alta de proceso? (Ponga el resultado en la casilla no) 1-30	7	4	

Habrá Cuestionarios que estarán acompañados de un asterisco. Estos controles son considerados de alto riesgo, por tanto indispensables. La idea es que un sistema sin estos controles podría abocar al desastre informático y en algunos casos al desastre de la empresa. En ocasiones no se da la debida importancia a los mismos y solamente se ponderan en lo que valen al ocurrir el problema. Estos controles deberán tenerse muy en cuenta a la hora de realizar la evaluación y, en caso de inexistencia, dar primacía a su implantación". (Piattini, 2005)

2 Capítulo II Levantamiento de Información

2.1 Estado de la información de la red

Según información recopilada la empresa Confecciones Pazmiño Castillo Cía. Ltda. posee una infraestructura de red nueva; donde sus dispositivos no cuentan con las seguridades adecuadas, haciéndola vulnerable ante cualquier ataque interno o externo; el área donde se encuentran los equipos no tiene una ventilación adecuada para el buen funcionamiento y evitar deterioro de los mismos.

2.1.1 Elaboración del diseño de infraestructura

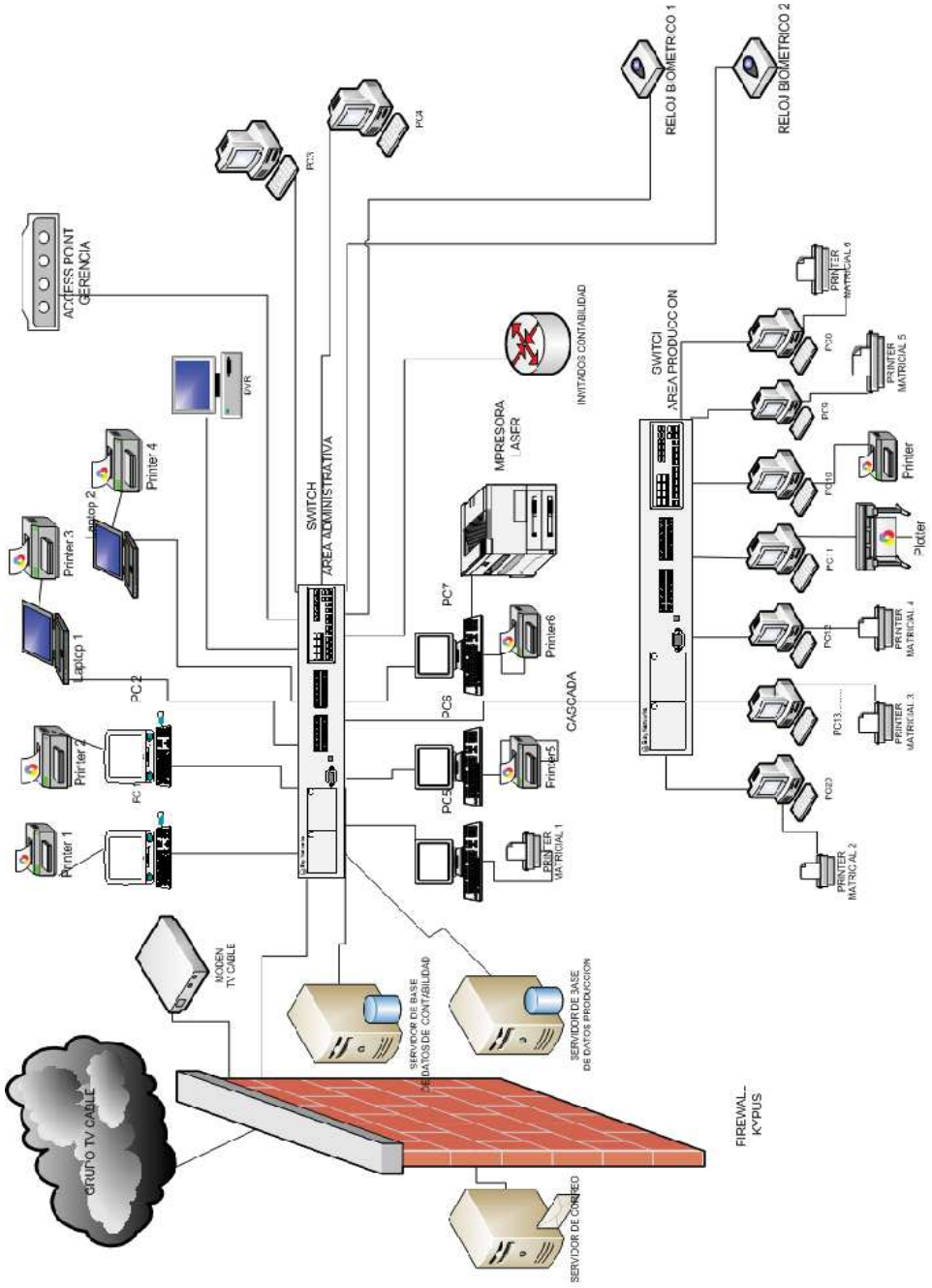


Figura 2.1 (Autor: Jazmín Mendoza, 19/04/2012) Diseño de la Infraestructura de red Confecciones Pazmiño Castillo Cía. Ltda.

2.1.2 Tipos de servidores

Existen 3 servidores en la infraestructura de la red. El primero es para la base de datos del sistema contable, el segundo para el sistema de producción y el tercero es el Kypus que administra el tráfico en la red.

En el primer servidor se encuentra instalado el sistema operativo Windows server 2003, los servicios no están levantados en su totalidad por lo que dificulta la administración del mismo; se encuentra en un 25% del rendimiento de sus recursos, no posee una contraseña robusta. En este servidor se encuentra alojado el antivirus NOD 32 con licenciamiento, el mismo que administra las actualizaciones para los equipos que se encuentran en la red. Está generando inconvenientes ya que no distribuye debidamente las actualizaciones en la base de firma de los virus para el resto de equipos.

El segundo servidor donde se localiza el sistema de producción no se encuentra en su completo funcionamiento ya que está en una etapa de implementación.

El tercer servidor Kypus, administra los servicios de la red, permitiendo tener el control para las estaciones de trabajo en las políticas implementadas; no posee una contraseña robusta. En este servidor se encuentra configurado un servidor DHCP, el cual entrega las direcciones IP para el router y access point.

Se cuenta con un servidor externo de correo, suministrando 10 cuentas de correo empresariales y un hosting el cual no está en utilización.

Características de los servidores

Servidor (1): HP Proliant ML150,

Características físicas:	Procesador Intel 1.6 GHz
	Memoria 12022 MB
	Disco Duro 550GB
Características lógicas:	Windows Server 2003 Enterprise Edition

Servidor (2): Stor Trends 1100i (American Megatrends)

Características físicas: Memoria 1Gb
4 Disco Duro HITACHI de 250GB
2 puertos USB

Servidor (3): Firewall. KMSA MULTIFUCTION SECURITY APPLIANCE para 24 usuarios.

2.1.3 Dispositivos y equipos terminales

Al utilizar varios servidores DHCP en la misma subred, crece la posibilidad de errores; en la red existen 3 servidores DHCP, el Kypus, router y access point.

- 1 Router Tp-Link: hay conflictos al momento de conexión en la red wireless debido a que existen otros servidores DHCP; el nivel de seguridad está encriptado pero no posee contraseña robusta y el SSID se está difundiendo a nivel broadcast.
- 1 Access Point D-link DWL-3200, su nivel de seguridad está encriptado, la contraseña no es segura y está generando inconvenientes al conectarse; debido a que ya se cuenta con un servidor DHCP y su SSID se encuentra difundiendo a nivel broadcast generando inseguridad. El status del CPU se encuentra en un 4% y su memoria utilizada es de un 65%.
- Switch 1 D-link DGS-1210-24: Administrable, soporta VLAN; asignado para el área de administración; se encuentran 20 puertos ocupados.

  VLAN 01 Servidores**:** En esta vlan están los dos servidores de aplicaciones de la empresa.

  VLAN 02 Administración: En esta vlan están los equipos de cómputo de administración y contabilidad .

  VLAN 03 Internet: En esta vlan está el servidor de Internet Kypus.

- Switch 2 D-link DGS-1210-24: Administrable, soporta VLAN; asignado para la parte de producción se encuentran 13 puertos ocupados, configurados con 3 VLAN.
- 1 modem Motorola: el cual provee de Internet a la empresa.
- Existen 37 equipos terminales, entre PC de escritorios, laptops e impresoras.

  El 85% de los equipos terminales entre PC y laptops se encuentra con software licenciado, mientras que el 15% restante tiene instalado software no licenciado.

  El antivirus: se encuentra con una vigencia de 1 año e instalado en los equipos terminales en un 86% y el 14% de las máquinas restantes poseen un antivirus sin licenciamiento.

  Del 100% de las máquinas, el 40 % se encuentran configuradas con contraseñas pocas robustas y privilegios de usuarios; el 60% no tienen contraseñas ni configuración de los privilegios de usuarios.

- Relojes Biométricos para el control de entrada al personal, su software se administra desde una máquina que no posee una contraseña robusta.

2.1.4 Cableado

El cableado estructurado se encuentra realizado con cable UTP categoría 6, sus especificaciones técnicas se encuentran en el anexo 1.

3 Capítulo III Auditoria de la red

3.1 Evaluación de Servidores y Servicios de la Red

Para evaluar los servidores y servicios de la red, se utilizará herramientas utilitarias las mismas que facilitarán al proceso de auditoría para obtener los resultados y requerimientos necesarios.

3.1.1 Servidor de Correo

Para la evaluación del servidor del correo se procede a realizar las siguientes pruebas que determinan el estado en que se encuentra.

3.1.1.1 Evaluación del Dominio

Para comprobar los registros del dominio de la empresa, es necesario saber en qué orden están alojados los servidores; para ello se realizará la prueba utilizando la página www.mxtoolbox.com, que es una herramienta utilitaria para determinar la configuración.

Figura 3.1 Evaluación del dominio

Una vez ingresado el nombre del dominio, a través de la opción Mx Lookup como muestra en la figura 3.1; busca una dirección de correo específico, la cual regresa una lista con los servidores responsables de entregar dicho correo; y la prioridad relativa para cada unos de los servidores.

Como resultado se observa en la figura 3.2, que el dominio de la compañía, se encuentra alojado en dos servidores y con su respectiva orden de prioridad.

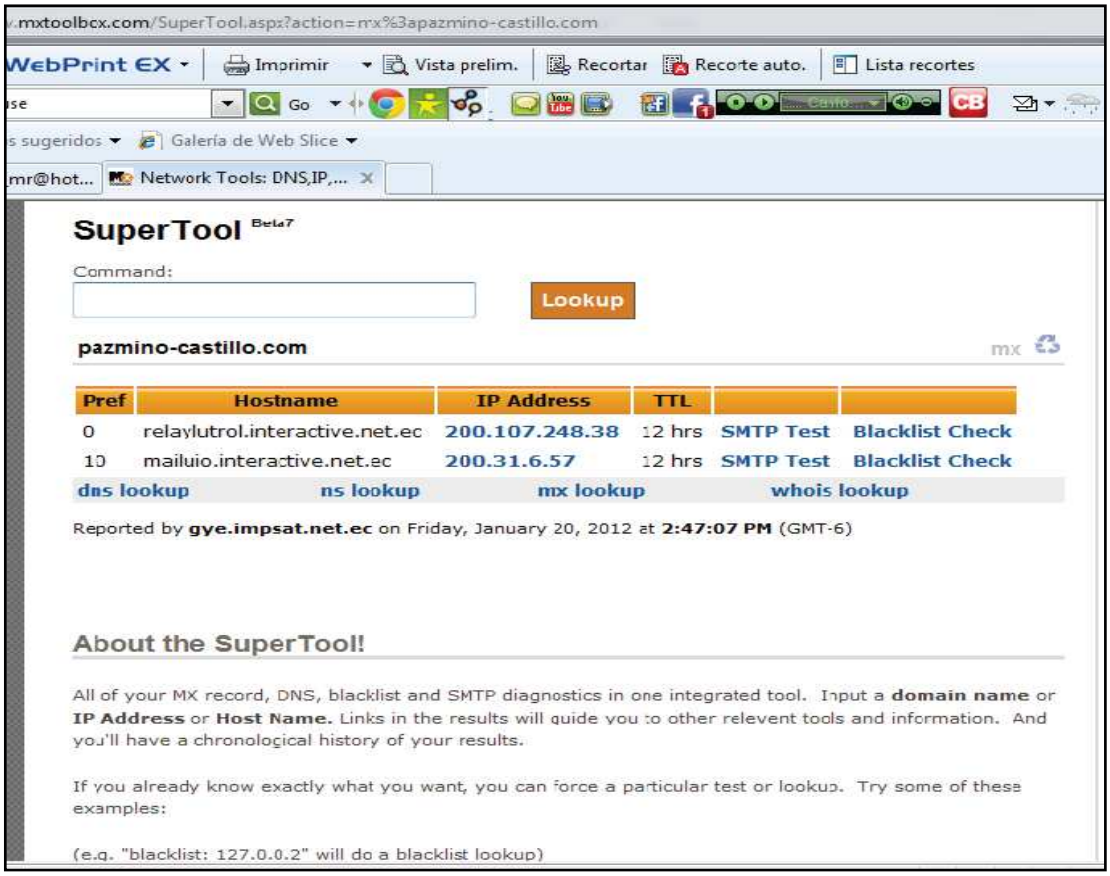


Figura 3.2: Resultado búsqueda de dominio a través de Mx Lookup.

3.1.1.2 Evaluación del Correo

El correo electrónico es uno de los medios más utilizados del internet; permite a una persona enviar y recibir datos a otros usuarios que se encuentran en diferentes lugares del mundo.

Ahora para evaluar los servicios del correo se realizará las pruebas siguientes.

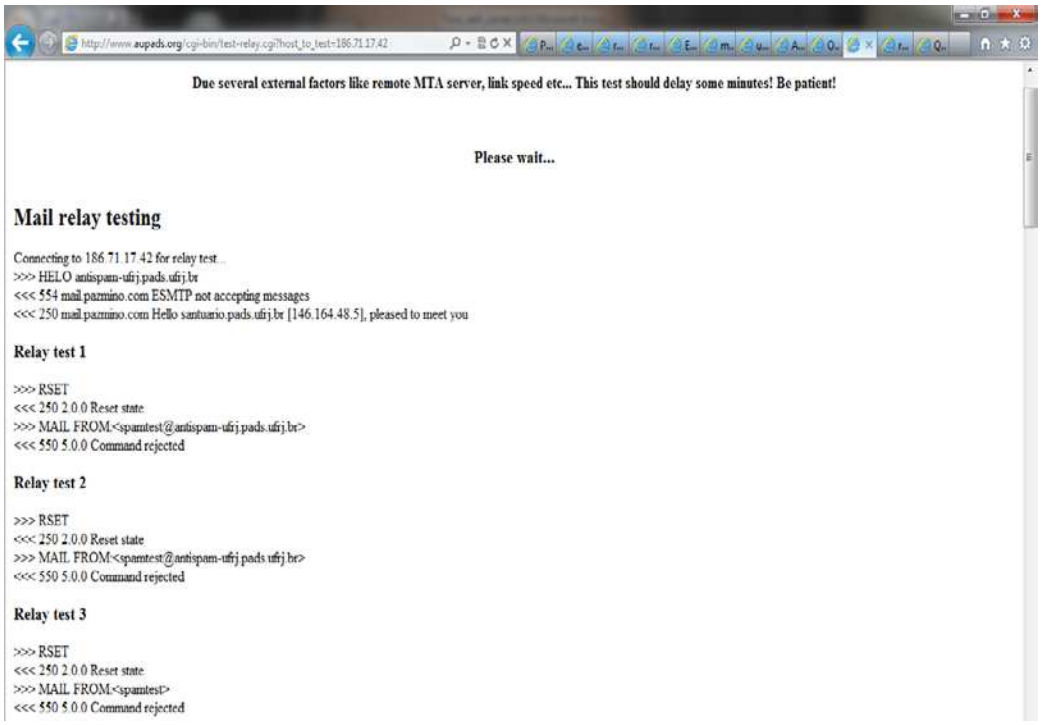
3.1.1.2.1 Open Relay Test

El Open Relay; es el que tiene la particularidad de permitir a un servidor enviar correos a través del nuestro. Si está abierto quiere decir que cualquier servidor podría enviar correos a través de nuestro servidor.

Para realizar esta prueba se utilizará el link http://www.aupads.org/test-relay.html, el mismo que pide ingresar la IP pública de la empresa.

Figura 3.3: Prueba de Open Relay Test

Ahora como se puede mostrar en la figura 3.4 se está haciendo la respectiva prueba para enviar correos, pero la prueba es fallida en este caso.



Relay test 4

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<>
<<< 550 5.0.0 Command rejected

Relay test 5

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

Relay test 6

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@42.186-71-17.uio.satnet.net>
<<< 550 5.0.0 Command rejected

Relay test 7

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

Relay test 8

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

Relay test 9

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

Relay test 10

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

Relay test 11

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

Relay test 12

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

Relay test 13

>>> RSET
<<< 250 2.0.0 Reset state
>>> MAIL FROM:<spamtest@[186.71.17.42]>
<<< 550 5.0.0 Command rejected

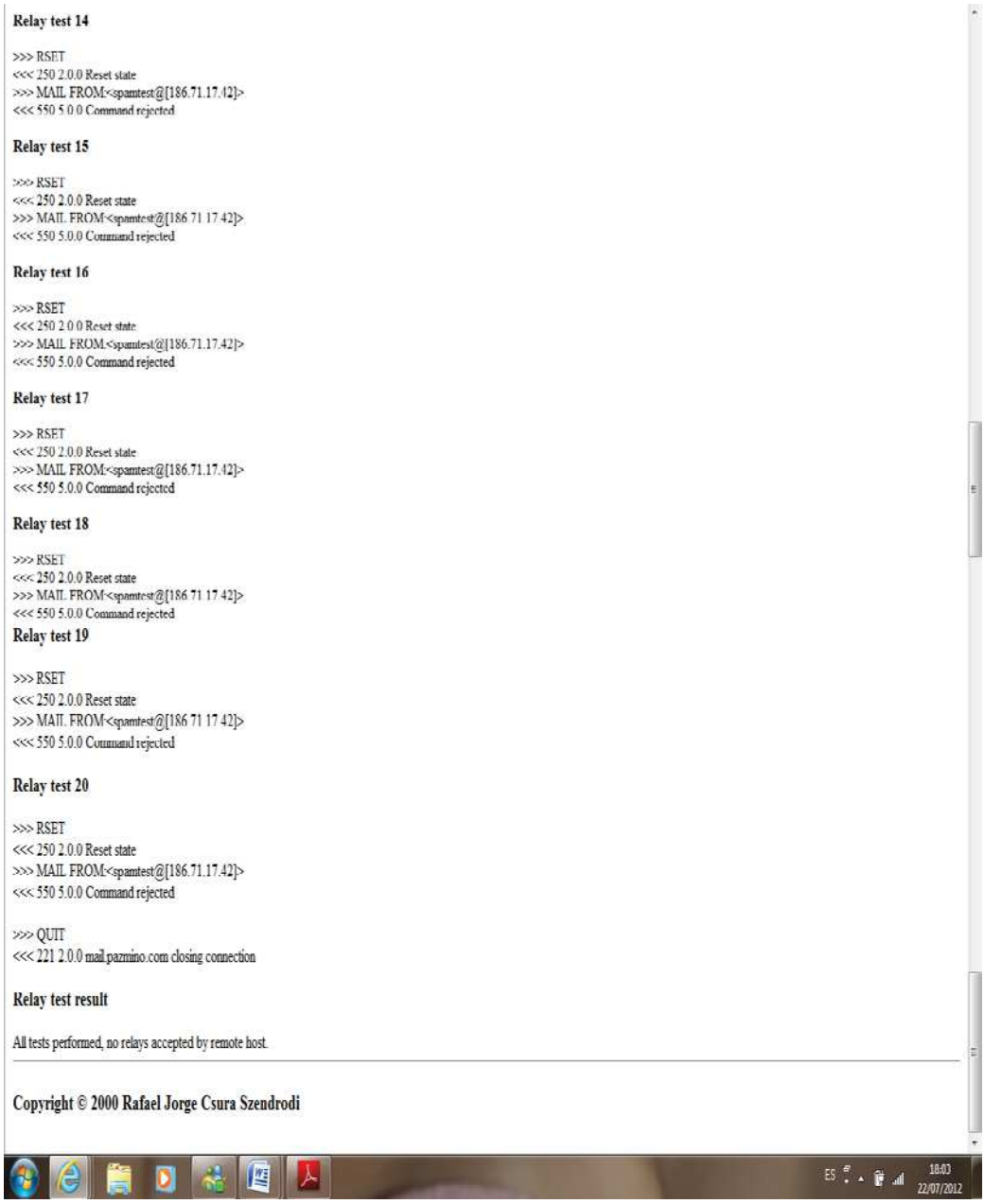


Figura 3.4: Resultados de la prueba del Open Relay Test

3.1.1.2.2 Listas Negras

Una lista negra (Black List), es una lista donde se registran las direcciones IPs que generan Spam de forma voluntaria o involuntaria.

Su funcionamiento consiste en que el servidor de correo verifica IPs o dominios contra una lista negra y si encuentra un coincidente deniega las conexiones

entrantes, esto aplica a todos los tipos de lista negras.

Seguidamente se procederá a evaluar la dirección IP de la empresa a través de la página http://whatismyipaddress.com/blacklist-check; este link pide ingresar la IP y seguidamente procede a ser el respectivo chequeo en las listas que tienen en su servidor.

Como se puede observar en la figura 3.5, se enlista cada uno de los sitios con proceso OK, lo que significa que no está la dirección IP en listas negras.

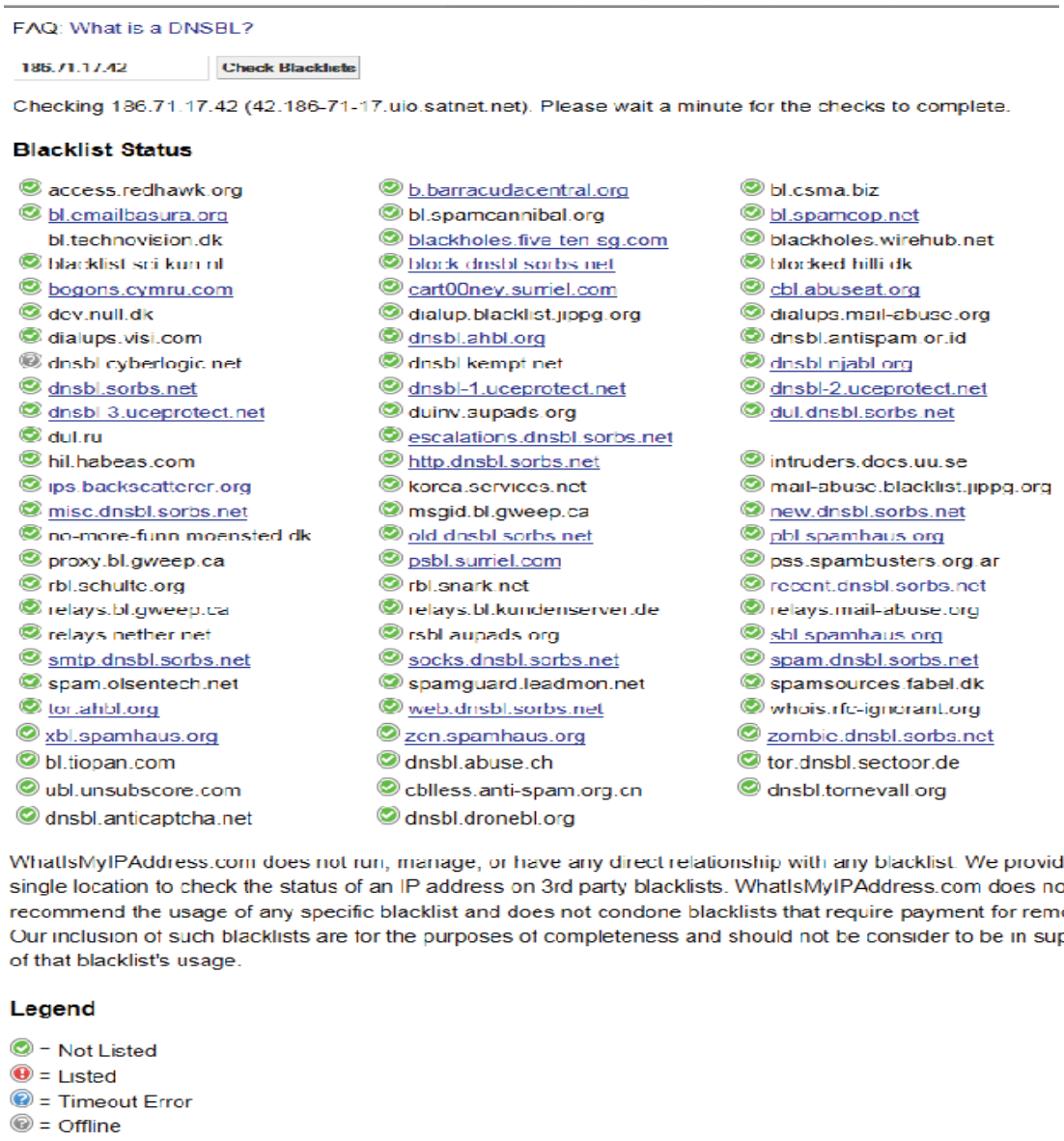


Figura 3.5: Resultados Test de Listas Negras

3.1.1.2.3 Escaneo de Puertos

El término escáner de puertos o escaneo de puertos se emplea para designar la acción de analizar por medio de un programa el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto, cerrado, o protegido por un cortafuego.

Se utiliza para detectar qué servicios comunes está ofreciendo la máquina y posibles vulnerabilidades de seguridad según los puertos abiertos. También puede llegar a detectar el sistema operativo que está ejecutando la máquina según los puertos que tiene abiertos.

Para el escaneo de puertos se utiliza la siguiente dirección http://www.puertosabiertos.com/, la misma que muestra la dirección IP pública de la empresa y la información del navegador

Figura 3.6: Información de la IP y su Navegador

Una vez que se tiene esta información que se muestra en la figura 3.6; se accede a la opción escanear puertos online, el cual mostrará un listado de los puertos que están abiertos o cerrados de acuerdo a los requerimientos de la empresa.

En este caso se observa en la figura 3.7 que tiene 3 puertos abiertos que son el 25, 80, 110.

Para cual se debe revisar si es necesario que dichos puertos estén abiertos, ya que los hackers pueden intentar atacar por medio de estos puertos y causar daños en la red.

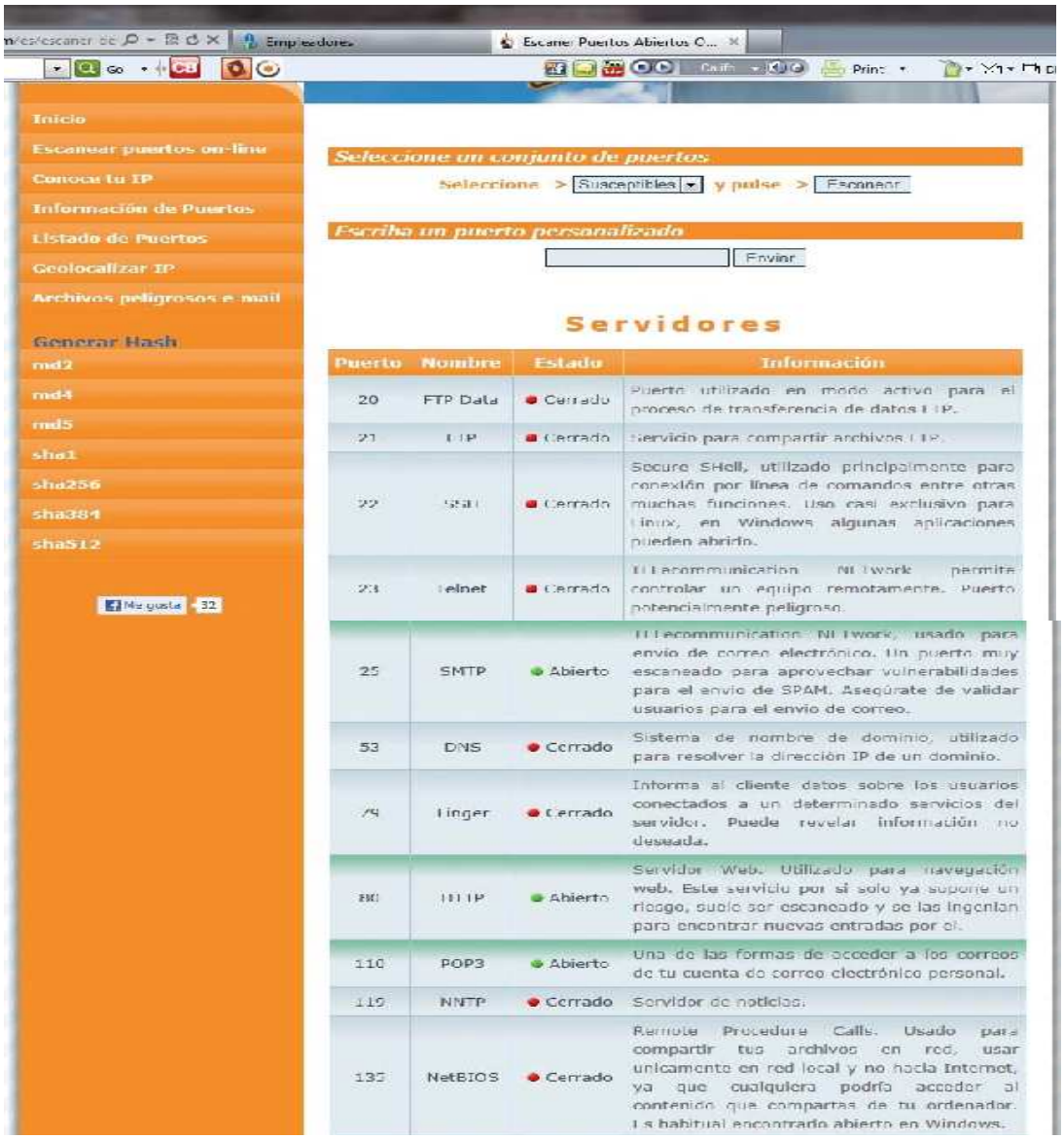


Figura 3.7: Resultado de Escaneo de Puertos

Prueba para evaluar si el servidor de correo tiene protección de antivirus.

Esta prueba es un patrón estándar del EICAR se la encuentra ingresando a la página www.aleph-tec.com/eicar/index.php; la misma que consiste en enviar unas cadenas de código ASSCI imprimibles con diferentes extensiones como texto y comprimidos.

Para comprobar la protección antivirus se enviará los siguientes archivos escogidos en la figura 3.4, luego se ingresará un nombre y la dirección del

correo electrónico donde se enviará la información.

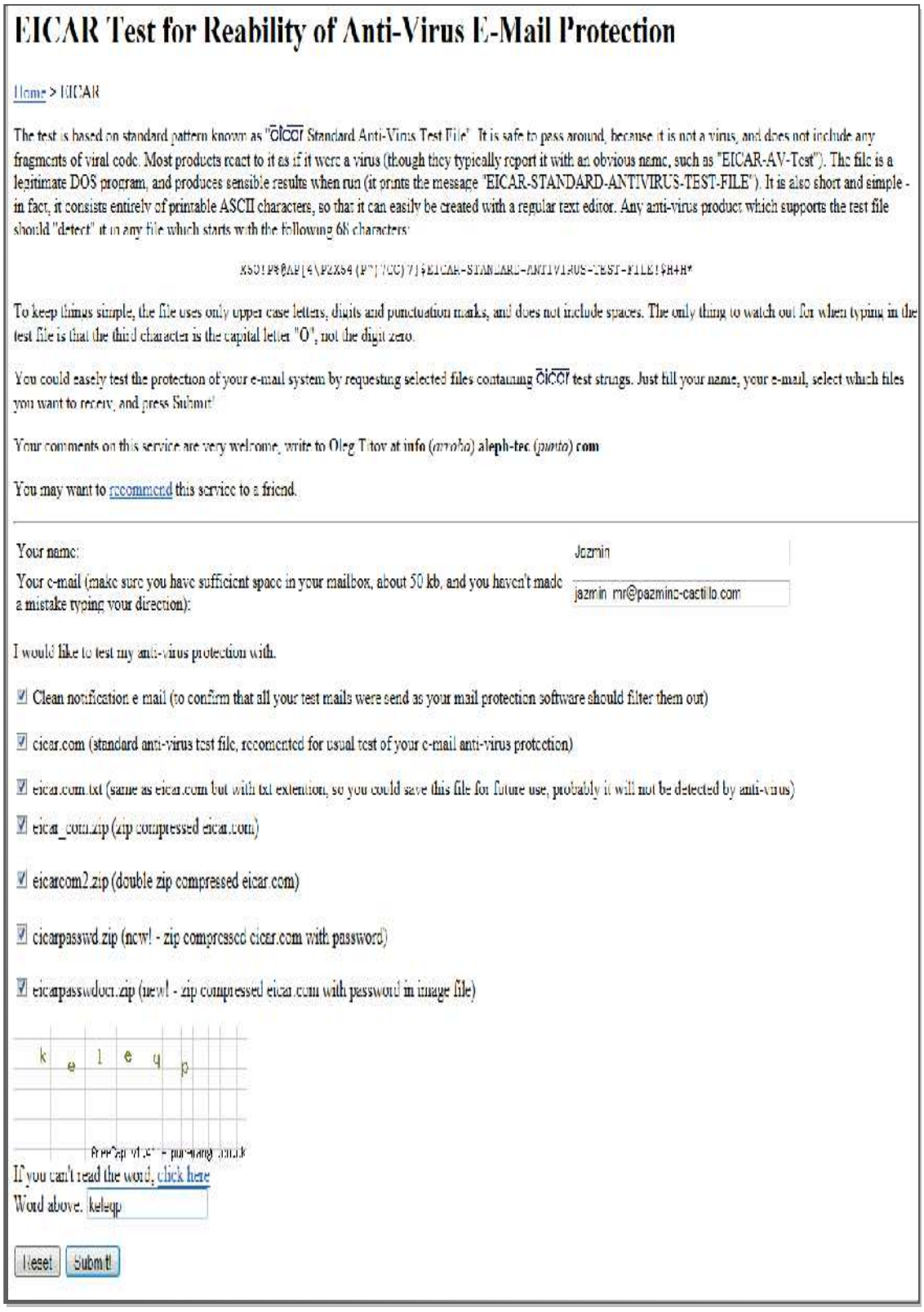
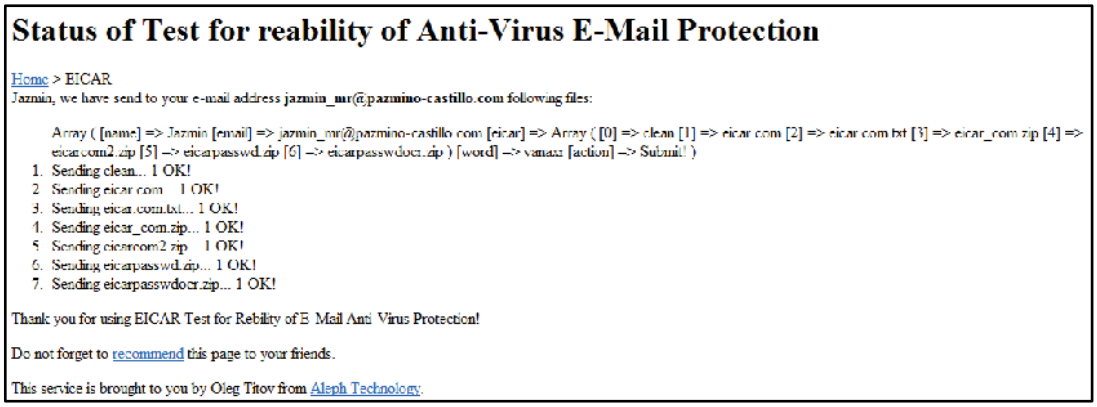


Figura 3.8: Prueba de EICAR, elección de archivos para enviar al correo.

En la figura 3.9 se puede observar que cada archivo se envió sin inconveniente alguno a la dirección del correo electrónico que se ingresó en la figura 3.8.



Status of Test for reability of Anti-Virus E-Mail Protection

Home > EICAR

Jazmin, we have send to your e-mail address jazmin_mr@pazmino-castillo.com following files:

Array ([name] => Jazmin [email] => jazmin_mr@pazmino-castillo.com [eicar] => Array ([0] => clean [1] => eicar.com [2] => eicar.com.txt [3] => eicar_com.zip [4] => eicarcom2.zip [5] => eicarpasswd.zip [6] => eicarpasswdocr.zip) [word] => vanaxi [action] => Submit!)

1. Sending clean... 1 OK!
2. Sending eicar.com ... 1 OK!
3. Sending eicar.com.txt... 1 OK!
4. Sending eicar_com.zip... 1 OK!
5. Sending eicarcom2.zip ... 1 OK!
6. Sending eicarpasswd.zip... 1 OK!
7. Sending eicarpasswdocr.zip... 1 OK!

Thank you for using EICAR Test for Rebility of E Mail Anti Virus Protection!

Do not forget to recommend this page to your friends.

This service is brought to you by Oleg Titov from Aleph Technology.

Figura 3.9: Envío de archivos al correo electrónico proceso OK

Ahora se procederá a revisar el correo electrónico, se puede observar que aparecen varios correos enviados por EICAR como un test y archivo adjunto. Se procede a abrir cada uno de los correos y si el antivirus es eficaz no lo permitirá.

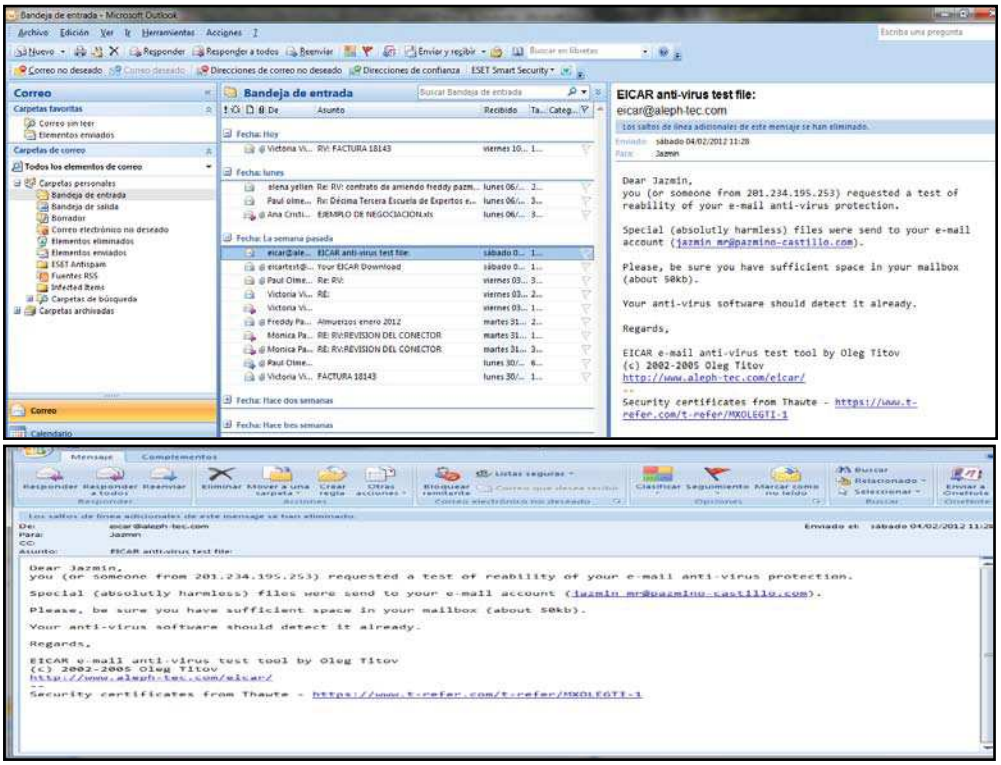


Figura 3.10: Revisión de los correos EICAR

Ahora se procede a abrir el archivo adjunto que se encontraba en la figura 3.10, el mismo que no se podrá acceder debido a que el antivirus lo detecta como un virus y deniega el acceso, tal como se muestra en la figura 3.12.

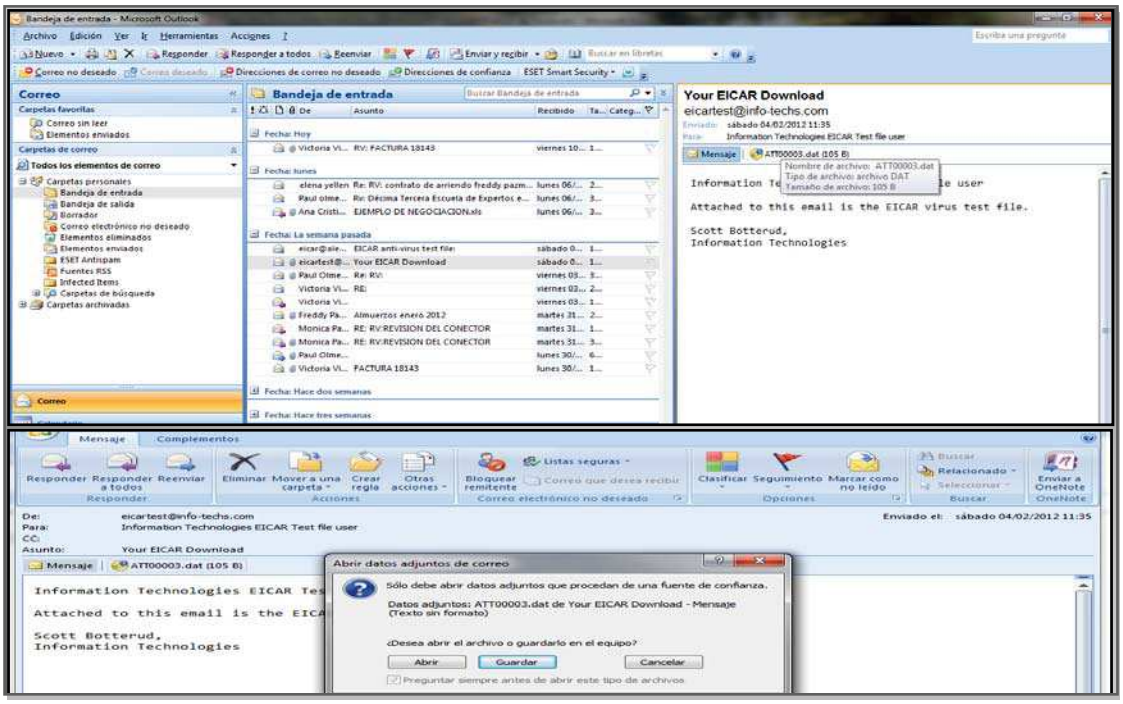


Figura 3.11: Descarga del archivo adjunto

Finalmente se puede observar que el antivirus denegó el acceso para poder revisar el archivo adjunto enviado desde la página EICAR.

Figura 3.12: Detección de virus al descargar el archivo

3.1.1.2.4 Server Test

Servidor de Prueba (Server test), mediante esta opción se logra evaluar la duración de contestación de cualquier servidor y comprueba el respectivo estado.

Como se puede observar en la figura 3.13, los resultados de esta prueba son exitosos sin ninguna novedad.

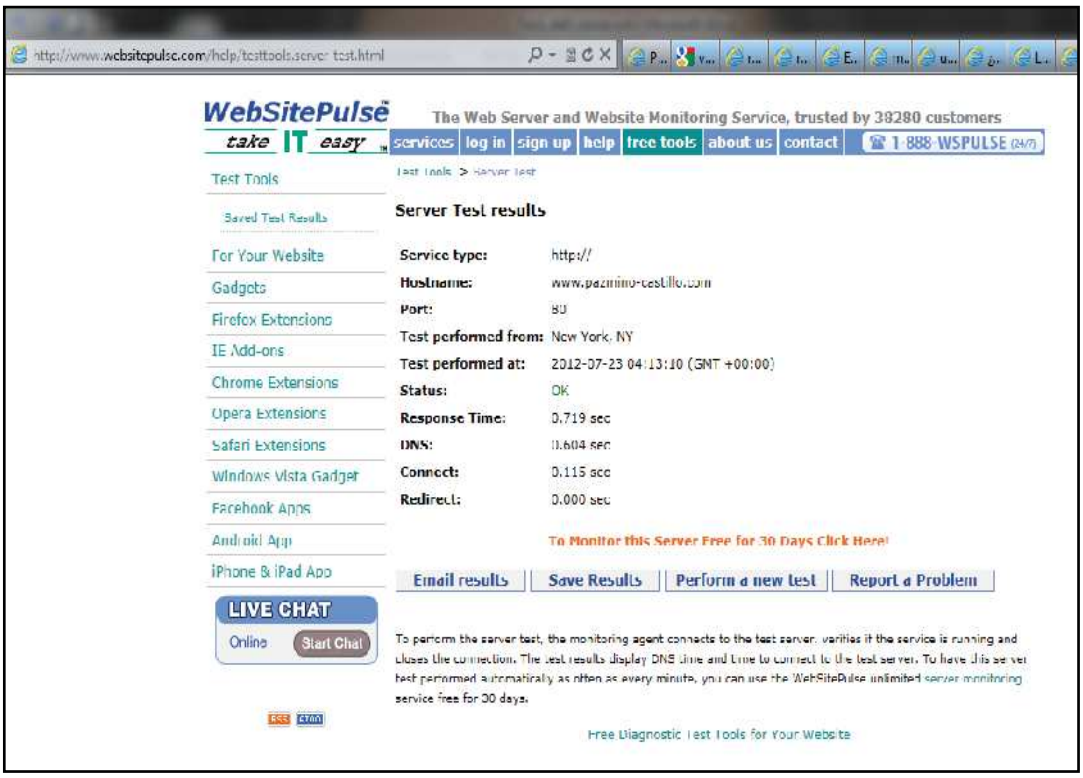


Figura 3.13: Resultado del servidor de prueba.

3.1.1.2.5 E-mail Address Validation Test

Prueba de validación de correo electrónico (E-mail AddressValidation Test) consiste en verificar si una dirección de correo se conecta con el servidor, y a la vez ver si es correcta o no.

Para realizar esta prueba se utiliza la dirección web www.website pulse.com/help/testtools.emailvalidation-test.html, muestra que la

dirección de correo ingresada es válida y que no tuvo ningún inconveniente al momento de realizarla.

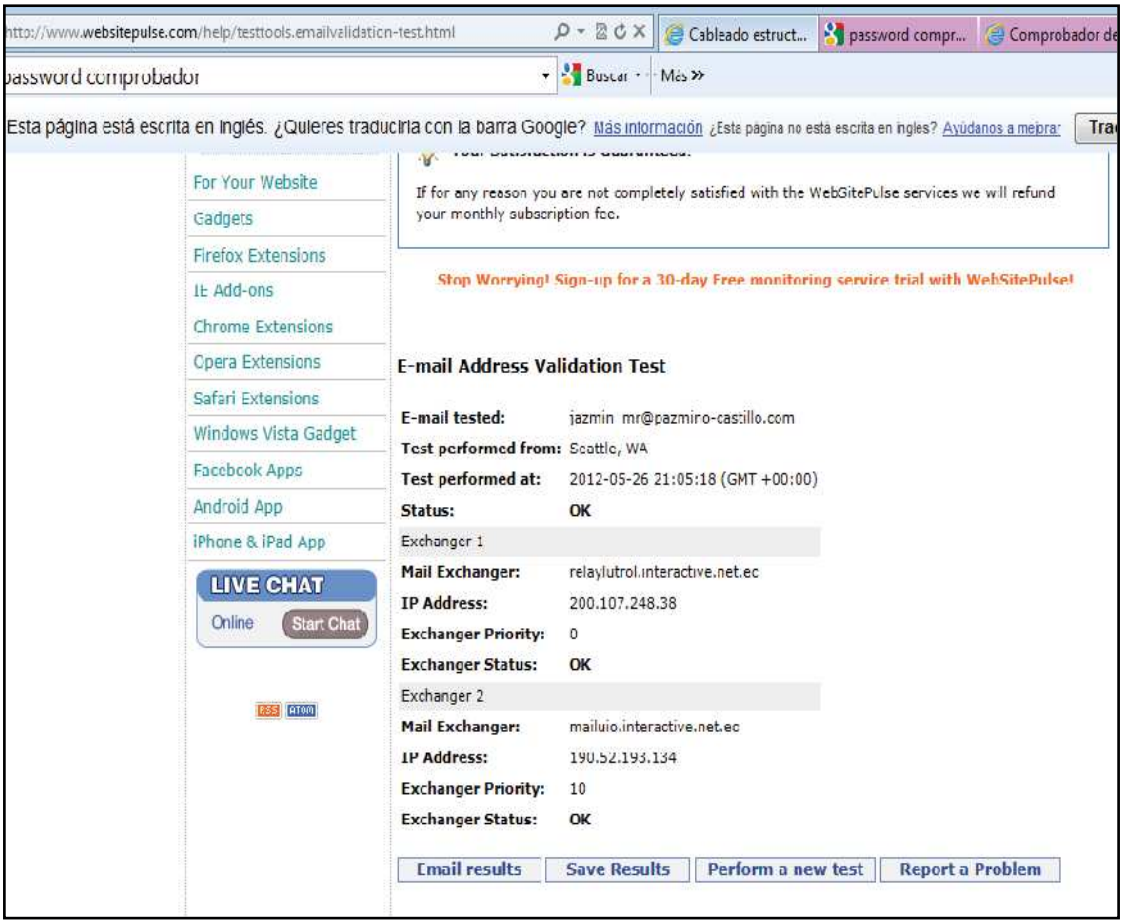


Figura 3.14: Prueba Validación de correo

3.1.2 Servidor DNS

El sistema de nombres de dominio (DNS); se encarga de asignar nombres equivalente a un dirección IP; a las equipos de los usuarios y servicios de red.

El DNS se utiliza para distintos propósitos, como la resolución de nombres; dado el nombre completo de un host, se obtiene su dirección IP, o a la inversa dada una dirección IP se obtiene el nombre asociado a la misma. También se utiliza para la resolución de servidores de correo, dado un nombre de dominio; obtener el servidor a través del cual debe realizarse la entrega del correo electrónico.

Para la evalución del DNS, se utilizó la página www.squish.net; teniendo el siguiente resultado.

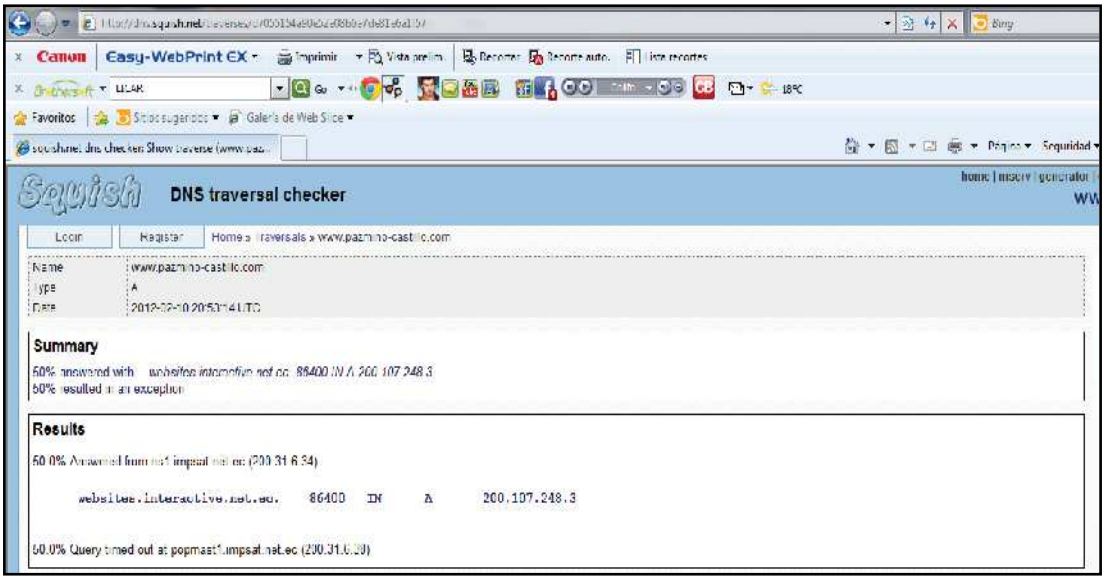


Figura 3.15: Resultados de la evaluación del DNS con el dominio.

Para evaluar más exhaustivamente el DNS se utiliza la prueba y comprobación en la siguiente página http://www.dnssy.com/, la misma que presenta un informe detallado sobre el DNS en la figura 3.17. En este informe se podrá ver los problemas y la configuración para un determinado dominio, proporcionando a su vez recomendaciones para mejorar la seguridad y el rendimiento.

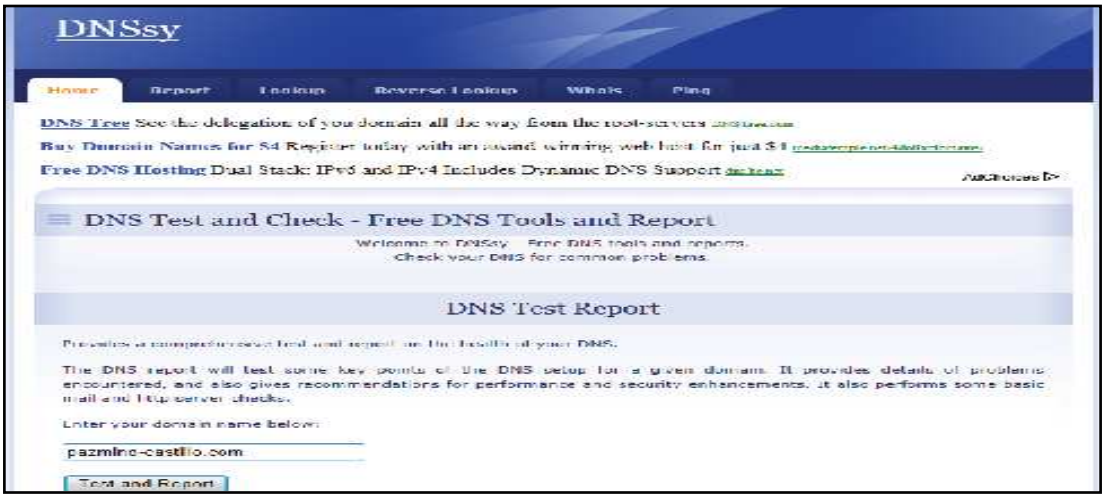


Figura 3.16: Ingreso del dominio para prueba Exhaustiva del DNS

DNS Test and Check - Free DNS Report

DNSsy Report Results

Results for pazmino-castillo.com

Test	Results	Status
Checking domain format:	Hostname looks good.	Pass
Checking for parent nameservers:	Found 13 parent nameservers.	Pass
Checking for parent glue:	Glue from root nameservers to parent nameservers is missing. This means that an extra lookup is required to find your parent nameservers. There is nothing you can do about this.	Info
NS records at parent nameserver:	Your NS records at your parent nameserver are: idns2.interactive.net.ec [no glue] TTL 172800 idns1.interactive.net.ec [no glue] TTL 172800 Provided by a.gtld-servers.net	Info
Nameservers listed at parent:	Your nameservers are listed at the parent nameserver.	Pass
Glue at parent nameservers:	Glue is not provided from parent nameserver to your nameservers. This means they did not provide the IP address of your nameservers, so an extra step is required to resolve your domain, giving slower lookup times. This is common if your nameservers are in a different TLD than your domain name. The following nameservers did not have glue: idns2.interactive.net.ec idns1.interactive.net.ec	Performance
Nameserver name validity:	The parent nameserver responded with NS records that appear valid.	Pass
Nameserver A records:	All of your nameservers have A records.	Pass
Nameserver A records match parent glue:	No glue - test cannot be performed.	Info
NS records at your nameservers:	Your NS records at your nameservers are: **idns2.interactive.net.ec reported:** idns2.interactive.net.ec [190.52.193.133] TTL 43200 idns1.interactive.net.ec [190.52.193.132] TTL 43200 **idns1.interactive.net.ec reported:** idns1.interactive.net.ec [190.52.193.132] TTL 43200 idns2.interactive.net.ec [190.52.193.133] TTL 43200	Info
Nameservers listed at your nameservers:	Your nameservers are listed at your nameservers.	Pass
Glue at your nameservers:	Glue is provided by your nameservers. This means they provided the IP address of your nameservers.	Pass
Nameserver A records match nameserver glue:	All of the glue provided by your nameserver matches the A records for your nameservers.	Pass
Parent glue matches your glue:	The glue provided by the parent nameserver and your nameserver matches.	Pass
Nameservers match (parent):	All nameservers returned by the parent nameserver are also returned by your nameserver.	Pass
Nameservers match (yours):	All nameservers returned by the your nameservers are also returned by the parent nameserver.	Pass
All nameservers responded:	All of your nameservers responded.	Pass
Only root nameservers returned:	Your nameservers returned at least 1 non-root nameserver reference.	Pass
Any root nameservers returned:	Your nameservers did not return any root nameserver references.	Pass
All of your nameservers match:	All of your nameservers return the same nameserver records.	Pass
All of your nameservers return an A record:	Some of your nameservers failed to return an A record for your domain. This is probably not what you want. The following nameservers did not return an A record: idns1.interactive.net.ec idns2.interactive.net.ec	Warning
Recursive lookups:	Some of your nameservers provide recursive lookups. This is bad since it could be used to poison caches or other DNS attacks. The following nameservers indicated that they support recursive lookups: idns1.interactive.net.ec	Security
Nameservers respond authoritatively:	All of your nameservers responded authoritatively for your domain.	Pass
Nameserver name validity:	All of your nameservers responded with NS records that appear valid.	Pass
Number of nameservers:	You have only 2 nameservers, which is the minimum allowed. There is a chance that they could both fail simultaneously. Although not necessary, you should consider increasing the number of nameservers to 3.	Warning

CNAME returned:	No CNAMES found when looking up your domain at your nameservers.	Pass
Nameservers on different class C:	Your nameservers are all on the same class C IP nomenclature. This is an indication (but not proof) that they may be co-located, which could be a risk should the internet connection to that location fail.	Warning
Nameservers on private IPs:	Your nameservers appear to be on public IP addresses.	Pass
SOA record:	Your SOA record at idns2.interactive.net.ec: Serial: 2011110000 Master Nameserver: idns1.interactive.net.ec. Hostmaster eMail: root.interactive.net.ec. Refresh: 10800 (3 hours) Retry: 3600 (60 mins) Expire: 604800 (7 days) Minimum TTL: 86400 (24 hours)	Info
Number of SOA records:	Each of your nameservers returned exactly 1 SOA record.	Pass
SOA Serial Match:	Each of your nameservers returned the same SOA serial number.	Pass
SOA Master Nameserver Match:	Each of your nameservers returned the same SOA master nameserver.	Pass
SOA Admin Email Match:	Each of your nameservers returned the same SOA admin email address.	Pass
SOA Refresh Match:	Each of your nameservers returned the same SOA refresh value.	Pass
SOA Retry Match:	Each of your nameservers returned the same SOA retry value.	Pass
SOA Expire Match:	Each of your nameservers returned the same SOA expire value.	Pass
SOA Minimum TTL Match:	Each of your nameservers returned the same SOA minimum TTL value.	Pass
SOA Serial Number:	Your SOA serial number is 2011110000. This does not match the recommended format of YYYYMMDDnn (RIPE-203). This is not necessarily a problem as long as	Warning
SOA Master Nameserver:	Your SOA master nameserver is idns1.interactive.net.ec. It is also listed at the parent nameservers. This is correct.	Pass
SOA Admin Email:	Your SOA admin email address is root@interactive.net.ec. This seems to be a valid email address.	Pass
SOA Refresh:	Your SOA refresh value is 3 hours. This specifies how often a slave nameserver checks for DNS updates at the master. This value is in OK. RFC 1912 recommends values between 20 minutes and 12 hours.	Pass
SOA Retry:	Your SOA retry value is 60 mins. This is the time a slave nameserver will wait if an attempt to contact a primary nameserver failed before it tries again. This seems to be OK.	Pass
SOA Expire:	Your SOA expire value is 7 days. This is how long a slave nameserver will cache data if it cannot reach the master nameserver. If your master nameserver is unreachable for longer than this your slave nameservers will no longer cache your DNS. This seems to be OK.	Pass
SOA Minimum TTL:	Your SOA minimum TTL value is 24 hours. This is interpreted by servers as the default TTL. It can be overridden on individual DNS entries. This seems high. This means that if you make DNS changes those changes may not propagate throughout the internet for a long time.	Warning
MX records:	I found the following MX records: relaylutro1.interactive.net.ec 0 [200.107.248.30] mailin.interactive.net.ec 10 [190.52.193.134] This is all of the MX servers I found.	Info
All nameservers return same MX:	All of your nameservers returned the same MX records.	Pass
MX records have A records:	All of your MX servers have A records.	Pass
MX records have CNAMEs:	None of your MX servers have CNAME records. This is good.	Pass
MX records are IPs:	None of your MX records are IP addresses. This is good.	Pass
MX records are valid:	All of your MX records appear to be valid hostnames.	Pass
MX use public IPs:	All of your MX servers have public IP addresses.	Pass
MX IPs have reverse DNS:	All of your MX servers have reverse DNS (PTR) entries. This is good since some mail server will refuse to accept email from you.	Pass
Connecting to MX 200.107.248.30:	I was unable to connect to the SMTP port on 200.107.248.30. I only waited 5 seconds, so it may be that your mail server is slow, or may not be responding. Skipping further tests for 200.107.248.30	Fail
Connecting to MX 190.52.193.134:	I was unable to connect to the SMTP port on 190.52.193.134. I only waited 5 seconds, so it may be that your mail server is slow, or may not be responding. Skipping further tests for 190.52.193.134	Fail
WWW record:	You have a WWW record setup for your domain. www.pazmino-castillo.com -> 200.107.248.3	Pass
WWW is public:	Your WWW record is a public IP address.	Pass
Connecting to WWW server:	Connected to WWW port on www.pazmino-castillo.com OK.	Pass
Checking HTTP version:	HTTP version 1.1 supported.	Pass
WWW server type:	Your web server says it is: Microsoft-IIS/7.0	Info
WWW server version:	Your web server appears to reveal version information. This can pose a security risk if vulnerabilities are identified in this version. You should consider disabling version information in your server configuration.	Security
WWW home page:	Your web server returned the home page of your web site.	Pass

Check another domain by entering the domain name below:

Test and Report

Figura 3.17: Resultados de la comprobación exhaustiva del DNS

3.1.3 Servidor Proxy

La función del servidor Proxy consiste en interceptar las conexiones de red que un cliente hace a un servidor de destino, por varios motivos como seguridad, rendimiento, anonimato, etc. Esta función puede ser realizada por un programa o dispositivo.

Para la evaluación del servidor se utilizó una lista de proxys anónimos. Esto se debe a las políticas de acceso que tiene la empresa para navegar en la web. Esta prueba se realizará tomando de ejemplo la página de facebook que es uno de los lugares restringuidos; se intentará ingresar, pero como se muestra en la figura 3.18 no se puede acceder a la dirección solicitada.

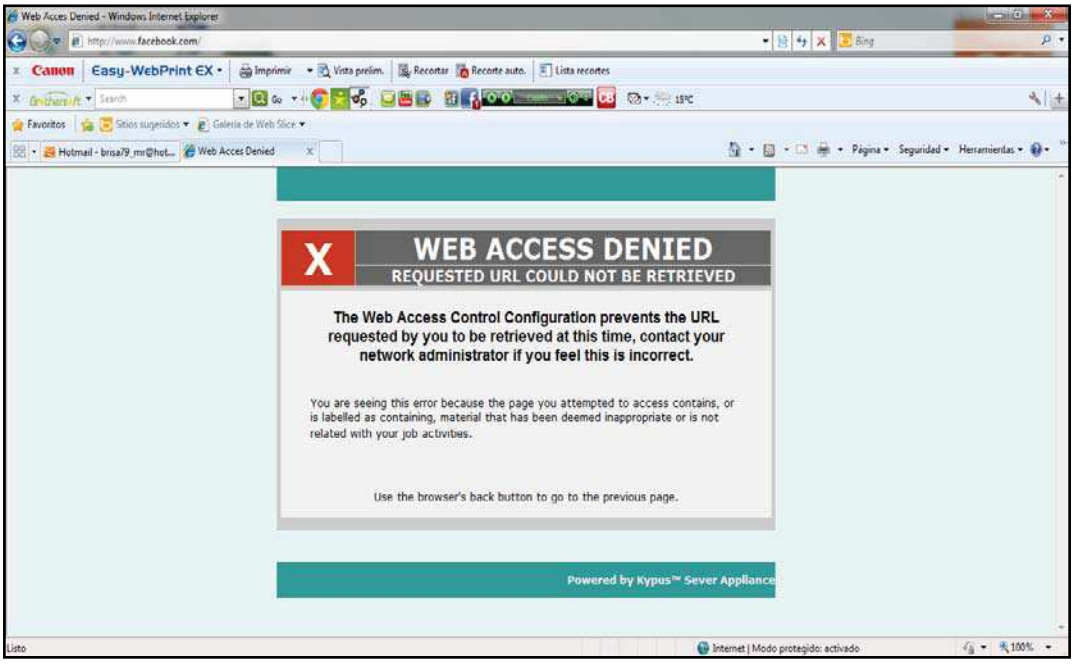


Figura 3.18: Ingreso al Facebook, página restringida a la navegación

Ahora a través de un buscador en este caso Google, se investiga en la página web un listado de direcciones de proxy anónimos, algunos de ellos que se encuentran enlistados permitirá navegar en la página solicitada.

Se procede a la búsqueda, numerosas veces con el listado de proxy; pero como se muestra en la figura 3.19 hasta ahora todos los intentos son fallidos.

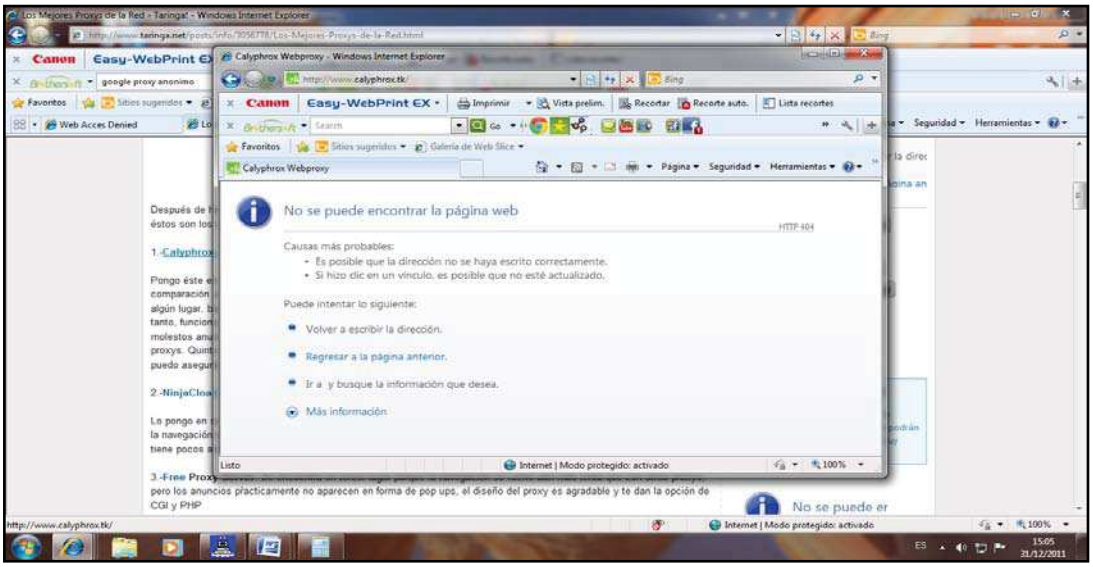


Figura 3.19: Búsqueda fallida en el proxy anónimo

Finalmente después de algunos intentos, del listado se pudo encontrar una página donde permitió acceder al sitio requerido, en este caso el link fue www.esproxy.com.

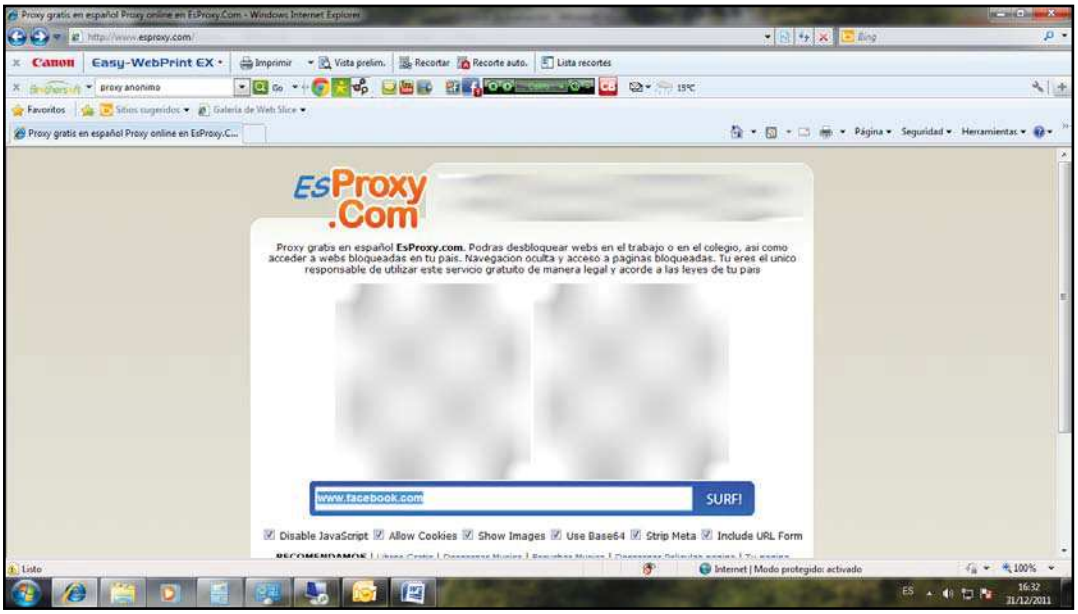


Figura 3.20: Navegación por medio del proxy anónimo

Ahora se accederá a navegar a la página requerida www.facebook.com, se observa en la figura 3.21 que se ingresó sin ningún problema; lo que significa

que a través de este proxy anónimo se puede navegar tranquilamente a los sitios restringidos.

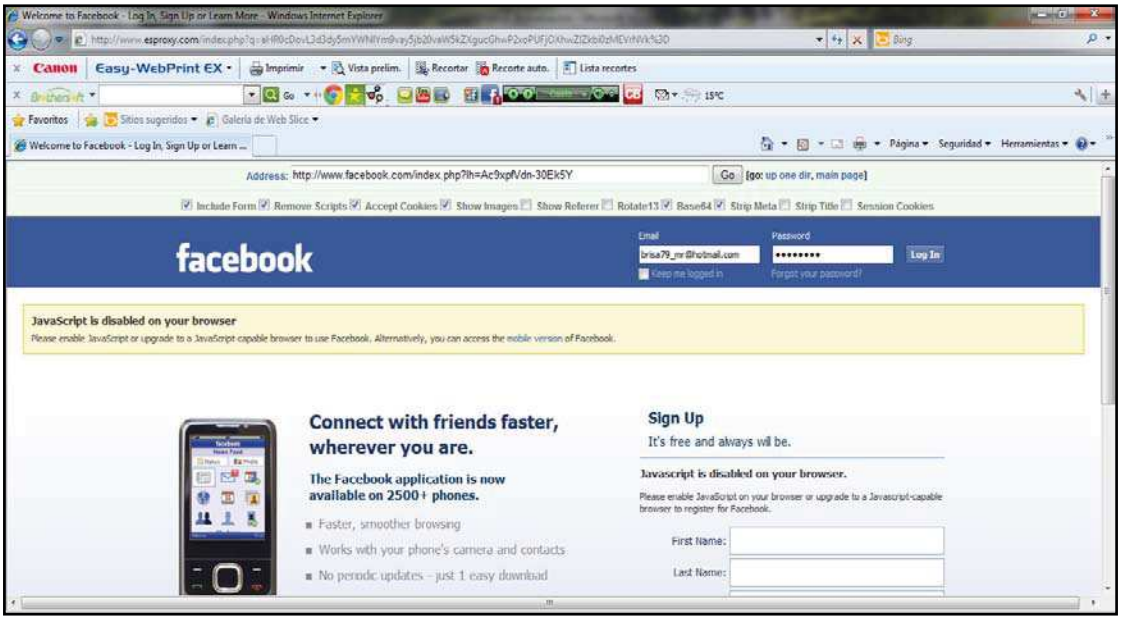


Figura 3.21 Ingreso a la página de Facebook

Después de digitar el usuario y clave se observa que el ingreso fue satisfactorio y se puede navegar sin ningún inconveniente en la página solicitada.

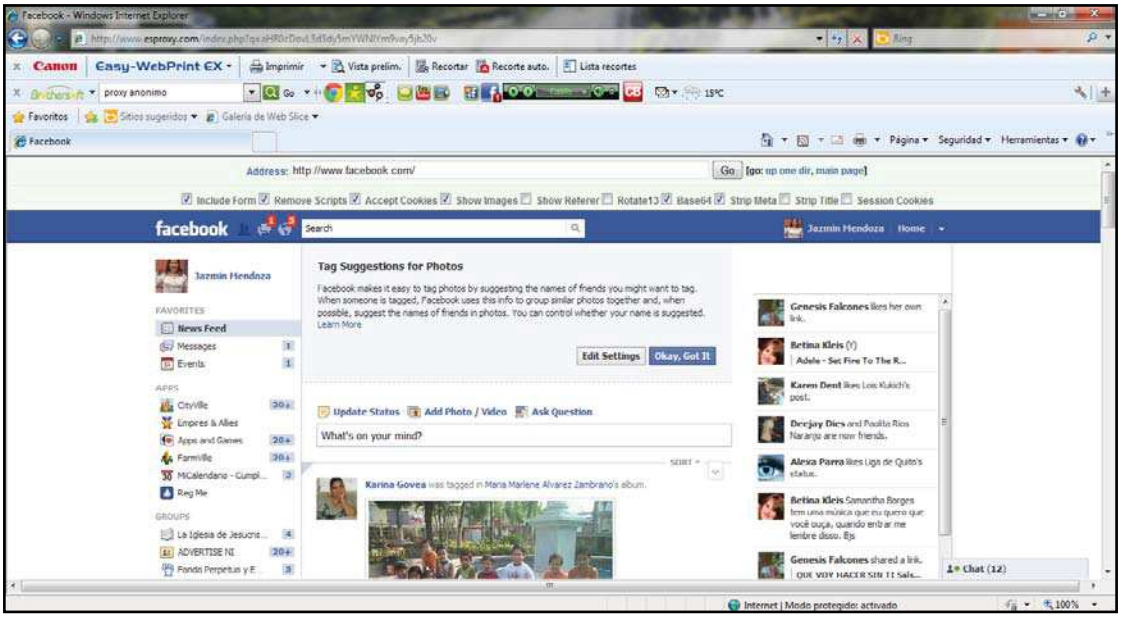


Figura 3.22: Navegación en la página Facebook

3.1.4 Evaluación de equipos terminales y dispositivos en la infraestructura de la red

Para la evaluación de los equipos terminales se procedió a revisar en cada terminal los perfiles de usuarios y los privilegios que gozan cada uno de los empleados. Con respecto a la evaluación de las contraseñas se utilizaron software tales como él: Passwordmeter y John the Ripper los mismos que permitieron ver la robustez de cada clave.

3.1.5 Evaluación de Wireless

Para la evaluación del wireless se utilizó el software WirelessNetView que se lo puede descargar desde esta dirección web http://wirelessnetview.softonic.com/; el mismo que sirve para detectar las redes que se encuentran disponibles y ver las características especificas de cada conexión.

Como se muestra en la figura 3.23, hay diferentes redes que se encuentran por la zona donde está instalado el router.

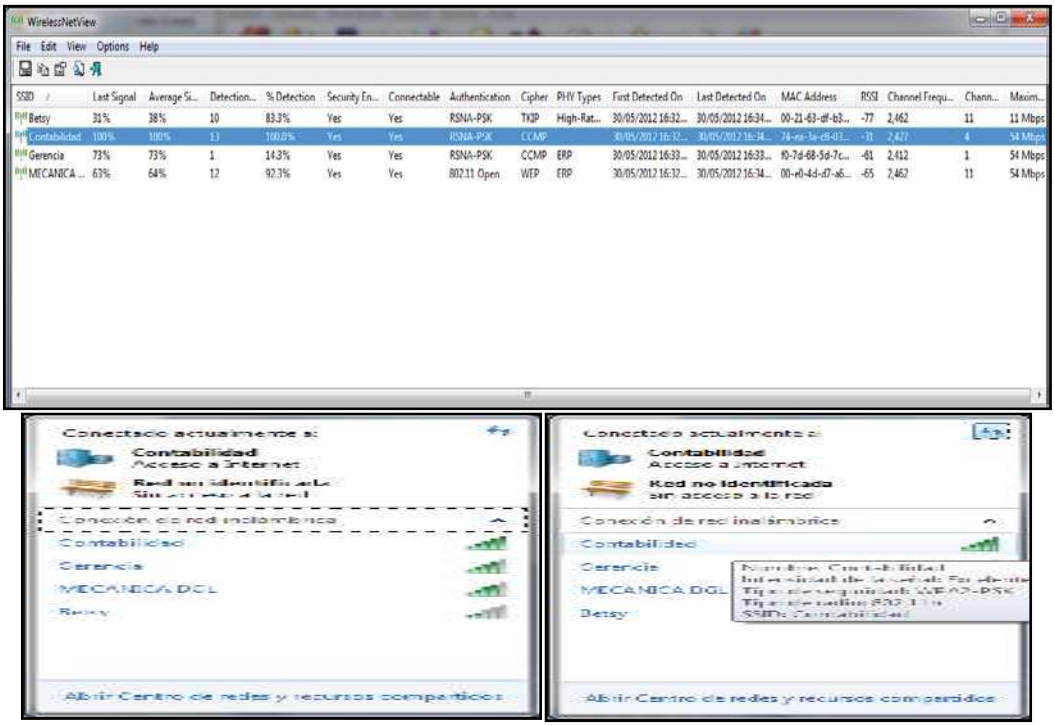


Figura 3.23: Representación Red Wireless de Contabilidad

En la siguiente figura 3.24, se capturarán los detalles de la red wireless que se encuentra en el segundo piso de la empresa.

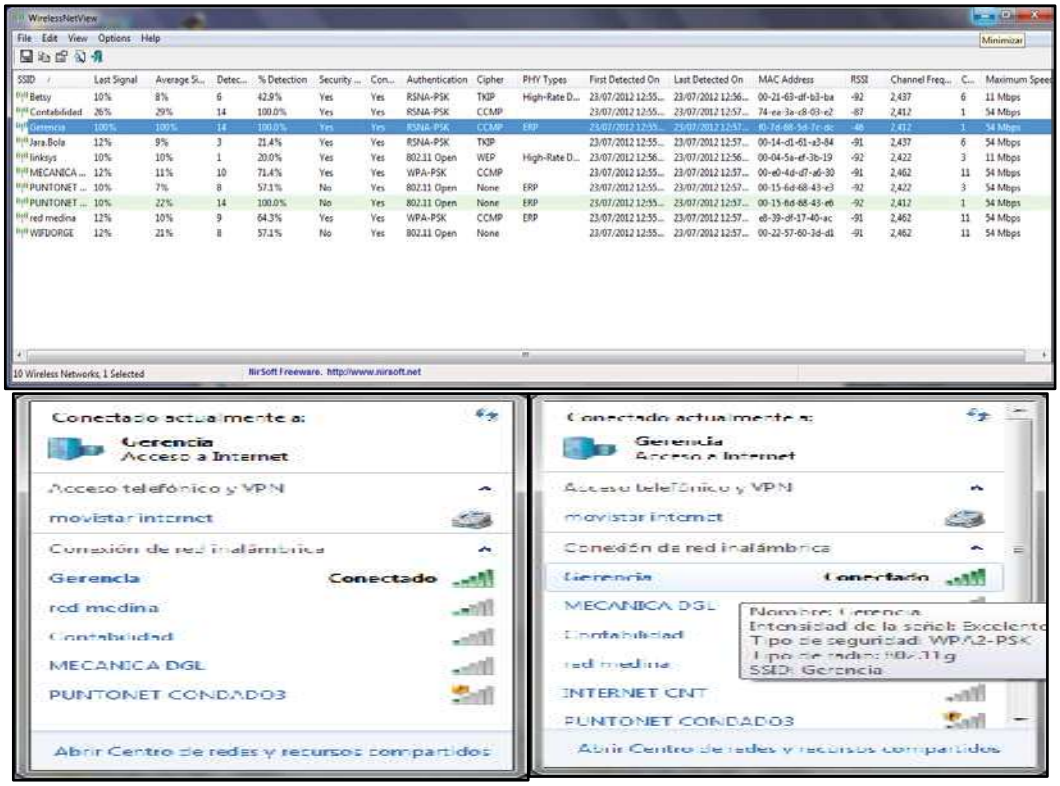


Figura 3.24: Representación Red Wireless Gerencia

3.1.6 Evaluación de contraseñas

Para la evaluación de las contraseñas se utilizó el programa John the Ripper, el mismo que permite descifrar a “fuerza bruta” la contraseña del equipo.

Se probó en cada uno de los equipos que poseían windows XP y como se muestran en las figura 3.28 se puede ver que en cuestión de segundos descifró la contraseña; lo que significa que no poseen contraseña segura. De la misma manera se procedió hacer las respectivas pruebas en los equipos que tienen Windows 7, pero los intentos fueron fallidos ya que John the Ripper no funciona para este SO.

En esta prueba se direcciona al disco donde se encuentra almacenado el archivo que se va ejecutar. En este caso D:\pwd seguidamente se digita el

siguiente comando D:\pwd>pwdump7 >misclaves.txt, tal como se muestra en la figura 3.25.

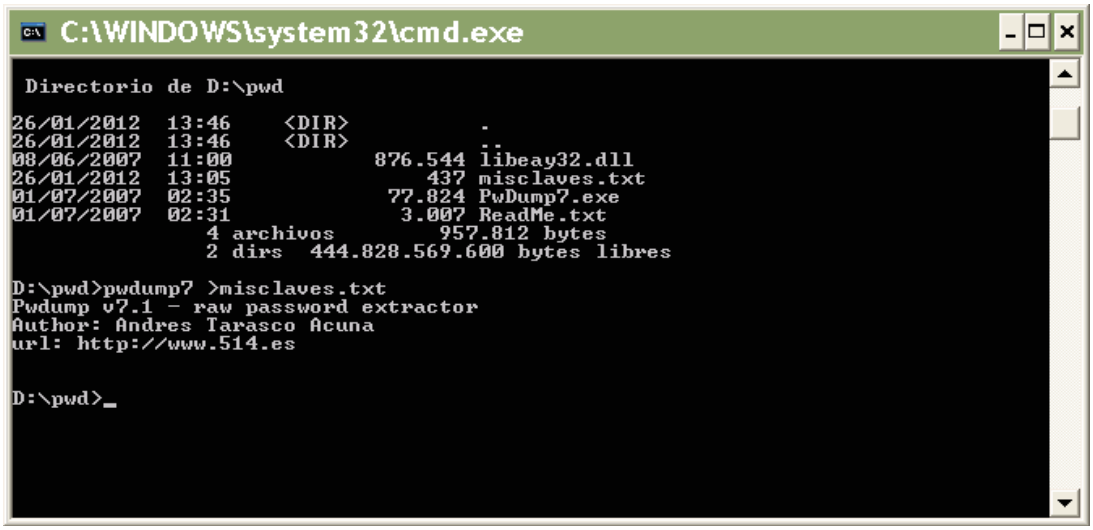


Figura 3.25: Ingreso a la información del archivo a ejecutarse.

Seguidamente en la figura 3.26, se mostrarán los usuarios que se encuentran creados en el computador con el password cifrado.

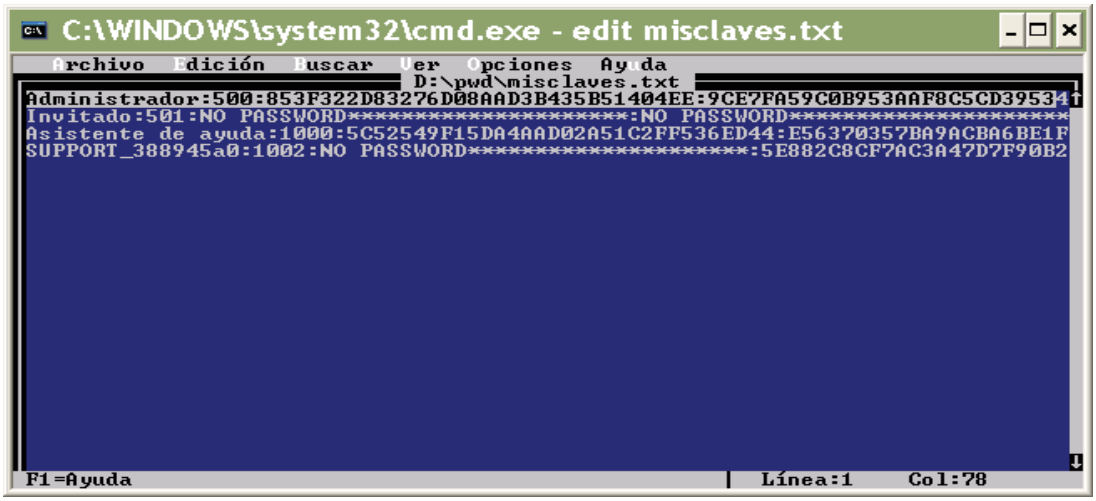


Figura 3.26: Resultados de usuarios encontrados con password cifrado.

Luego se debe salir de la ventana que se muestra en la figura 3.26 para editar y copiar el archivo donde se encuentran las claves. Los comandos son los siguientes:

D:\pwd>edit misclaves.txt

D:\pwd>copy misclaves.txt D:\john176\run

D:\pwd>cd D:\john176\run

D:\john176\run>dir

Este último comando desplegará la lista del directorio en donde se encontrará el archivo que se utilizará para descifrar la contraseña del equipo. Segudamente se procederá a ejecutar el comando que finalmente encontrará la clave; si esta es robusta tal vez no se pueda descifrar o durará horas para forzar su identidad; pero si es muy débil, el programa la descifrará en cuestión de segundos.

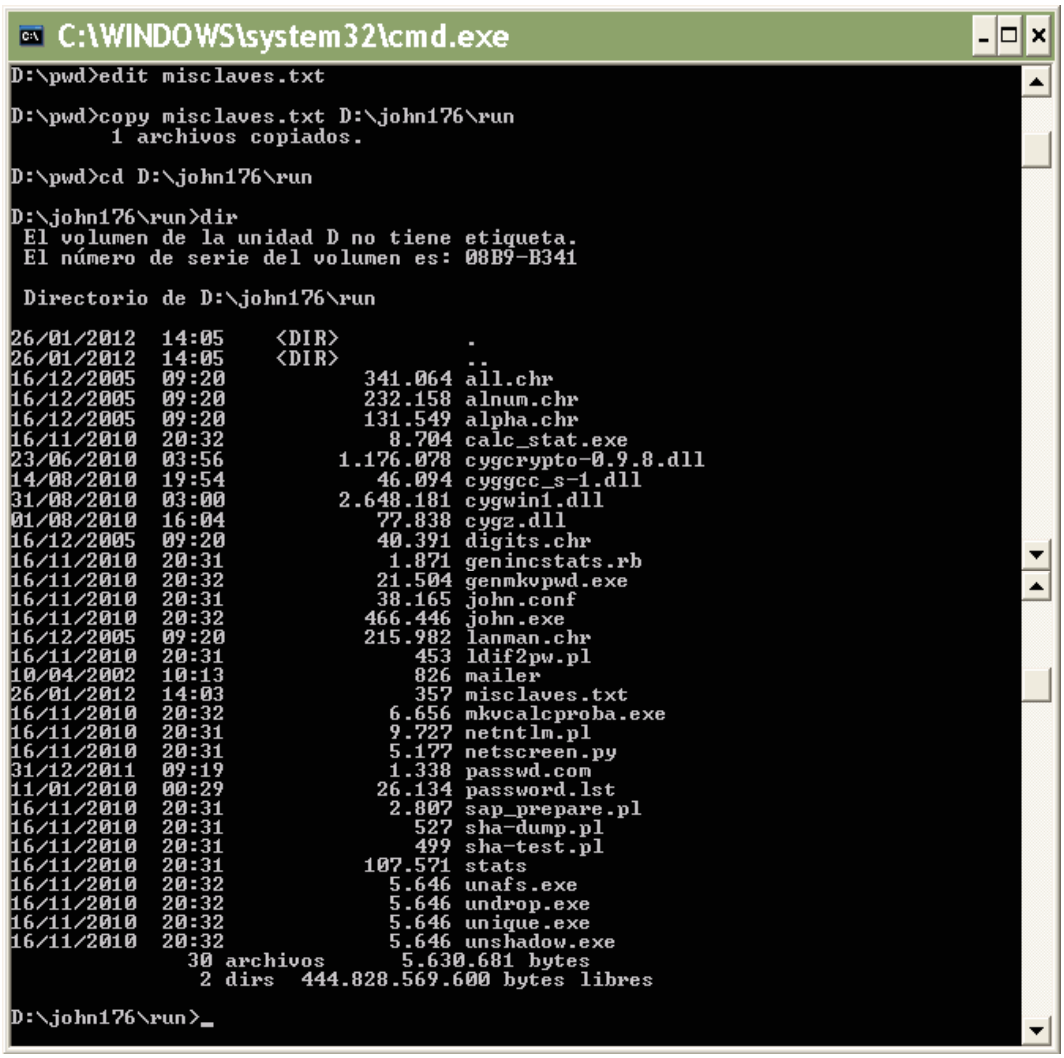


Figura 3.27: Despliegue de archivos contenidos en John the Ripper

Finalmente una vez ejecutado cada uno de los pasos; se procede al descifrado de la clave, este resultado se lo puede observar en la figura 3.28; en este caso no se tomó mucho tiempo para obtener la clave del computador.

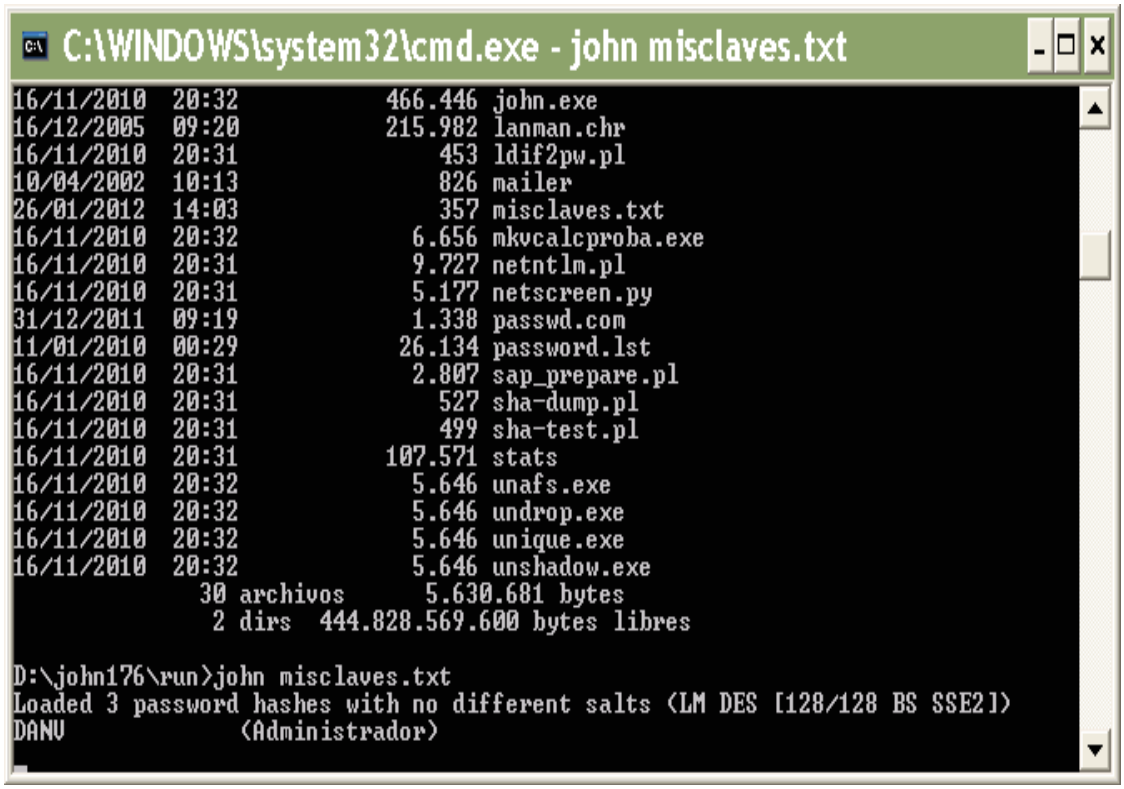


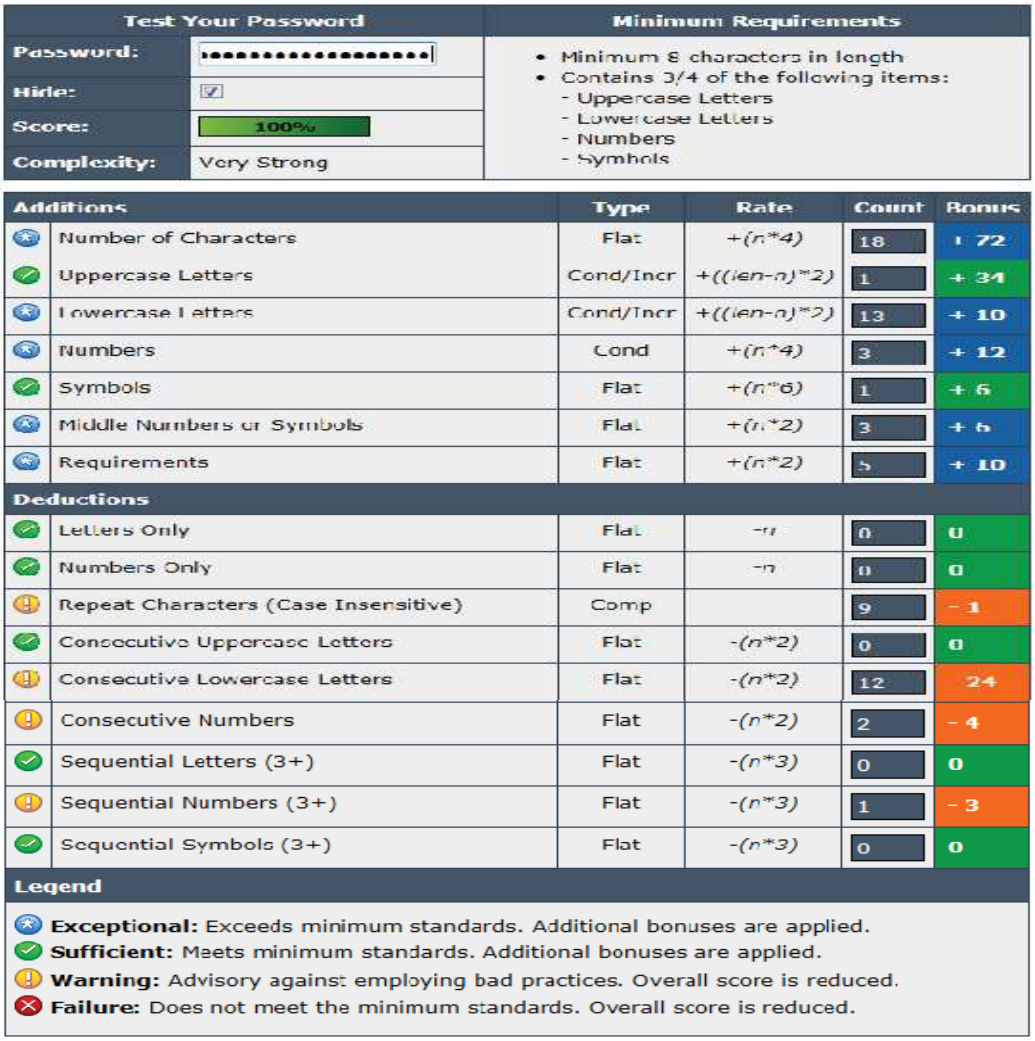
Figura 3.28: Resultado de la clave a través de John the Ripper.

Ahora se procederá a evaluar la robustez de las contraseñas en los dispositivos y equipos terminales de la infraestructura de la red.

Para esta evaluación se necesitará ingresar a la siguiente dirección http://www.passwordmeter.com/; donde se encontrará una aplicación para evaluar la solidez de una contraseña.

Esta aplicación proporciona un medio al usuario para mejorar la robustez de las contraseñas y mantener un buen hábito para no crear contraseñas incorrectas.

En este momento se procederá a escribir la contraseña para el router, se puede observar que es una contraseña muy fuerte y que difícilmente un hackers podrá acceder al equipo.



Test Your Password	
Password:	••••••••••••••••••••
Hide:	☑
Score:	100%
Complexity:	Very Strong

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

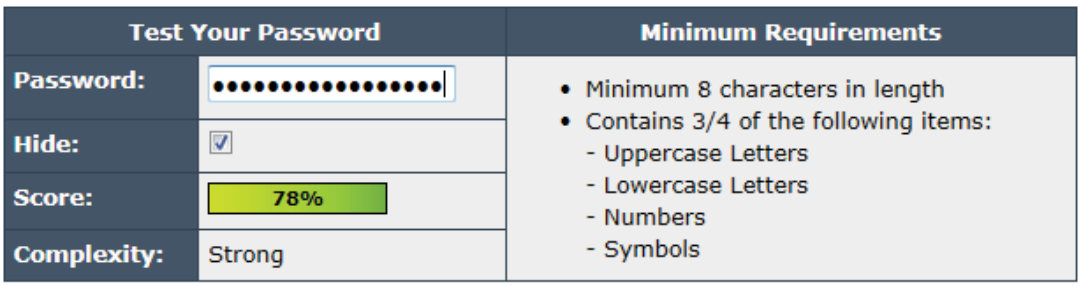
Additions	Type	Rate	Count	Bonus
Number of Characters	Flat	+(n*4)	18	+ 72
Uppercase Letters	Cond/Incr	+((len-n)*2)	1	+ 34
Lowercase Letters	Cond/Incr	+((len-n)*2)	13	+ 10
Numbers	Cond	+(n*4)	3	+ 12
Symbols	Flat	+(n*6)	1	+ 6
Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
Requirements	Flat	+(n*2)	5	+ 10
Deductions				
Letters Only	Flat	-n	0	0
Numbers Only	Flat	-n	0	0
Repeat Characters (Case Insensitive)	Comp		9	- 1
Consecutive Uppercase Letters	Flat	-(n*2)	0	0
Consecutive Lowercase Letters	Flat	-(n*2)	12	24
Consecutive Numbers	Flat	-(n*2)	2	- 4
Sequential Letters (3+)	Flat	-(n*3)	0	0
Sequential Numbers (3+)	Flat	-(n*3)	1	- 3
Sequential Symbols (3+)	Flat	-(n*3)	0	0

Legend

Exceptional: Exceeds minimum standards. Additional bonuses are applied.
Sufficient: Meets minimum standards. Additional bonuses are applied.
Warning: Advisory against employing bad practices. Overall score is reduced.
Failure: Does not meet the minimum standards. Overall score is reduced.

Figura 3.29: Resultado de la clave del Router.

Seguidamente se evaluará la contraseña del Access Point, esta contraseña es fuerte pero no cumple con todos los requisitos para que sea una contraseña segura.



Test Your Password	
Password:	••••••••••••••••••
Hide:	☑
Score:	78%
Complexity:	Strong

Minimum Requirements

- Minimum 8 characters in length
- Contains 3/4 of the following items:
  - Uppercase Letters
  - Lowercase Letters
  - Numbers
  - Symbols

Figura 3.30: Resultado clave de Access Point.

Seguidamente se procede evaluar la contraseña del servidor como se puede observar es demasiado débil.

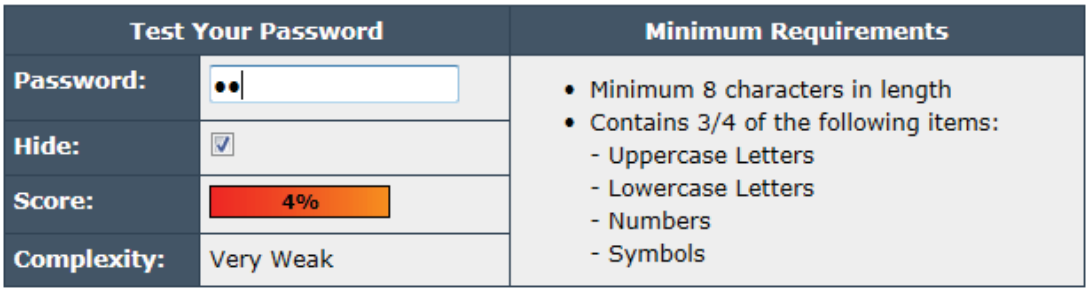


Figura 3.31: Resultado clave Servidor de datos.

En esta gráfico se evaluará la contraseña del firewall, es fuerte pero no completamente segura.

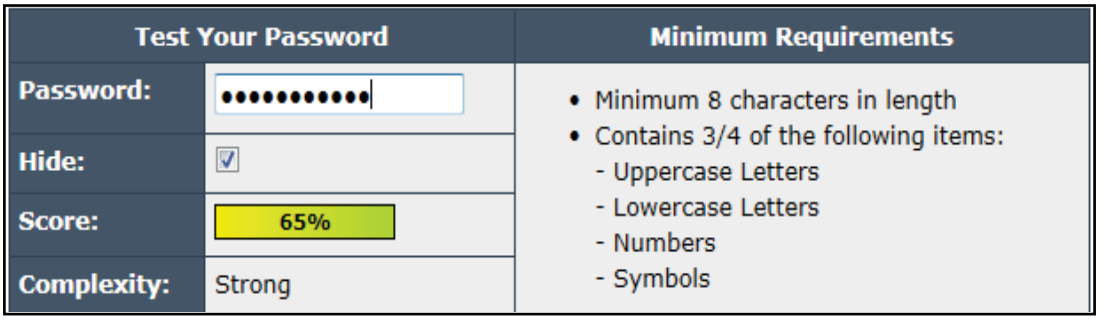


Figura 3.32: Resultado clave Firewall.

Ahora se procederá a evaluar la contraseña en las máquinas, como se puede observar tiene una contraseña muy fuerte difícil de descifrar.

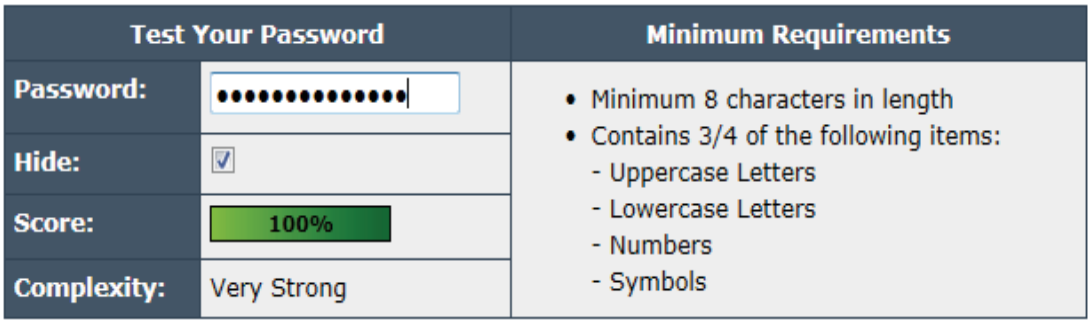


Figura 3.33: Resultado clave máquina de usuario.

Se realiza las pruebas en cada una de las máquinas que poseen contraseña, pero se observa que en cada prueba las contraseñas siguen siendo muy débiles.

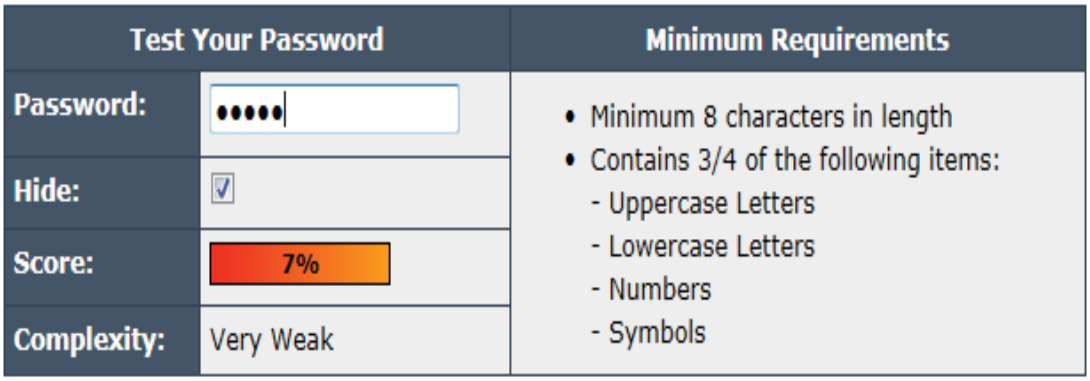


Figura 3.34: Resultado clave máquina de usuario.

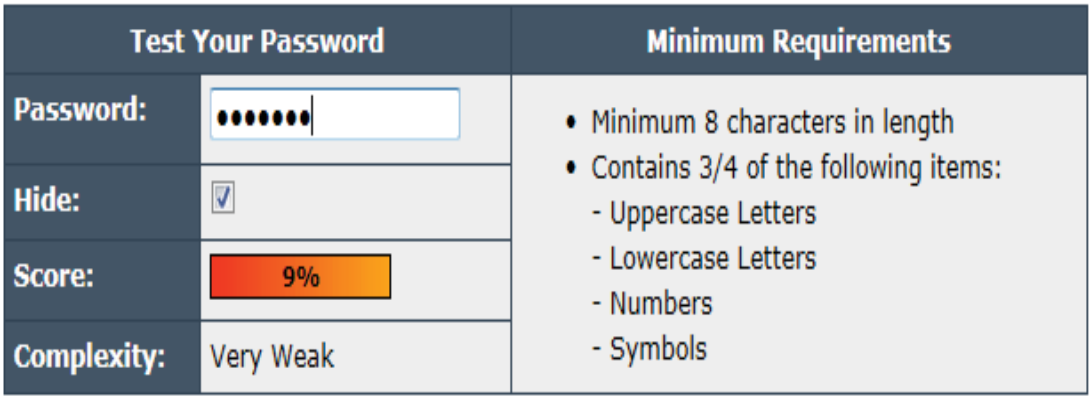


Figura 3.35: Resultado clave máquina de usuario.

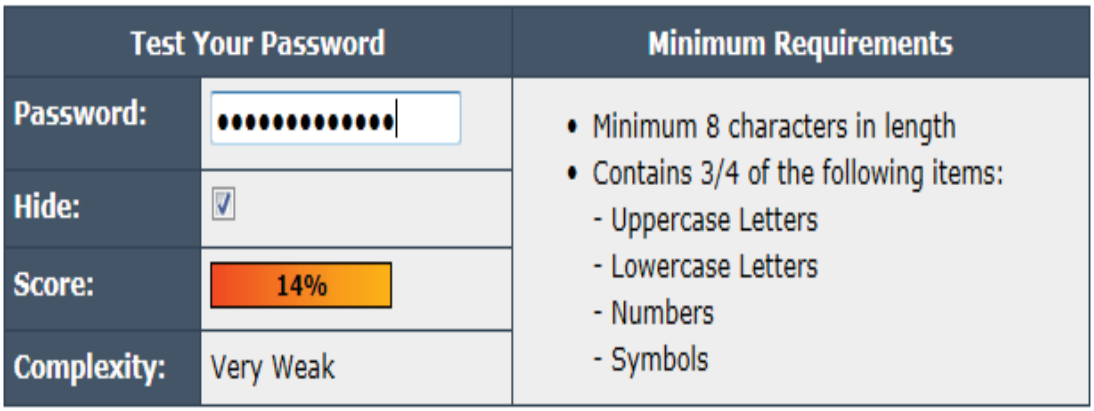


Figura 3.36: Resultado clave máquina de usuario.

3.1.7 Evaluación de antivirus

Para la evaluación del antivirus se utilizará la página www.eicar.org; la misma que permitirá probar la eficiencia del antivirus ESET NOD 32.

Ingresando a la página, se encontrará un archivo Anti-Malware; que consiste en una cadena de caracteres ASCII imprimibles.

Este archivo se copiará en un editor de texto; para este caso es el bloc de notas.

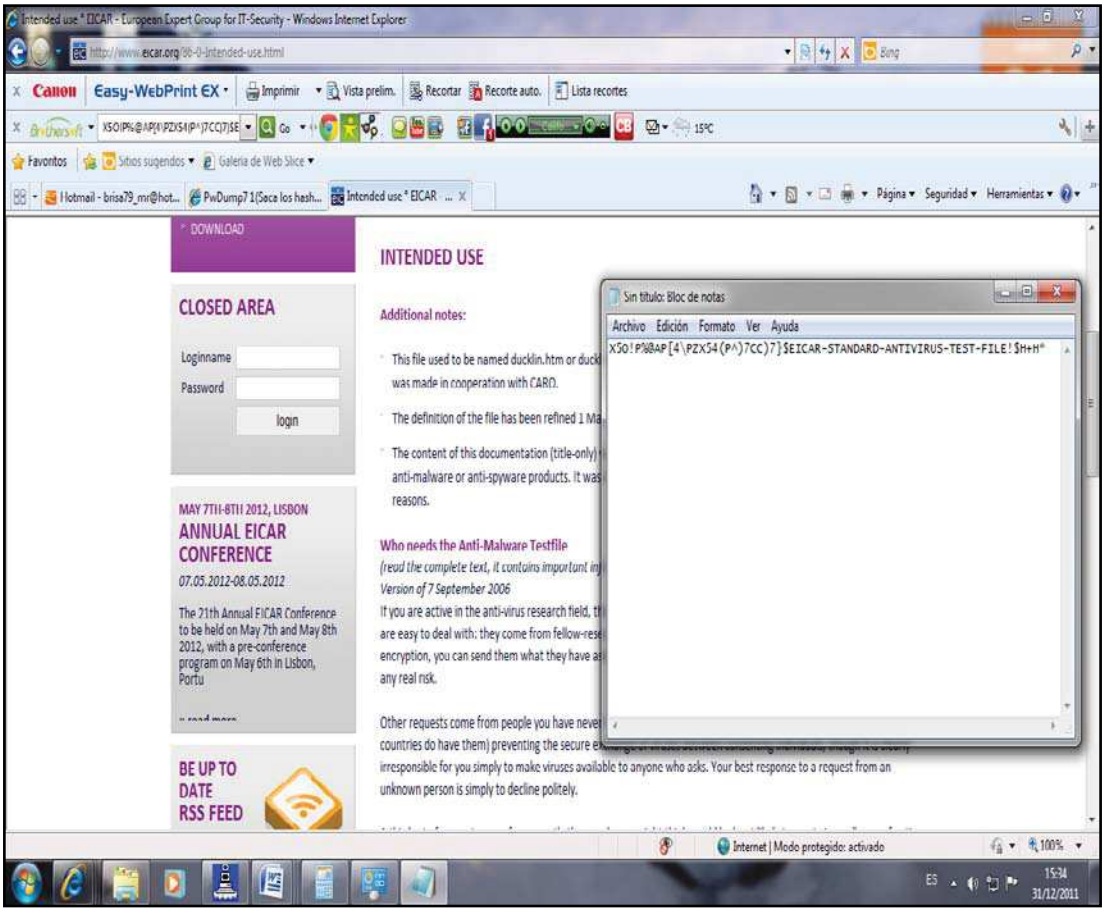


Figura 3.37: Ingreso a la página EICAR.

Una ves creado el archivo en el editor de texto, se procederá a guardarlo. El antivirus actúa de manera eficaz evitando guardar el archivo porque lo detecta como un programa malicioso.

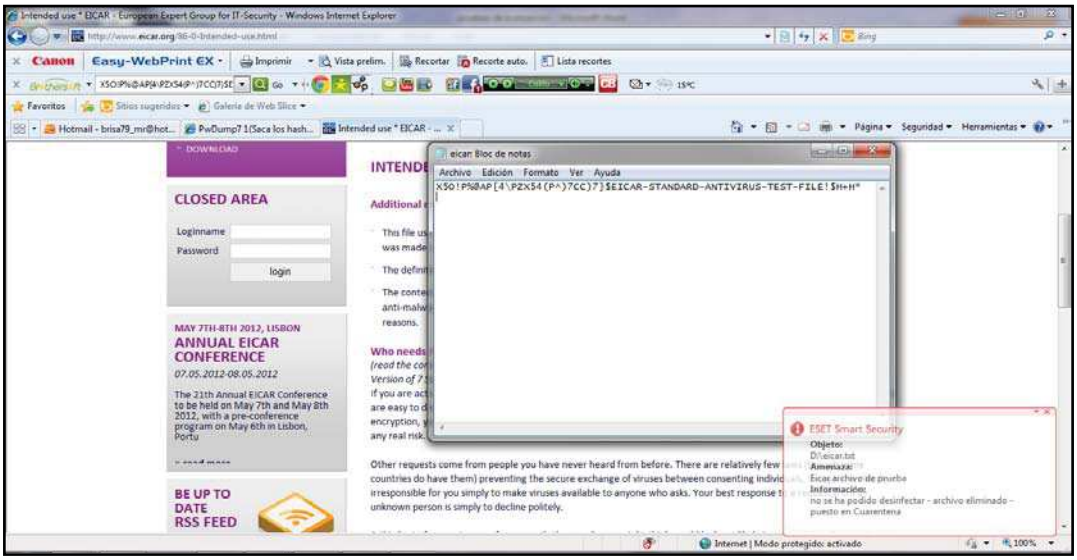


Figura 3.38: Creación del archivo texto en el computador.

Ahora se probará la funcionalidad del antivirus con otra dirección web, se verá si realmente está protegiendo la información ingresada desde el exterior; en esta página http://www.vsantivirus.com/eicar-test.htm se tendrá que acceder a cada una de las direcciones que se muestran.

A continuación se tratará de ingresar a la primera dirección http://www.eicar.org/download/eicar.com y como se observa en la figura 3.40 el antivirus automáticamente rechaza la operación requerida.

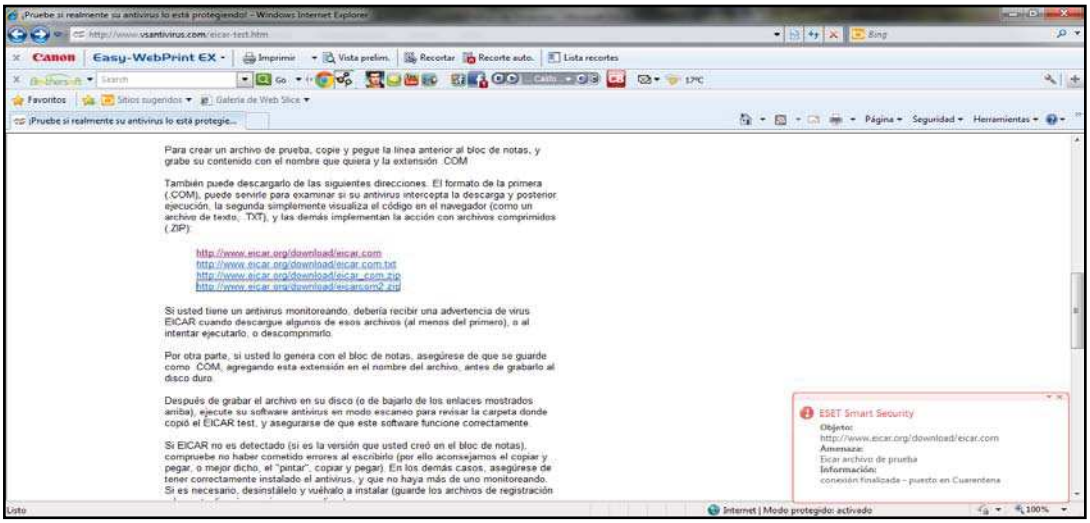


Figura 3.39: Presentación páginas de prueba EICAR.

En la figura 3.40 se tiene como resultado la no navegación de la dirección solicitada.

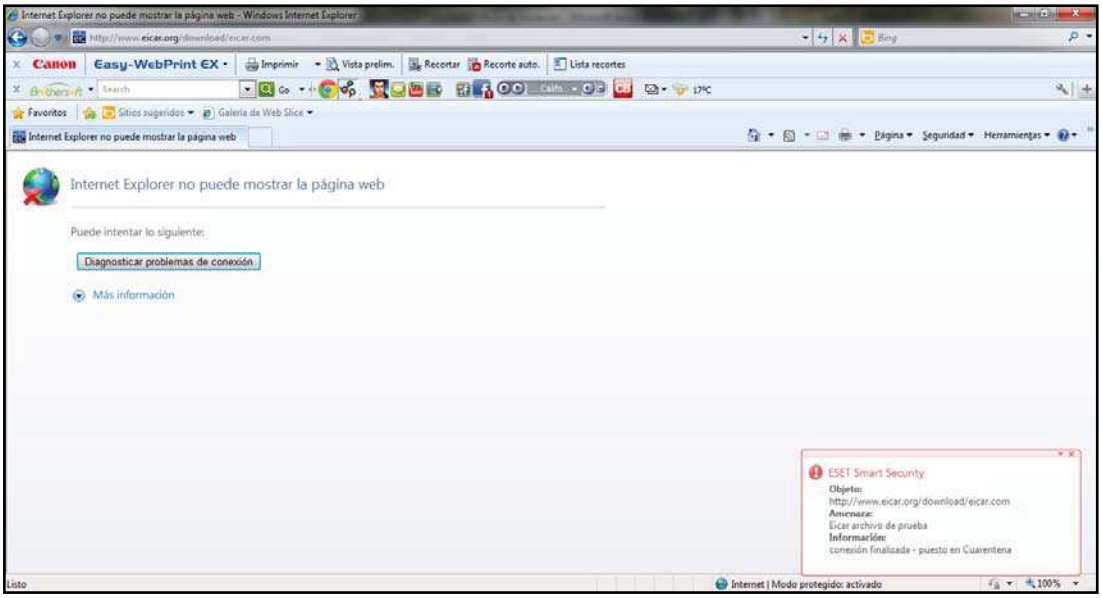


Figura 3.40: Bajada de archivos con extensión .com.

De la misma manera se procede acceder a la siguiente dirección http://www.eicar.org/download/eicar.com.txt, teniendo como resultado el bloqueo de la misma porque el antivirus rechaza la acción solicitada.

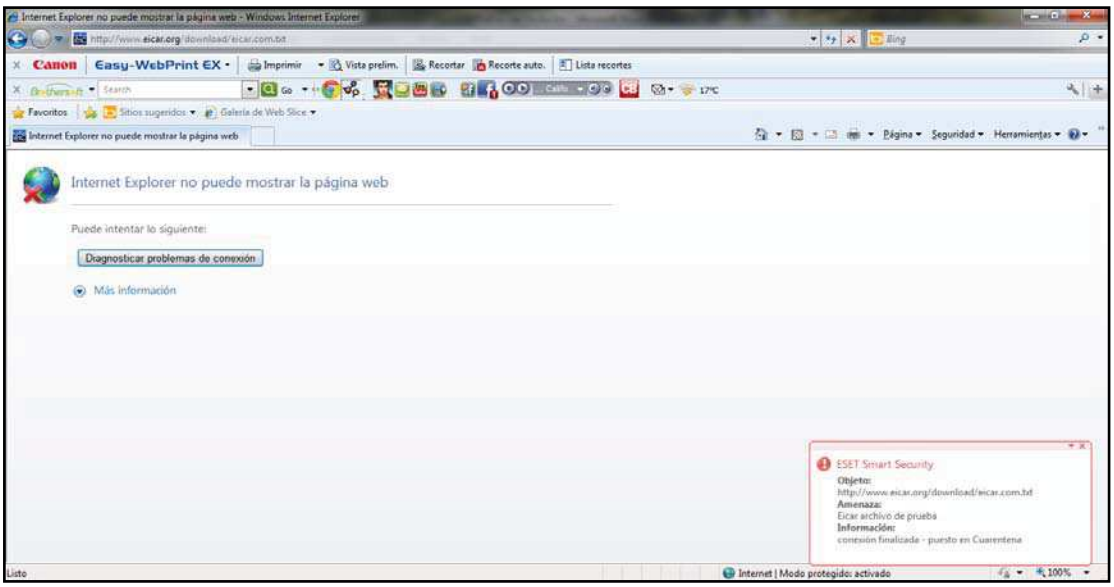


Figura 3.41 Bajada de archivos con extensión .com.txt.

Ahora se ingresará a la siguiente dirección que se encuentra comprimida http://www.eicar.org/download/eicar_com.zip, se observa que el antivirus la bloquea y no permite abrir la página.

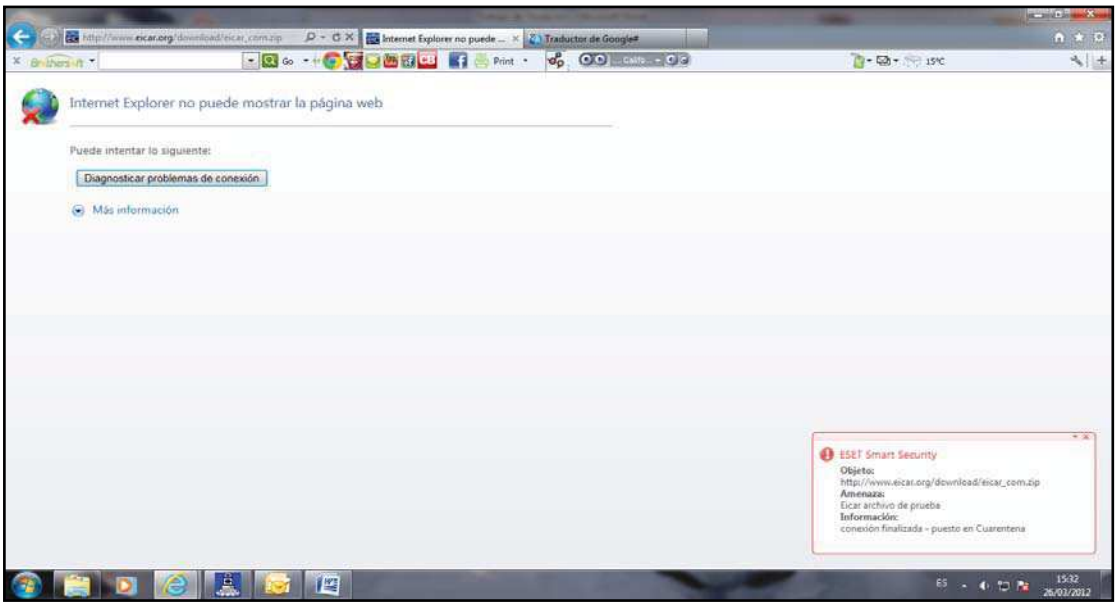


Figura 3.42 Bajada de archivos con extensión .com.zip.

Y por último se ingresará a http://www.eicar.org/download/eicarcom2.zip, al igual que las páginas anteriores, el antivirus no permite el acceso para poder ingresar a la información requerida.

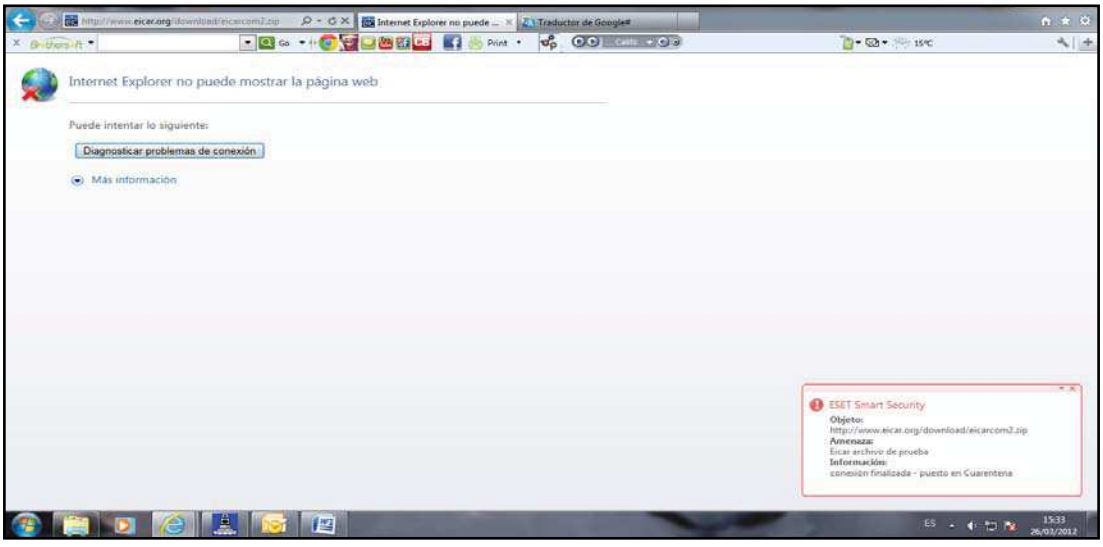


Figura 3.43 Bajada de archivos con extensión .com2.zip.

Evaluación de máquinas con antivirus Avira.

De acuerdo a la información recopilada y realizada en las pruebas anteriores se procede a ingresar a la página www.eicar.org, desarrollando los respectivos pasos que se muestra en la figura 3.37 con el antivirus ESET NOD 32.

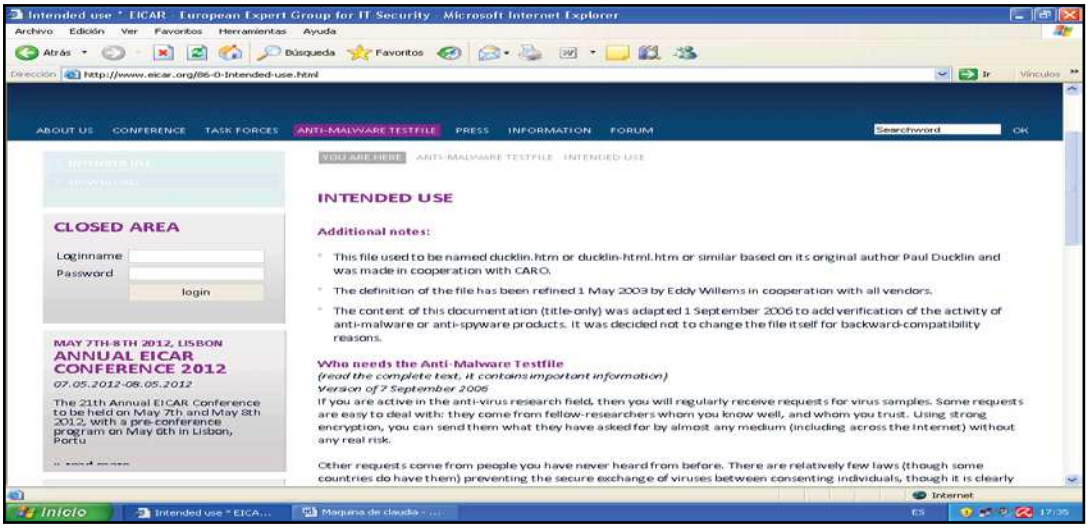


Figura 3.44: Ingreso a la página EICAR

A continuación en la figura 3.45 se procederá abrir un editor de texto para crear el archivo que guardará la cadena de caracteres que probará la eficacia del antivirus.

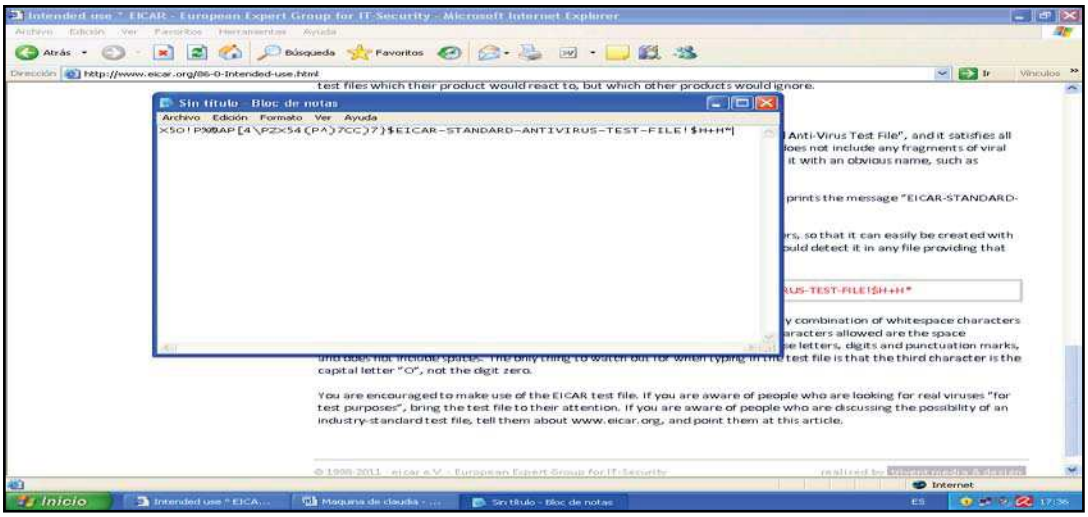


Figura 3.45: Creación del archivo texto en el computador.

En la figura 3.46 se procede a guardar el archivo de texto, pero el antivirus no detecta ninguna amenaza y lo deja pasar.

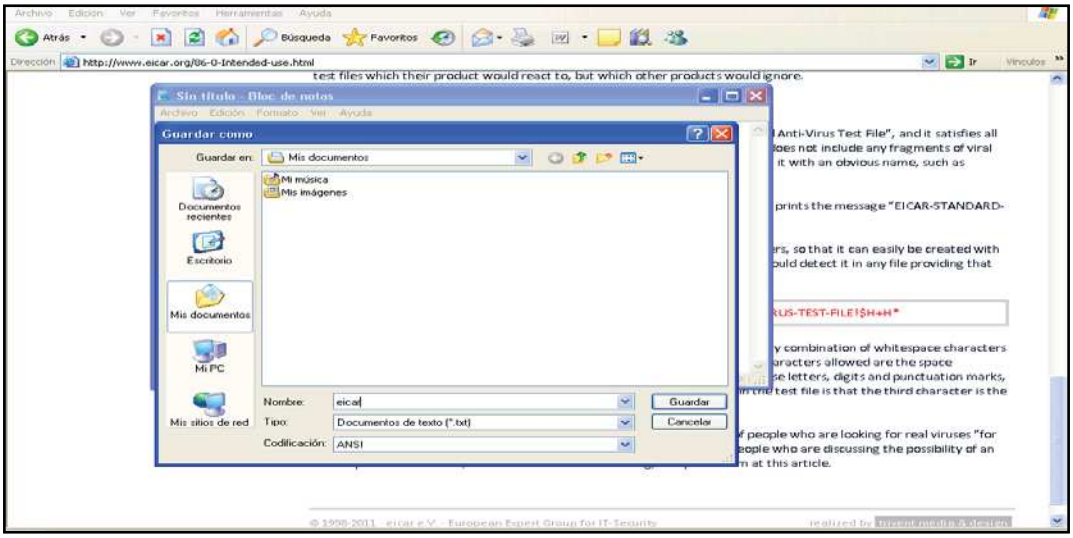


Figura 3.46: Presentación del archivo texto en el computador.

Ahora se continuará con las pruebas de archivos con extensiones, que tendrán el mismo procedimiento que se muestra en la figura 3.39, las mismas que comprobará la eficacia del antivirus. Se ingresará a la página http://www.vsantivirus.com/eicar-test.htm, como se observa en la figura 3.47 el antivirus deniega el acceso.

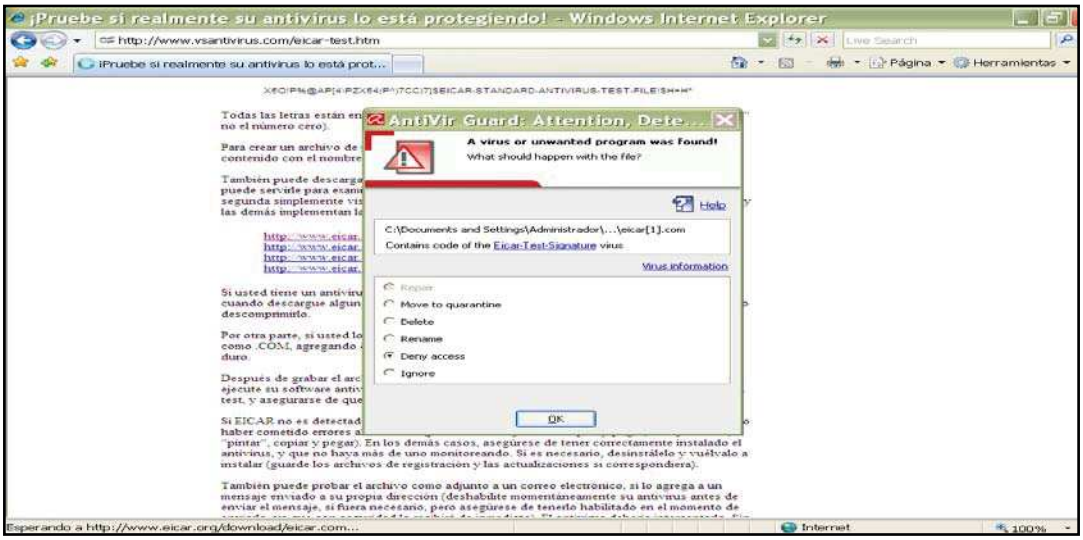


Figura 3.47: Bajada de archivo con extensión .com.

En esta prueba se observa que el antivirus permite abrir el archivo con la extensión .com.txt.

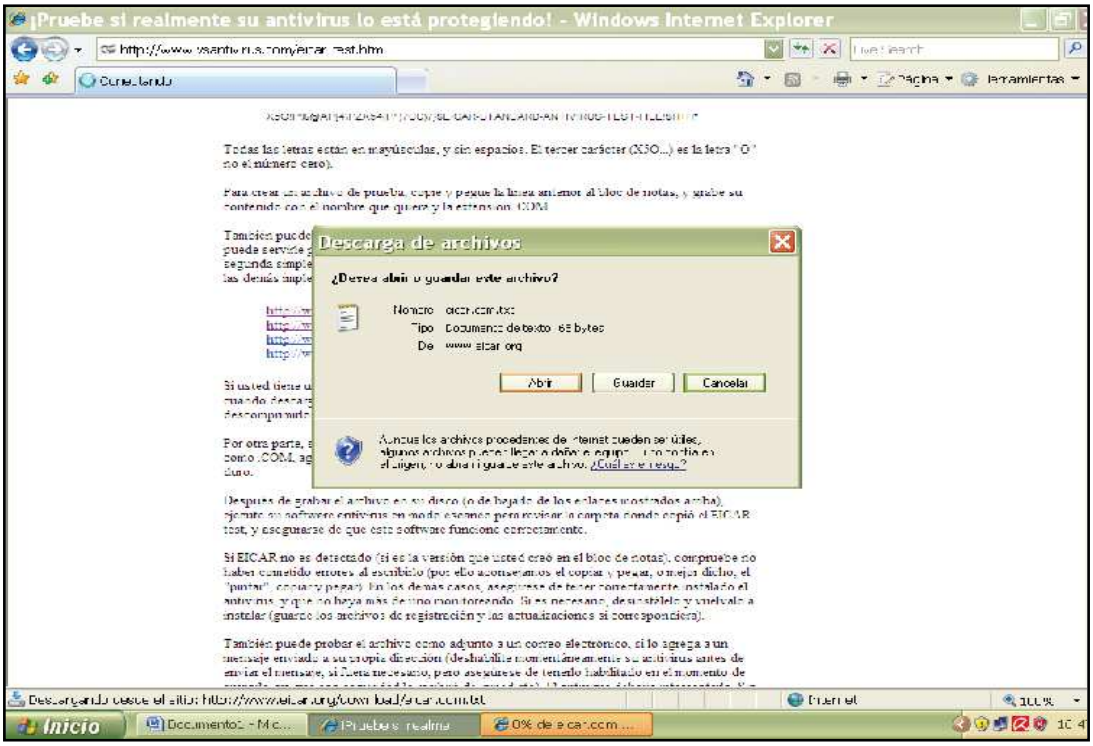


Figura 3.48: Bajada de archivo con extensión .com.txt.

Se puede observar claramente en la figura 3.49, el resultado que se obtuvo al hacer la prueba con el antivirus.

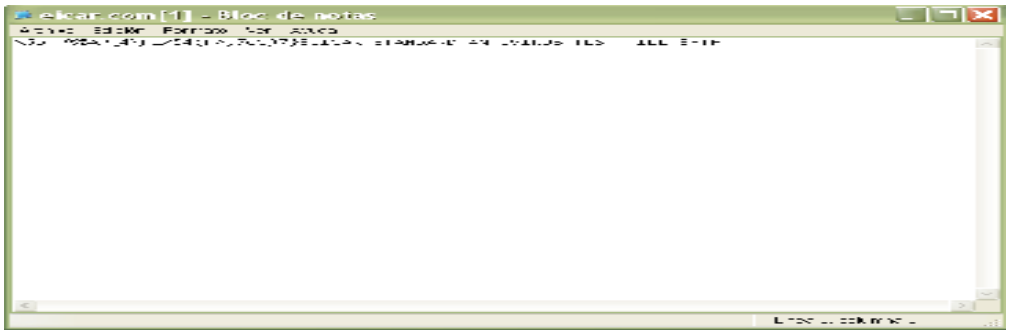


Figura 3.49: Resultado del archivo extensión.com.txt

Ahora se procederá abrir el archivo con extensión .com.zip, como se podrá observar en la siguiente figura 3.52 el antivirus denegará el acceso para esta petición.

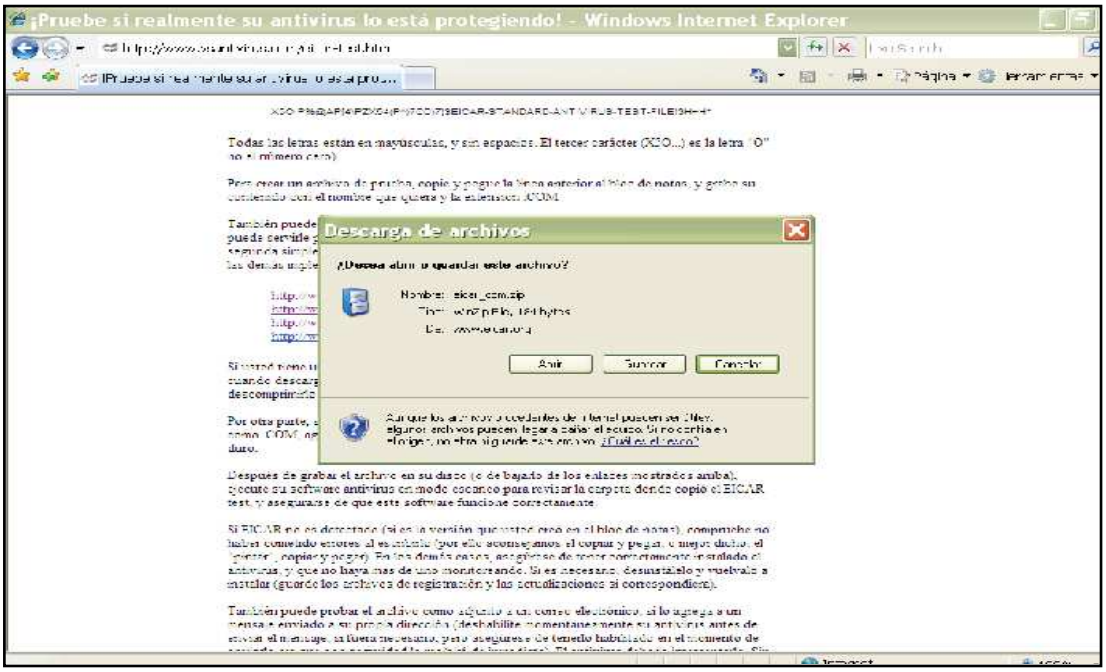


Figura 3.50: Bajada de archivo con extensión .com.zip.

En esta figura se intenta abrir el archivo comprimido, el mismo que permitirá abrir como se muestra en la figura 3.52.

Figura 3.51: Resultado del ingreso al archivo con extensión .com.zip.

Como se muestra en esta figura, después del proceso para abrir el archivo comprimido; al final el antivirus deniega el acceso al archivo.

Figura 3.52: Resultado denegado al acceso del archivo por antivirus.

Seguidamente se procederá abrir el archivo que se encuentra con un comprimido doble, se harán los mismos pasos de la prueba anterior. Obteniendo como resultado la denegación en el archivo con extensión .com2.zip.

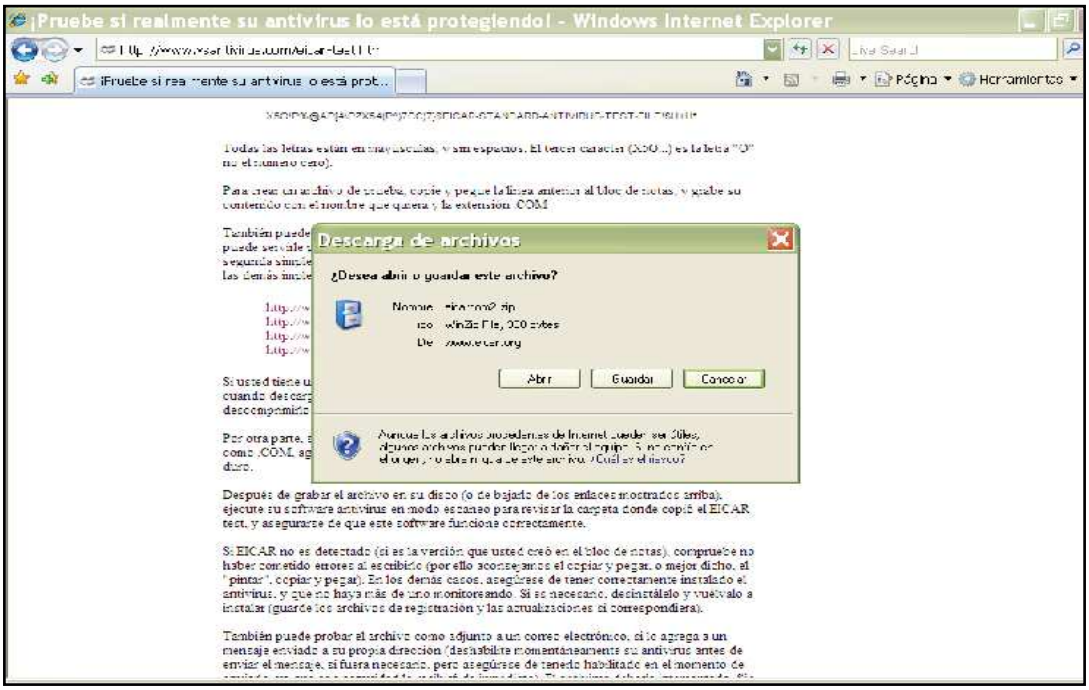


Figura 3.53: Bajada de archivo con extensión com2.zip.

Nuevamente se procede abrir en la figura 3.54 el segundo archivo comprimido; pero el antivirus lo detecta y rechaza el acceso.

Figura 3.54: Resultado de archivo con extensión .com2.zip

Como resultado final; se tiene que el archivo con extensión .com2.zip, no se pudo abrir debido a que el antivirus denegó totalmente los accesos para poder visualizar su contenido.

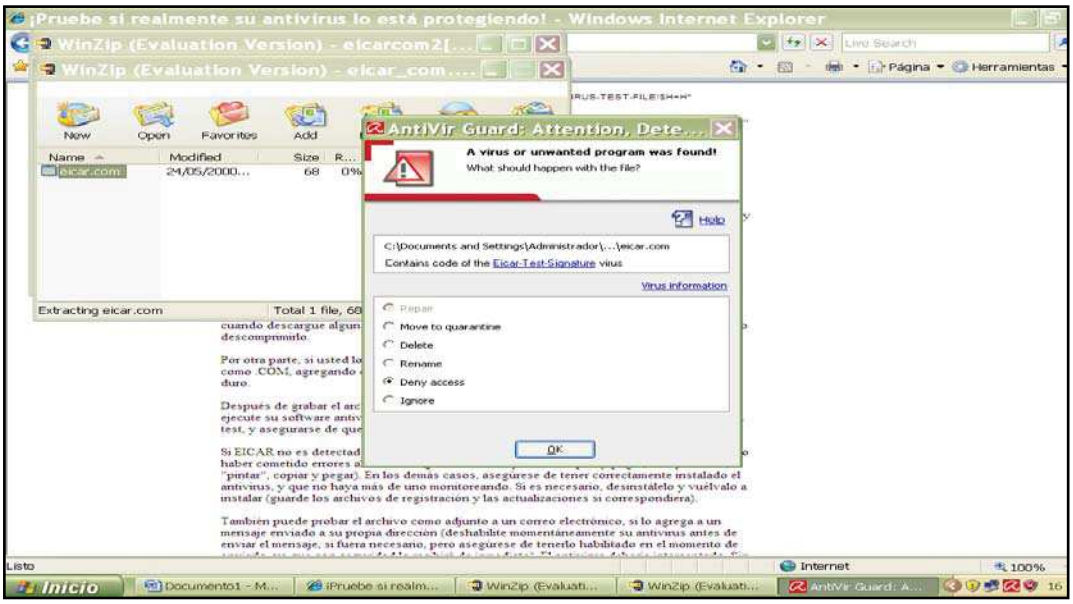


Figura 3.55: Resultado denegado al acceso del archivo por el antivirus.

Ahora se procederá a realizar la siguiente prueba que se encuentra en el siguiente link http://www.info-techs.com/eicar.shtml; consiste en el archivo de prueba EICAR; donde personas expertas en el tema colocan archivos con cadena de caracteres de códigos ASCII imprimibles, para simular un virus.

A continuación se ingresará a la página, donde se encontrará un listado de archivos por bajar y otros archivos para enviar al correo electrónico.

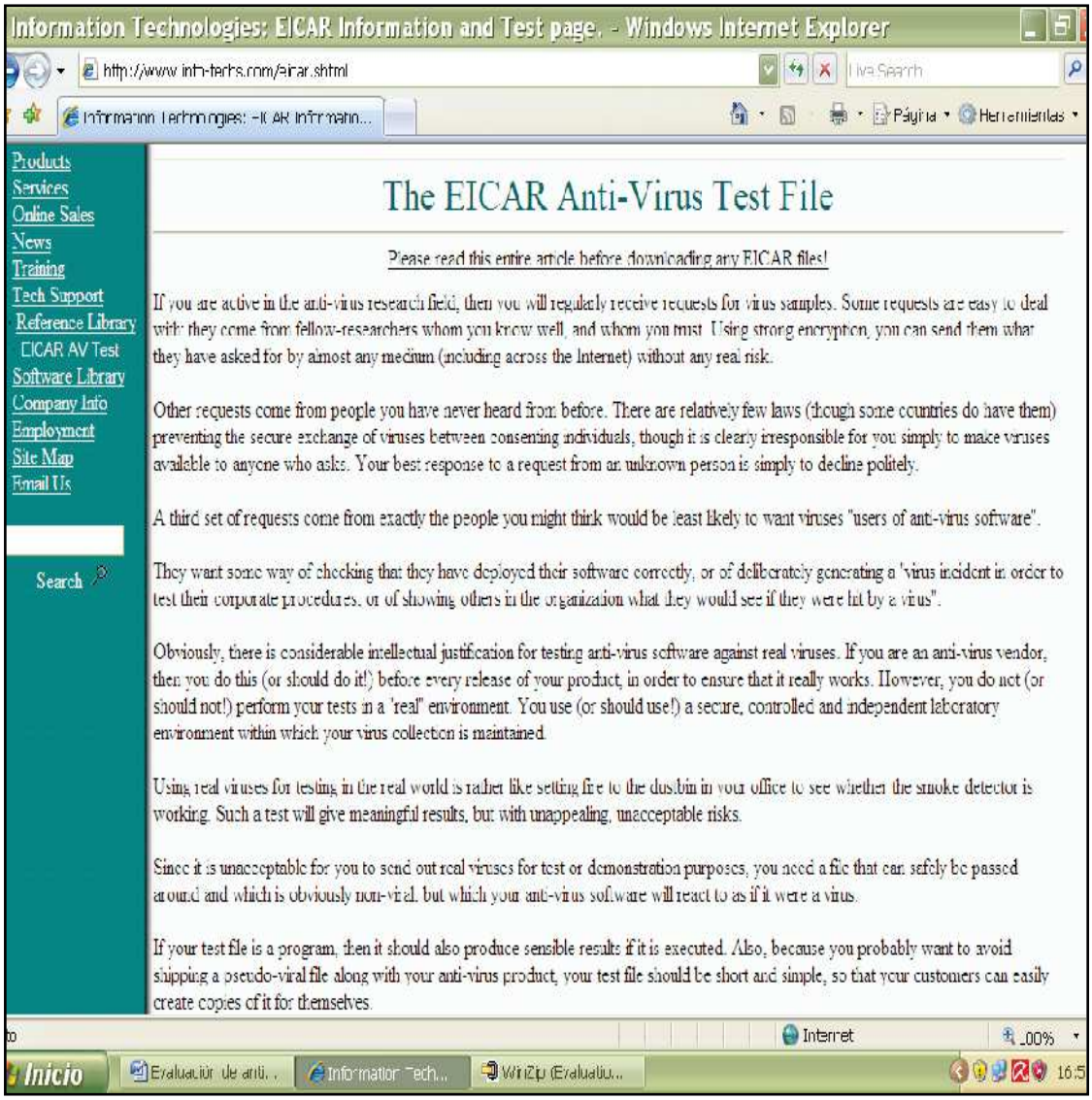


Figura 3.56: Presentación de archivo de prueba EICAR

Seguidamente se procederá a bajar todos los archivos EICAR y se observará en la figura 3.58 que el antivirus no permitirá abrir la solicitud requerida.

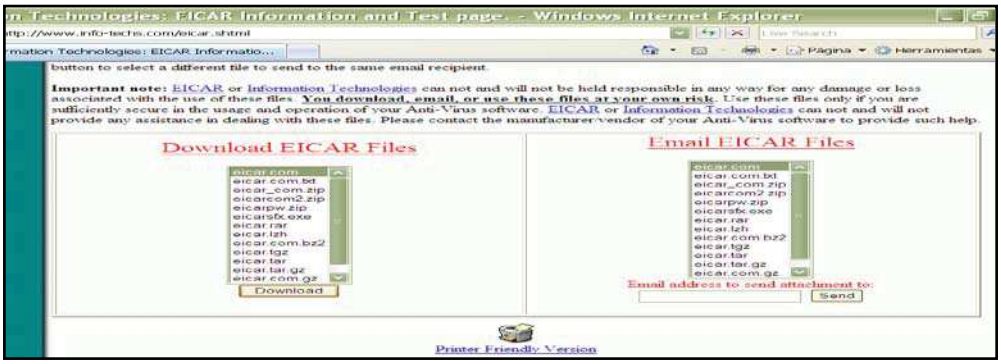


Figura 3.57: Archivos para descargar y enviar al correo electrónico.

En esta figura se muestra que el antivirus no deja descargar los archivos ya que lo detecta como un virus.

Figura 3.58: Bajada de archivos EICAR.

Seguidamente se presenta la advertencia de seguridad donde se informa que no será posible abrir el archivo.

Figura 3.59: Presentación de advertencia al abrir el archivo EICAR.

Finalmente no se pudieron descargar los archivos, como se muestra en la figura 3.60.

Figura 3.60: Presentación de descarga del archivo.

Ahora se procederá a enviar los archivos a través del correo electrónico como se muestra en esta figura.

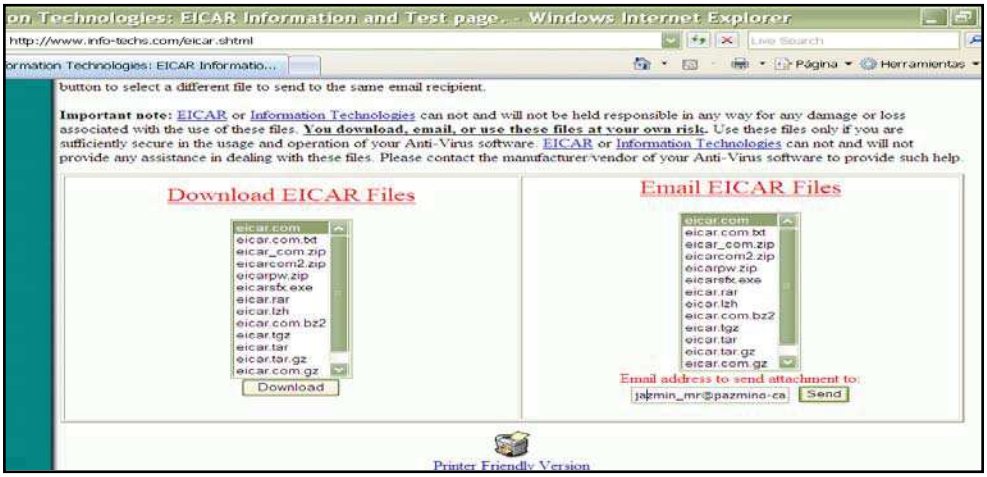


Figura 3.61: Archivos para enviar al correo electrónico.

Los archivos fueron enviados satisfactoriamente a la dirección de correo ingresada.

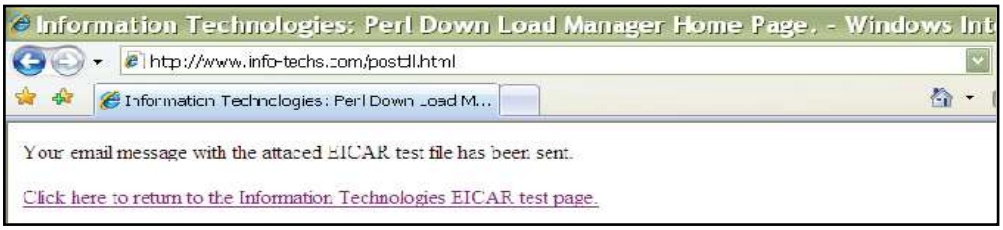


Figura 3.62: Resultados de envío de los archivos al correo electrónico.

Se procede a revisar el correo, y se observa que no es posible abrir el archivo adjunto.

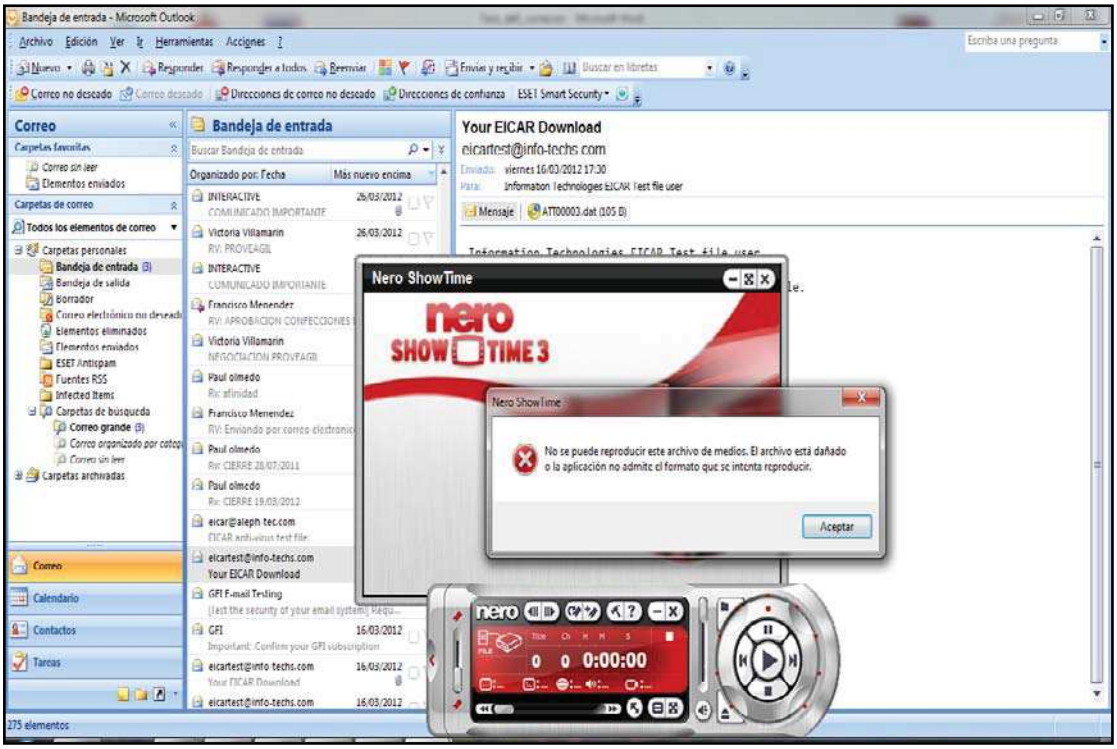
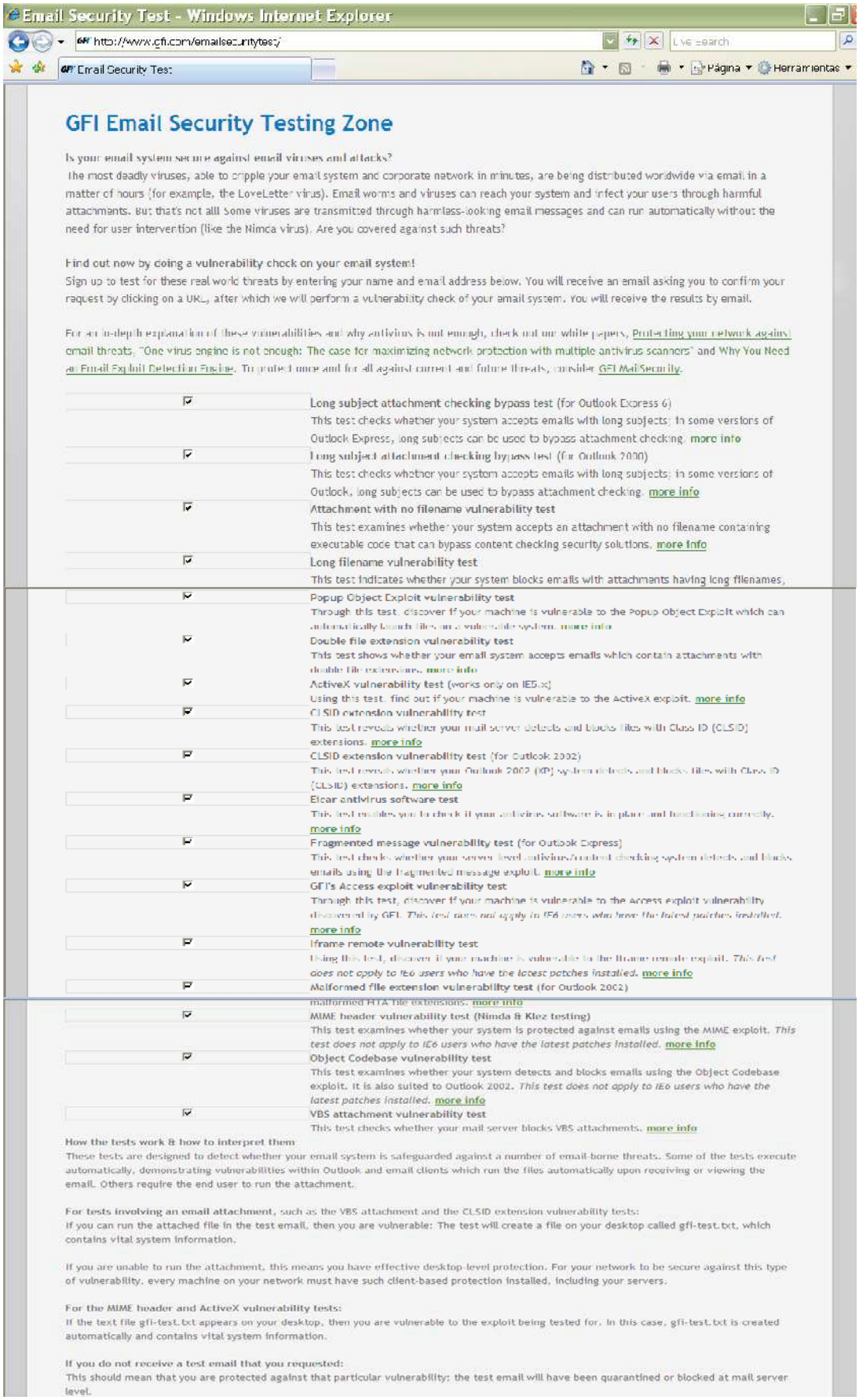


Figura 3.63: Resultado al intentar abrir el archivo desde el correo electrónico.

Ahora se ingresará al siguiente link www.gfi.com/emailsecuritytest/, GFI es una empresa dedicada a la solución de software de seguridad, de correo y anti-spam para Exchange Server y otros servidores de correo; protegiendo la red de virus y otras amenazas malware llegadas por correo y proporcionando un porcentaje de captura de spam al 99%.

¿Cómo funciona? Se envía un mail con una vulnerabilidad usada por códigos de virus; como se muestra en la figura 3.64, este mail enviado simula la actividad de código malicioso, en este caso se eligió todas las técnicas que dispone para hacer las respectivas pruebas.

Una vez elegida las opciones, se coloca el nombre y el correo de destino y se señala la aceptación de recibir dicho chequeo porque caso contrario no se recibirá correo alguno.


Email Security Test - Windows Internet Explorer
http://www.gfi.com/emailsecuritytest/
Email Security Test
Página
Herramentas
GFI Email Security Testing Zone
Is your email system secure against email viruses and attacks?
The most deadly viruses, able to cripple your email system and corporate network in minutes, are being distributed worldwide via email in a matter of hours (for example, the LoveLetter virus). Email worms and viruses can reach your system and infect your users through harmful attachments. But that's not all! Some viruses are transmitted through harmless-looking email messages and can run automatically without the need for user intervention (like the Nimda virus). Are you covered against such threats?
Find out now by doing a vulnerability check on your email system!
Sign up to test for these real world threats by entering your name and email address below. You will receive an email asking you to confirm your request by clicking on a URL, after which we will perform a vulnerability check of your email system. You will receive the results by email.
For an in-depth explanation of these vulnerabilities and why antivirus is not enough, check out our white papers, Protecting your network against email threats, "One virus engine is not enough: The case for maximizing network protection with multiple antivirus scanners" and Why You Need an Email Exploit Detection Engine. To protect once and for all against current and future threats, consider GFI MailSecurity.
Long subject attachment checking bypass test (for Outlook Express 6)
This test checks whether your system accepts emails with long subjects. In some versions of Outlook Express, long subjects can be used to bypass attachment checking. more info
Long subject attachment checking bypass test (for Outlook 2000)
This test checks whether your system accepts emails with long subjects. In some versions of Outlook, long subjects can be used to bypass attachment checking. more info
Attachment with no filename vulnerability test
This test examines whether your system accepts an attachment with no filename containing executable code that can bypass content checking security solutions. more info
Long filename vulnerability test
This test indicates whether your system blocks emails with attachments having long filenames,
Popup Object Exploit vulnerability test
Through this test, discover if your machine is vulnerable to the Popup Object Exploit which can automatically launch files on a vulnerable system. more info
Double file extension vulnerability test
This test shows whether your email system accepts emails which contain attachments with double file extensions. more info
ActiveX vulnerability test (works only on IE5.x)
Using this test, find out if your machine is vulnerable to the ActiveX exploit. more info
CLSID extension vulnerability test
This test reveals whether your mail server detects and blocks files with Class ID (CLSID) extensions. more info
CLSID extension vulnerability test (for Outlook 2002)
This test reveals whether your Outlook 2002 (XP) system detects and blocks files with Class ID (CLSID) extensions. more info
Eicar antivirus software test
This test enables you to check if your antivirus software is in place and functions correctly. more info
Fragmented message vulnerability test (for Outlook Express)
This test checks whether your server-level antivirus/content checking system detects and blocks emails using the fragmented message exploit. more info
GFI's Access exploit vulnerability test
Through this test, discover if your machine is vulnerable to the Access exploit vulnerability discovered by GFI. This test does not apply to IE6 users who have the latest patches installed. more info
Iframe remote vulnerability test
Using this test, discover if your machine is vulnerable to the Iframe remote exploit. This test does not apply to IE6 users who have the latest patches installed. more info
Malformed file extension vulnerability test (for Outlook 2002)
malformed HTA file extensions. more info
MIME header vulnerability test (Nimda & Klez testing)
This test examines whether your system is protected against emails using the MIME exploit. This test does not apply to IE6 users who have the latest patches installed. more info
Object Codebase vulnerability test
This test examines whether your system detects and blocks emails using the Object Codebase exploit. It is also suited to Outlook 2002. This test does not apply to IE6 users who have the latest patches installed. more info
VBS attachment vulnerability test
This test checks whether your mail server blocks VBS attachments. more info
How the tests work & how to interpret them
These tests are designed to detect whether your email system is safeguarded against a number of email-borne threats. Some of the tests execute automatically, demonstrating vulnerabilities within Outlook and email clients which run the files automatically upon receiving or viewing the email. Others require the end user to run the attachment.
For tests involving an email attachment, such as the VBS attachment and the CLSID extension vulnerability tests:
If you can run the attached file in the test email, then you are vulnerable: The test will create a file on your desktop called gfi-test.txt, which contains vital system information.
If you are unable to run the attachment, this means you have effective desktop-level protection. For your network to be secure against this type of vulnerability, every machine on your network must have such client-based protection installed, including your servers.
For the MIME header and ActiveX vulnerability tests:
If the text file gfi-test.txt appears on your desktop, then you are vulnerable to the exploit being tested for. In this case, gfi-test.txt is created automatically and contains vital system information.
If you do not receive a test email that you requested:
This should mean that you are protected against that particular vulnerability: the test email will have been quarantined or blocked at mail server level.

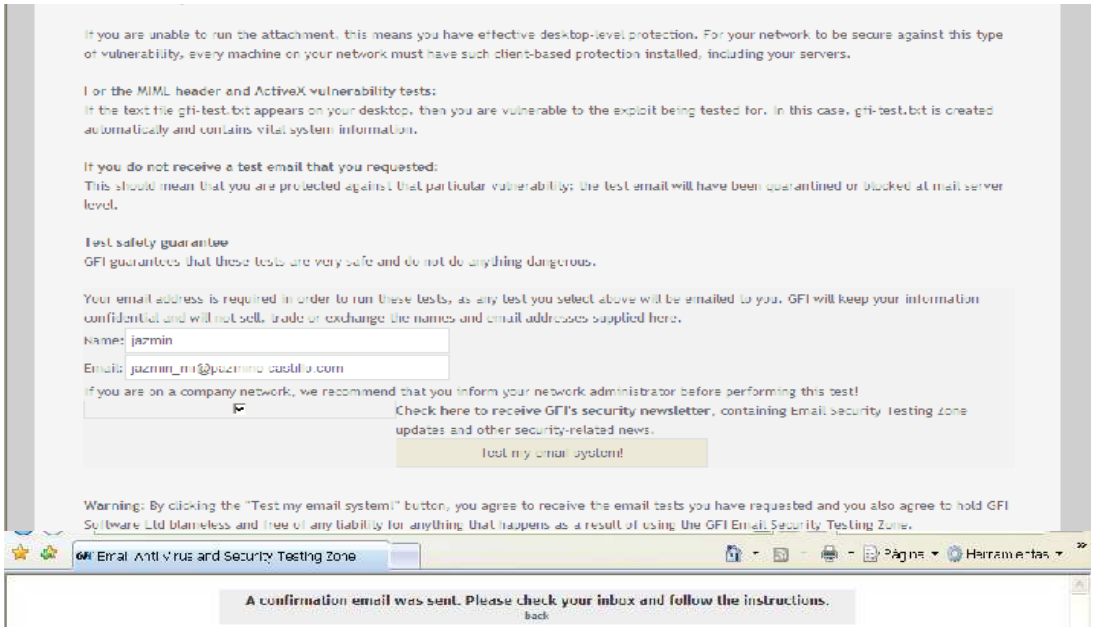


Figura 3.64 Envío de correo Spam para el respectivo testeo

Luego de haber enviado se revisa el correo, y efectivamente se observa en la figura 3.65 los dos correos que han llegado, los cuales piden confirmación de los test solicitados, si no se envía la confirmación en algunos casos enviarán falsas alarmas a usuarios desprevenidos.

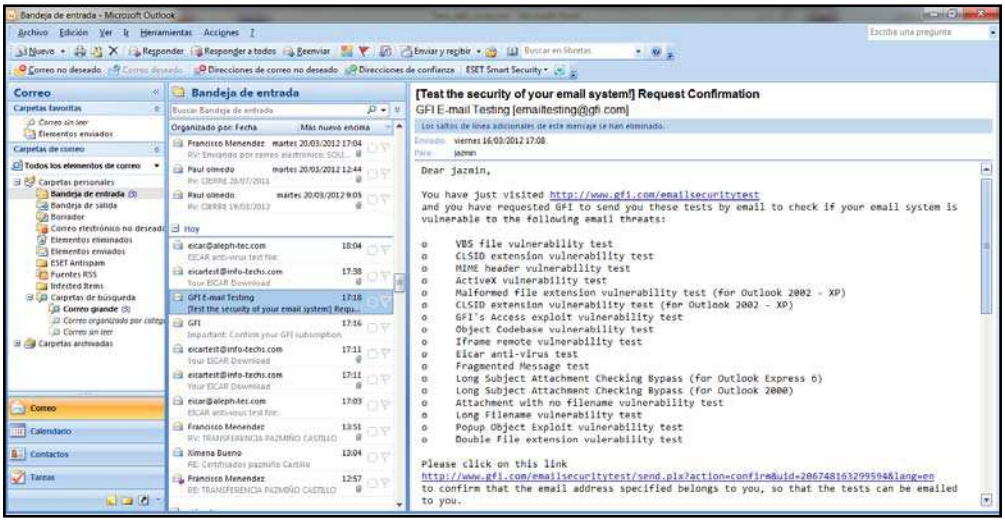


Figura 3.65: Revisión de correo enviado por GFI.

En esta figura se puede observar que la dirección que pide ingresar en el link de la figura 3.65, no se encuentra disponible la página.

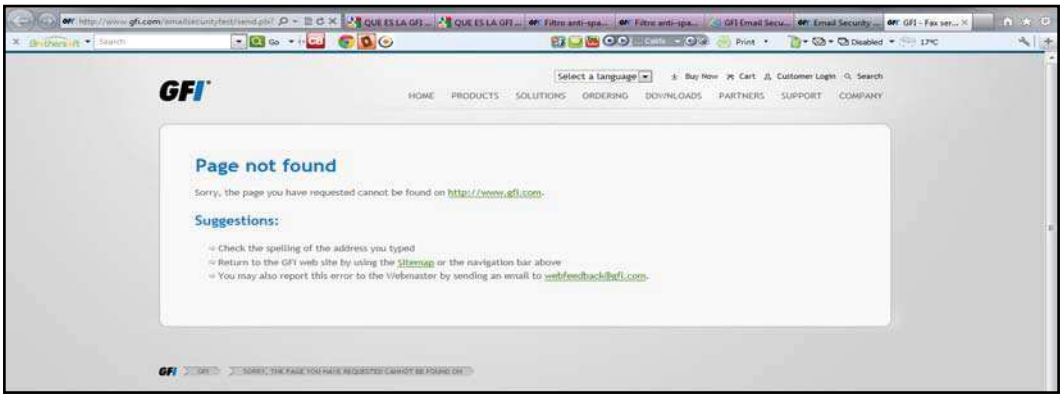


Figura 3.66: Resultado de la revisión de test de seguridad.

En el segundo correo muestra la confirmación para la inscripción del chequeo de seguridad, si uno se inscribe llegarán correos con los testeos de códigos malicioso, donde se explica cómo identificar si se es o no vulnerable.

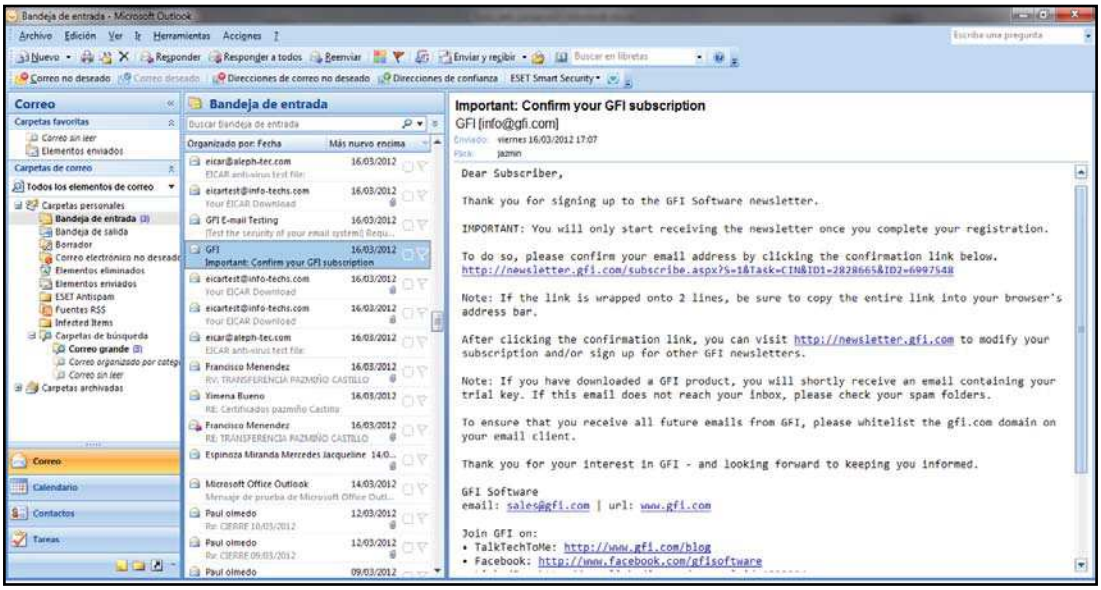


Figura 3.67: Resultado de mail de confirmación y suscripción.

En este caso el proceso llegó hasta el envío a la dirección del correo, debido a que no se hizo la respectiva inscripción al sistema de la empresa GFI.

Teniendo como resultado final que la prueba de correo GFI no permitió abrir el link donde se enviaron todos los testeos de las pruebas, debido a que los consideró como un correo basura.

4 Capítulo IV Análisis y evaluación de resultados

4.1 Presentación de resultados

Para la presentación de resultados se requirió hacer los respectivos cuadros comparativos en los cuales se verá el resultado final de la auditoría realizada, para ello se recopiló la información de cada prueba ejecutada.

4.1.1 Sistemas Operativos Instalados

En este gráfico se representa el porcentaje total de máquinas existentes en la empresa, así como también el sistema operativo que están utilizando.

SISTEMA OPERATIVO	% MAQUINAS
WINDOWS XP	63,00%
WINDOWS 7	32,00%
SERVER 2003	5,00%

Gráfico 4.1: Representación de máquinas existentes

4.1.2 Licenciamiento del Sistema Operativo

En este gráfico se muestra el porcentaje de licenciamiento de cada máquina de acuerdo al sistema operativo que utilizan, como se muestra en el gráfico 4.2 el sistema operativo Windows no está licenciado en la totalidad de las máquinas que se evaluó en el gráfico 4.1.

SISTEMA OPERATIVO	LICENCIAMIENTO
WINDOWS XP	39,00%
WINDOWS 7	100%
SERVER 2003	100%

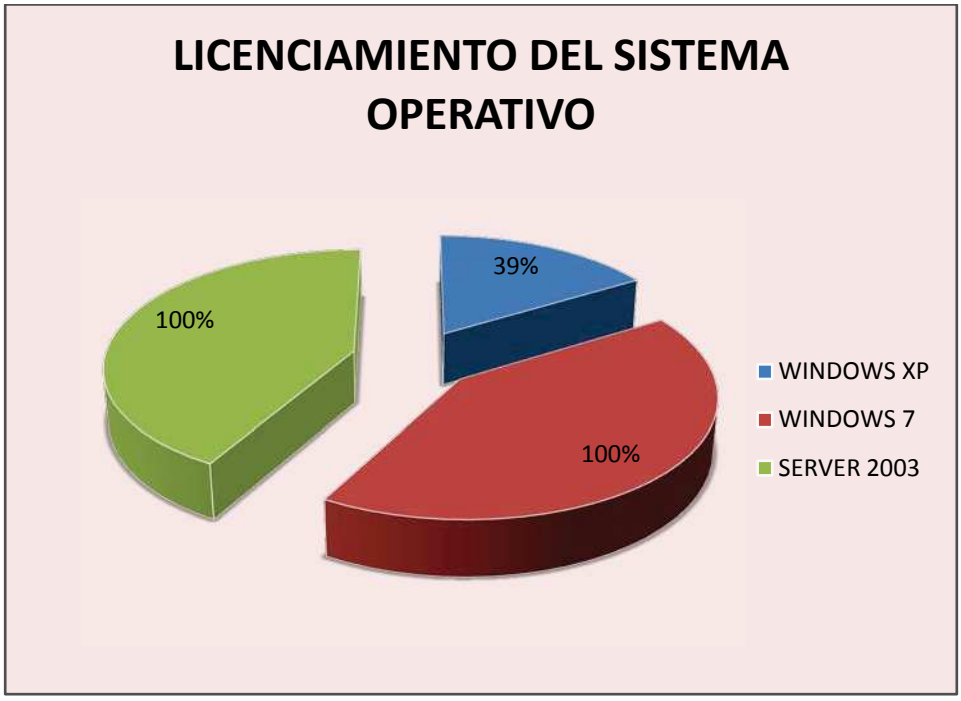


Gráfico 4.2: Porcentaje de licenciamiento en el sistema operativo

4.1.3 Licenciamiento de Aplicaciones

En el gráfico 4.3 se muestra las aplicaciones de office instaladas en la totalidad de las máquinas con su respectivo licenciamiento.

APLICACIONES - OFFICE	
LICENCIADO	**NO LICENCIADO**
59,00%	41,00%

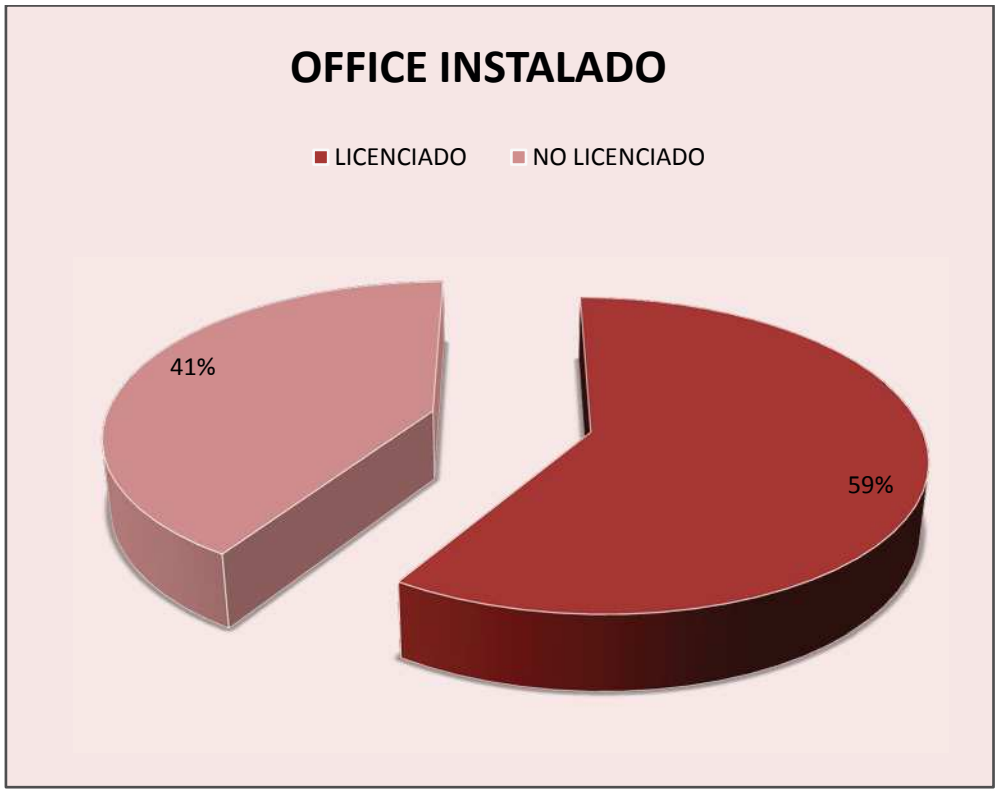


Gráfico 4.3: Representación de aplicaciones Office.

4.1.4 Antivirus Instalado y Licenciado

Como se muestra en el gráfico 4.4, las máquinas disponen de dos antivirus en su mayoría se encuentra instalado el antivirus NOD32 debidamente licenciado.

APLICACIONES - ANTIVIRUS		
ANTIVIRUS	% MAQUINAS	LICENCIADO
NOD 32	91,00%	100,00%
AVIRA	9,00%	100,00%

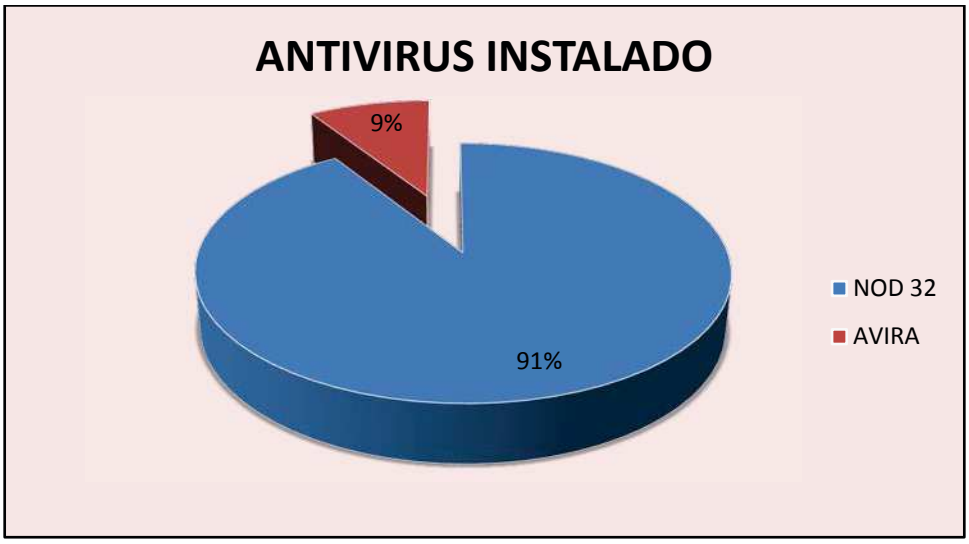


Gráfico 4.4: Representación de antivirus instalado en la máquinas.

4.1.5 Pruebas Realizadas con Antivirus

En esta prueba se recopilaron los resultados obtenidos con los dos antivirus de la empresa como NOD32 y Avira obteniendo los siguientes resultados.

PRUEBAS EICAR	NOD 32	AVIRA
Cadena de texto	OK	FALLO
eicar.com	OK	OK
eicar.com.txt	OK	FALLO
eicar_com.zip	OK	OK
eicarcom2.zip	OK	OK
eicarpasswd.zip	OK	OK
eicarpasswdocr.zip	OK	OK
Download Eicar Files	OK	OK
Email Eicar Files	OK	OK
Correo Electrónico	OK	OK
GFI Email Securuty	OK	OK

Gráfico 4.5: Resultados obtenidos de la pruebas EICAR.

4.1.6 Contraseñas en Máquinas y Dispositivos de Comunicación

Se muestra en el gráfico 4.5 que las contraseñas tanto en los dispositivos como en los equipos terminales, en su mayoría no son robustas lo que hace que sean vulnerables ante cualquier ataque tanto interno como externo.

EQUIPOS Y DISPOSITIVOS	CONTRASEÑAS		
	ROBUSTAS	POCO ROBUSTAS	NO POSEE
COMPUTADORAS	5%	36%	59%
ROUTER	100%		
ACCES POINT	78%		
FIREWALL	65%		

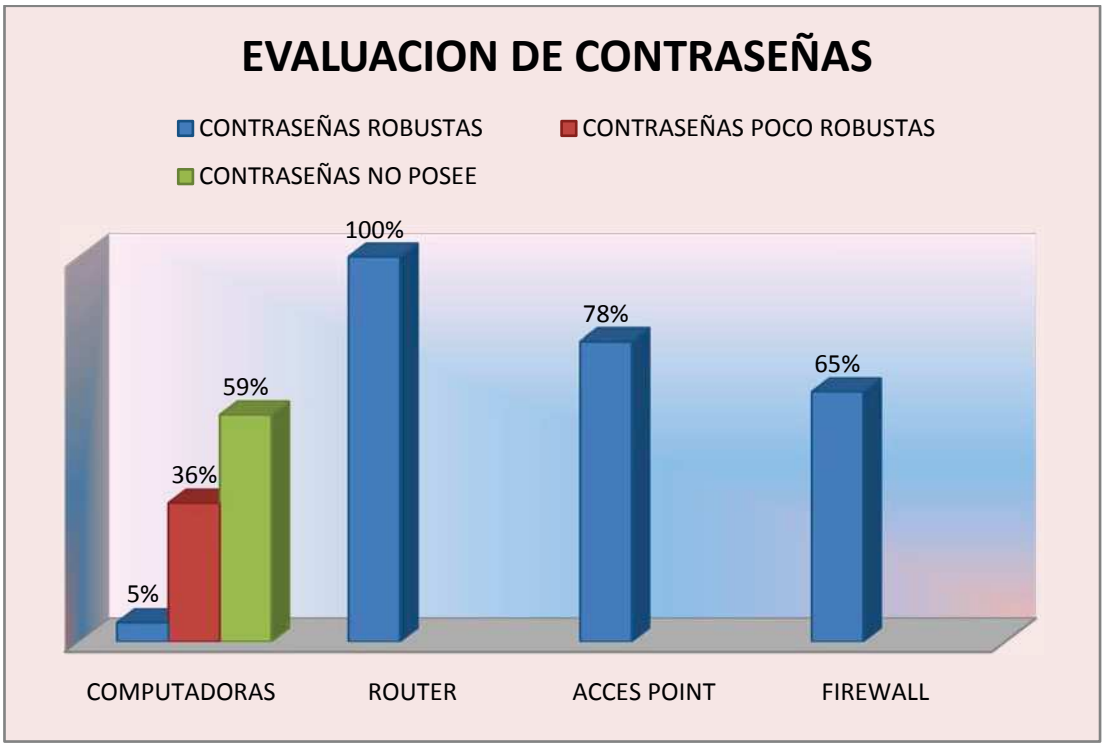


Gráfico 4.6: Representación de contraseñas en PCS y dispositivos.

4.1.7 Configuración de Perfiles en las máquinas

En los perfiles de las máquinas se examinó en cada una de ellas, su respectiva configuración. Teniendo como resultado un mayor porcentaje en las cuentas de administrador, la cual podrá controlar y manejar los recursos compartidos de las PCs.

PERFILES	PORCENTAJE
ADMINISTRADOR	59%
USUARIO	41%

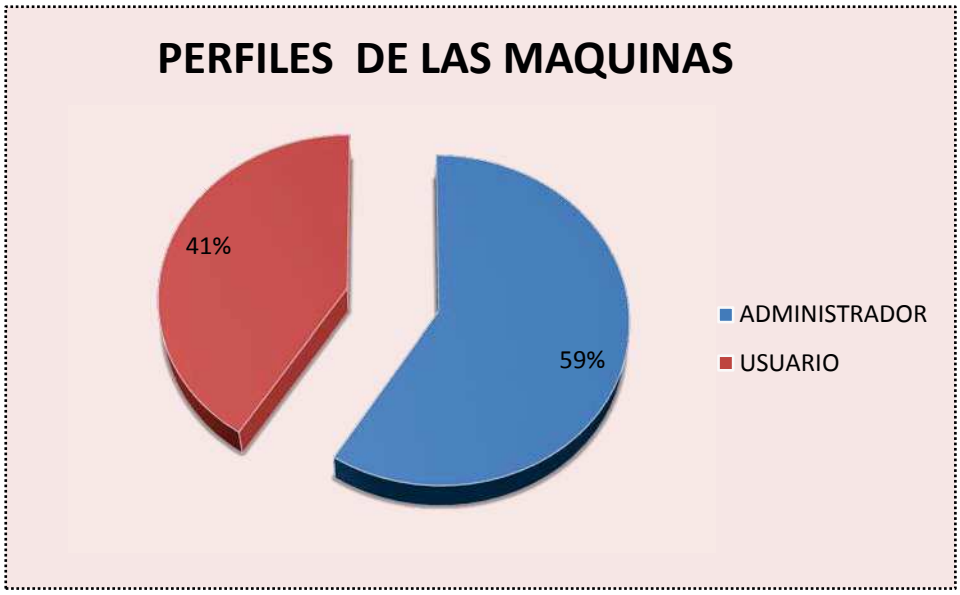


Gráfico 4.7: Representación de porcentajes de perfiles en las PCs.

4.1.8 Niveles de los resultados de la Auditoría

En este gráfico se aprecia que hay determinados niveles de vulnerabilidad en la empresa que no se encuentran en su debido funcionamiento para obtener resultados eficaces al momento de utilizar la red, lo cual genera pérdidas en la información y retrasos en los servicios utilizados por los usuarios.

En consecuencia, se tiene que un 21% está en un nivel de riesgo potencialmente alto, lo que indica que se debe tomar medidas inmediatas para solucionar los inconvenientes previstos.

De igual manera se tiene que un 43% se encuentra en un nivel medio, y un 36% en un nivel bajo; lo cual no deja de ser preocupante ante los posibles fallos en la red y hacen que los sistemas sean vulnerables ante cualquier atacante.

DESCRIPCION	NIVEL DE VULNERABILIDAD		
	BAJO	MEDIO	ALTO
LICENCIAMIENTO DEL SISTEMA OPERATIVO			
LICENCIAMIENTO DE APLICACIONES(OFFICE)			
LICENCIAMIENTO DE ANTIVIRUS			
EVALUACION DE CONTRASEÑAS			
PERFILES DE USUARIOS			
BACKUPS DE LA INFORMACION			
SERVIDOR DE CORREO			
EVALUACION DEL DOMINIO			
LISTAS NEGRAS			
ESCANEO DE PUERTOS			
PRUEBAS DE EFECTIVIDAD DEL ANTIVIRUS			
SERVIDOR DNS			
SERVIDOR PROXY			
SERVIDOR DHCP			

Gráfico 4.8: Niveles de Vulnerabilidad en las pruebas realizadas

4.1.9 Checklist de la Empresa Confecciones Pazmiño Castillo Cía. Ltda.

Este cuestionario muestra los controles de la empresa, en cuanto al departamento de informática, y así advertir las vulnerabilidades en las que se encuentra expuesto el sistema de información.

CONTROLES	SI	NO	N/A
Existen planes a largo plazo para el departamento de informática.	*		
Valore la conexión de estos planes con planes generales de la empresa	3		
Cubren los planes del D.I. los objetivos a largo plazo de la empresa, valórelo.	3		
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.	4		
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.	5		
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.		4	
¿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.			*
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 sí).	6		
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)		6	
¿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)?	13	10	
Evalúe la capacidad de los recursos humanos para satisfacer la demanda en la época alta de proceso(resultado en si)	6		
Evalúe el exceso de capacidad de los recursos humanos disponibles para satisfacer la demanda en la época baja de proceso (resultado en no).		5	
¿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)?	6	5	
¿Existe un calendario de mantenimiento preventivo a las PCS?		*	
¿Se verifica que dicho calendario no incluya revisiones en periodos de carga alta de trabajo?		*	
¿Realiza 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?	*		
¿Existe una pre asignación para la solución de problemas específicos de tratamiento de datos?		*	
¿Se ha determinado una prioridad en la resolución de problemas de tratamiento de datos?		*	
¿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?	5		
¿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?	*		
¿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?	*		
¿Existen planes de formación 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?		*	
¿Se han desarrollado o adquirido procedimientos automáticos para resolver o evitar cierres del sistema (abrazos mortales)?		*	
¿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?		*	

Grafico 4.9: Checklist Confecciones Pazmiño Castillo

4.2 Conclusiones

- La infraestructura de red no posee las seguridades adecuadas, haciéndola vulnerable ante cualquier ataque interno o externo; por lo que hay que prevenir errores en un futuro y proporcionar las medidas necesarias para asegurar la integridad de los datos.

- El no tener software licenciado acarrea muchos inconvenientes tanto en su instalación como en su manejo; y el no saber la procedencia y su estado carece de un soporte original del mismo, arriesgándose en ocasiones a que este software sea manipulado para introducir algún malware. Así mismo no se puede tener las debidas actualizaciones del software ya que para ello se necesita tener un registro.

- El poseer Antivirus ineficientes, provoca que deje pasar los virus causando daños irreparables a las máquinas.

- El poseer varios servidores DHCP, ocasiona inconvenientes al momento de conectarse a la red, debido a que no se sabrá que servidor responderá la solicitud del cliente.

- El desconocimiento de contraseñas seguras en los equipos de cómputos, hace que personas puedan acceder fácilmente a la información.

4.3 Recomendaciones

- Es necesario implementar políticas de seguridad, para proteger la información tanto en nivel físico como lógico, debido a que no existe una restricción jerárquica y hay facilidad para acceder a los datos de la compañía.

- Crear un plano donde describa la infraestructura de la red y tener la documentación de la misma, así como también del antivirus; esto ayudará en un futuro a obtener una solución efectiva.

- Se recomienda que todas las máquinas tengan licenciado y actualizado el sistema operativo ya que esto ayudará en los recursos de la empresa y a optimizar el tiempo para alcanzar resultados eficientes.

- Las computadoras deben tener un mantenimiento mínimo semestral, debido a la actividad económica de la empresa.

- La información es de vital importancia por lo cual se debe implementar un sistema de Backus, ya que la pérdida de información genera retrasos en la programación destinada a las labores cotidianas.

- Todos los equipos y dispositivos deben tener toma eléctrica regulada, para evitar daños en los mismos.

- Se recomienda corregir la configuración en los servidores DHCP, para que no genere interrupciones en la conexión.

Referencias

ACISSI. (2011). *Seguridad Informática Ethical Hacking.* Barcelona: Ediciones ENI.

Aguilar, G. H. (26 de 09 de 2012). *Scridb.* Recuperado el 01 de 03 de 2013, de Objetivos de la Auditoría Informática: http://es.scribd.com/doc/81128724/17/Objetivos-de-la-auditoria-informatica

Bertucci, J. (17 de 06 de 2011). *Scribd.* Recuperado el 06 de 07 de 2012, de Auditoría en Infomática: http://es.scribd.com/doc/58107282/Auditoria-a-Unidad-II-6

Hurtado, A. G. (2011). *SEGURIDAD INFORMÁTICA Sistemas Microinformáticos y Redes.* Madrid, España: Gráficas Rogar.

López, P. A. (2010). *SEGURIDAD INFORMÁTICA.* Madrid: Editex S.A.

Piattini, M. G. (2005). *AUDITORÍA INFORMÁTICA Un enfoque practico 2da edicion.* México: ALFA OMEGA GRUPO EDITOR S.A.

Rivas, G. A. (1989). *Auditoría Informática.* Madrid: Ediciones Díaz de Santos S.A.

Santos, J. C. (2010). *SEGURIDAD INFORMÁTICA.* Madrid - España: Editorial Ra-Ma.

Wener, J. L. (01 de Mayo de 2010). *EQUIPAMENTO TECNOLOGICO-Seguridad y mantenimiento*. Recuperado el 24 de Febrero de 2013, de http://recursostic.educacion.es/observatorio/web/es/component/content/article/805-monografico-seguridad-en-internet?start=2

Anexos

Quito, 28 noviembre 2011

INFORME DEL ESTADO FINAL DE LA RED DE DATOS DE LA EMPRESA CONFECCIONES PAZMIÑO CASTILLO CIA. LTDA.

INTRODUCCIÓN

Simax certifica que la empresa otorga garantía técnica a la instalación de cableado estructurado que se detalla a continuación, por el tiempo de 1 año, vigente a partir de la fecha de entrega de la factura correspondiente.

Confecciones Pazmiño Castillo, ubicada en la calle Juan Procel OE7-43 y el Reventador; teléfono 2490757.

MATERIALES

1. Cable UTP categoría 6

Especificaciones Técnicas:

- rendimiento mínimo 1000BASE-T
- IEEE 802.3ab,
- IEEE 802.3af Poder sobre Ethernet para Voz sobre IP,
- Testeado a 650 mhz mínimo
- Verificado por ETL, UL
- TIA/EIA 568-B.2-1
- Gigabit Ethernet / 1000BASE-T / IEEE 802.3ab
- 4 Pair 23 AWG UTP
- características eléctricas TIA/EIA 568-B.2-1 Y ISO/IEC 11801 Categoría 6

- 28 Mínimo dB ACR 100 MHz
- ATM hasta 155 Mbps,
- ANSI.X3.263 FDDI TP-PMD

2. Patch Panel Circuito Impreso (24 puertos)

Especificaciones Técnicas:

- Perdida de Retorno tipica de 20dba 200 mhz para proporcionar un margen de 11dB
- Verificado por ETL , UL
- Certificado por CSA
- Velocidad a 300mhz
- Desempeño a Gigabit Ethernet verificado, según las especificaciones de IEE802.3ab

Dimensiones

Puertos	Altura(mmS)	Unidades de Rack
24	1.75" (45)	1

3. Modulo RJ-45

Especificaciones Técnicas:

- Categoría 6
- Contactos en punta – Cobre de berilio con un mínimo de 50 micro-pulgadas de cobertura de oro sobre níquel.
- PS-ACR 300 MHz
- Desempeño de transmisión de 10GBE
- Desempeño verificado de Gigabit Ethernet, conforme al especificaciones de IEEE 802.3ab en Cat. 6
- Contactos IDC 110-100 micros - pulgadas de cobertura de plomo estañado 60/40 sobre bronce fósforo.
- Verificado por ETL, UL, CSA

4. Cordones de Parcheo

Especificaciones Técnicas:

- 1000BASE-TX (TIA-854)

- 10/100/1000BASE-T (IEEE 802.3).
- Voz (Análoga y Voz (VoIP) Digital.
- Categoría 6
- Modulo RJ-45 Contactos en punta – Cobre de berilio con un mínimo de 50 micro-pulgadas de cobertura de oro sobre níquel.
- aplicaciones IEEE 802.3af
- Verificado por ETL, UL
- Longitudes (pulgadas) : 3", ,10"

5. Rack de Piso

Especificaciones Técnicas:

- Rack de piso color Negro altura 10', 45 unds, 19" de ancho
- Construido en Aluminio Ligero , capacidad para 500 lbs .
- Ancho de Rack de 19", Ancho del Canal 3.25" acabado en color negro, hendiduras Frontales / Traseras para pasar el cable

6. Organizador Horizontal

Especificaciones Técnicas:

- Organizador de Cables Horizontal de 19" de ancho,2 unidades de Rack ,3.50 " de altura del panel , 3.50 de profundidad de anillo, con cubierta, con organizador trasero de cable.

DIRECCIONAMIENTO

1. Red de administración de equipos:

En esta red están los equipos que tengan dirección de administración, a través de la cual se accede a su configuración, a continuación el detalle:

CLASE A PRIVADA	10.0.0.0/8
SWITCH 01	10.90.90.90
SWITCH 02	10.90.90.91
AP 01	10.90.90.93

2. **VLANS**

Se configuraron 3 VLANs para segmentar el dominio de broadcast, a continuación el detalle:

VLAN 01 **Nombre:** Servidores
Descripción: En esta vlan están los dos servidores de aplicaciones de la empresa.

VLAN 02 **Nombre:** Administración
Descripción: En esta vlan están los equipos de cómputo de administración y contabilidad

VLAN 03 **Nombre**: Internet
Descripción: En esta vlan está el servidor de internet kypus.

3. IPS de usuarios

Al momento todos los equipos se encuentran en la red 192.168.0.0/192, en esta red máxima se tienen 62 ips asignadas dinámicamente por el servidor DHCP.

4. Distribución de puertos

A continuación se detallan los puertos asignados a los diversos equipos de red de la empresa:

UBICACION DE PUERTOS SW01		
REFERENCIA	**PUERTOS SW1**	**ETIQUETA**
RELOJ-01	DATOS 01	CTC01-1A-01
BODEGA	DATOS 02	CTC01-1A-02
RECEPCION	DATOS 03	CTC01-1A-03
CONTADOR1	DATOS 04	CTC01-1A-04
CONTADOR2	DATOS 05	CTC01-1A-05
ROUTER	DATOS 06	CTC01-1A-06
JAZMIN	DATOS 07	CTC01-1A-07
CONTADOR	DATOS 08	CTC01-1A-08

GERENTE COMERCIAL	DATOS 09	CTC01-1A-09
CAMARAS	DATOS 10	CTC01-1A-10
SUBGERENTE	DATOS 11	CTC01-1A-11
SALA DE REUNIONES	DATOS 12	CTC01-1A-12
ACCESS POINT	DATOS 13	CTC01-1A-13
GERENTE GENERAL	DATOS 14	CTC01-1A-14
SERVIDOR APLICACIÓN	DATOS 15	CTC01-1A-15
SERVIDOR DISEÑO	DATOS 16	CTC01-1A-16
KYPUS	DATOS 17	CTC01-1A-17
RELOJ-02	DATOS 18	CTC01-1A-18
LIBRE	DATOS 19	CTC01-1A-19
LIBRE	DATOS 20	CTC01-1A-20
LIBRE	DATOS 21	CTC01-1A-21
LIBRE-ADMINISTRACION SWITCH	DATOS 22	CTC01-1A-22
BACKBONE	DATOS 23	CTC01-1A-23
BACKBONE	DATOS 24	CTC01-1A-24
UBICACION DE PUERTOS SW02		
REFERENCIA	**PUERTOS SW1**	**ETIQUETA**
DISEÑO PC-01	DATOS 01	CTC01-1A-01
DISEÑO PC-02	DATOS 02	CTC01-1A-02
DISEÑO PC-03	DATOS 03	CTC01-1A-03
DISEÑO PC-04	DATOS 04	CTC01-1A-04
DISEÑO PC-05	DATOS 05	CTC01-1A-05
PRODUCCION DOLORES	DATOS 06	CTC01-1A-06
PRODUCCION PC7	DATOS 07	CTC01-1A-07
PRODUCCION PC8	DATOS 08	CTC01-1A-08
PRODUCCION PC9	DATOS 09	CTC01-1A-09
PRODUCCION PC10	DATOS 10	CTC01-1A-10
BODEGA	DATOS 11	CTC01-1A-11
CORTE	DATOS 12	CTC01-1A-12
PASILLO	DATOS 13	CTC01-1A-13
LIBRE	DATOS 14	CTC01-1A-14
LIBRE	DATOS 15	CTC01-1A-15
LIBRE	DATOS 16	CTC01-1A-16
LIBRE	DATOS 17	CTC01-1A-17
LIBRE	DATOS 18	CTC01-1A-18
LIBRE	DATOS 19	CTC01-1A-19
LIBRE	DATOS 20	CTC01-1A-20
LIBRE	DATOS 21	CTC01-1A-21
LIBRE-ADMINISTRACION SWITCH	DATOS 22	CTC01-1A-22
LIBRE	DATOS 23	CTC01-1A-23
LIBRE	DATOS 24	CTC01-1A-24

5. Seguridades

En vista que la empresa no cuenta con políticas de seguridad se mantienen las contraseñas por defecto hasta que a futuro las cambien en base a los requisitos definidos en las políticas de seguridad.

CONTRASEÑAS		
SWITCH 01	USUARIO	ADMIN
	PASSWORD	
SWITCH 02	USUARIO	ADMIN
	PASSWORD	
ACCESS POINT 01	USUARIO	ADMIN
	PASSWORD	

6. Recomendaciones

- Es urgente que se definan las políticas de seguridad de la empresa, y que se las dé a conocer a todo el personal, como sugerencia se las puede ingresar al sitio web, algunas de las subsiguientes sugerencias deberían ir en las políticas de seguridad de la empresa.
- La red de administración de equipos debe estar separada de la red interna de la empresa.
- Si se piensa segmentar la red en subredes se recomienda enrutarlas usando el kypus.