ESCUELA DE TECNOLOGÍA EN REDES Y TELECOMUNICACIONES

AUDITORIA DE SEGURIDAD INFORMÁTICA INTERNA Y PERIMETRAL PARA LA EMPRESA SERVIHELP S.A.

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

Profesor Guía:
Ingeniero Jack Vidal

Autor:
Gabriel Eduardo Jarrín Ortiz.

Año

2013

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.”

……

Jack Vidal

Ingeniero

Número Cédula

1711502920

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”

…….

Gabriel Eduardo Jarrín Ortiz.

1719670570

AGRADECIMIENTO

En primer lugar agradezco a Dios por todas sus bendiciones. Agradezco a todas las personas que estuvieron a mi lado apoyándome en el trascurso de mi vida. Agradezco a todos los profesores que me han transmitido sus conocimientos. A mi madre quien supo guiarme y brindarme todo su apoyo la que deposito su confianza en mí y nunca me dejo solo hasta alcanzar mí objetivo.

DEDICATORIA

Este logro se lo dedico a mi madre quien con su amor y enorme sacrificio ayudo a sus hijos a cumplir sus metas demostrándole que todo su esfuerzo no fue en vano. Se lo dedico a Dios quien me ha bendecido con una familia que me quiere y siempre ha estado a mi lado en los buenos y malos momentos

RESUMEN

Este proyecto se enfoca sobre las seguridades y vulnerabilidades de la red LAN que opera con datos y telefonía, esto se enfocara en la verificación de toda la red y todos los servicios que maneje la misma.

Utilizaremos varias herramientas que nos permita buscar vulnerabilidades en la red para así probar la seguridad de firewall como también se realizara la verificación de los equipos utilizados en la red.

Las verificaciones que realizaremos en la red serán basadas en los siguientes aspectos:

- Firewall los filtros, ancho de banda y su direccionamiento IP
- El medio físico de la red WAN
- Las características de equipos activos
- El cableado estructurado y sus componentes
- Condiciones y uso de la red LAN datos y telefonía
- Seguridad y características de servidores
- Recursos necesarios e innecesarios
- Respaldos de información
- Contraseñas seguras
- Análisis de la integridad y protección de archivos de la red
- Protección de antivirus y su seguridad

ABSTRACT

This project focuses on securities and LAN network vulnerabilities that operates with data and telephony, it will focus on the verification of the entire network and all the services that manage it.

We will use various tools to enable us to find vulnerabilities in network security and firewall testing and also undertake the verification of the equipment used in the network.

The verifications to carry out in the network will be based on the following:

- Firewall filters, bandwidth, IP address
- The physical environment of the WAN
- Characteristics of active devices
- Structured cabling and components
- Terms and LAN network usage data and telephony
- Security and Server Features
- Resources necessary and unnecessary
- Backups of information
- Passwords
- Analysis of the integrity and protection of network file
- Virus protection and security

ÍNDICE

Introducción

El término de auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación, cuyo único fin es detectar errores y señalar las fallas. De todo esto sacamos como deducción que la auditoria es un examen crítico pero no mecánico, que no implica preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

A finales del siglo XX, los Sistemas Informáticos se han constituidos en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los sistemas de información de la empresa.

La información que es transmitida en una red es crítica, por lo tanto es necesario mantener la información segura aplicando políticas y procesos de acuerdo a las necesidades de una empresa o usuarios. La tecnología ha avanzado de manera vertiginosa y de la misma forma también los riesgos y amenazas para vulnerar las seguridades. Actualmente las redes de telecomunicaciones están basadas en plataformas IP las mismas que nos permiten brindar mayor seguridad ya que poseen herramientas que nos ayudan a mantener una red informática segura.

El término de Seguridad quiere decir que se debe proteger contra intrusos internos y externos que quieren acceder a información confidencial que solo pueden acceder personas autorizadas.

Una auditoria Informática nos permite verificar las vulnerabilidades de los sistemas informáticos y de acuerdo a los resultados obtenidos podemos implementar, actualizar o corregir políticas de seguridad.

La informática es el campo que se encarga del estudio y aplicación práctica de la tecnología, métodos, técnicas y herramientas relacionados con las computadoras y el manejo de la información por medios electrónicos, el cual

comprende las áreas de la tecnología de información orientadas al buen uso y aprovechamiento de los recursos computacionales para asegurar que la información de las organizaciones (entidades internas y externas de los negocios) además es el proceso metodológico que se desarrolla de manera permanente en las organizaciones.

1 Capítulo I Marco Teórico

1.1 Definición del proyecto.

1.1.1 Antecedentes

La empresa SERVIHELP S.A especializada en ingeniería de redes de alta tecnología y en telecomunicaciones con desarrollos propietarios en voz sobre IP (VOIP) consiste en la creación de una red de transmisión de alta frecuencia que integra servicios de Voz, Video y Datos, los mismos que serán trasmitidos por un solo cable.

Según información recopilada la empresa SERVIHELP S.A posee una infraestructura de red antigua, 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 posee una ventilación adecuada para el buen funcionamiento y evitar deterioro de los mismos.

A continuación se detallan los puntos que se consideran críticos dentro de su infraestructura:

1. El enlace de última milla de servicio de internet que provee la empresa Tv Cable tiene muchos problemas de caídas y perdidas en el servicio.
2. La estructura de la red no presenta un buen desempeño y sus funciones no se cumplen correctamente.
3. Mala organización del rack donde se encuentran servidores y equipos activos.
4. No existe documentación de equipos con licencia.
5. La empresa no consta con un sistema de respaldo de la información.

1.1.2 Formulación del problema

Con respecto al enlace de última milla el problema que genera es grande ya que la empresa necesita salir a internet para la comunicación con clientes y proveedores y el tiempo de respuesta por parte del proveedor para resolver el problema es demasiado lento.

La red no presenta un buen funcionamiento ya que por la misma pasan los servicios de voz y datos y no se encuentran separados en segmentos con redes virtuales (Vlan) que puedan generar un mejor funcionamiento y proveer calidad de servicio (QoS) para la red.

La existencia del firewall es indispensable en una empresa pero para que sea una buena arma contra las amenazas tenemos que complementar con filtros, permisos y perfiles para poder llevar control en el sistema de navegación y compartición de archivos.

La principal consecuencia de manejar sistemas operativos piratas es su bajo rendimiento ya que posee limitaciones con respecto a actualizaciones que necesita el sistema para realizar mejoras en el mismo.

Al no tener un sistema de antivirus estándar afecta a la misma empresa ya que los computadores tienen el riesgo de infectarse con malware, gusanos, troyanos y virus esto puede introducirse en la red y eliminar archivos importantes de la empresa.

Uno de los problemas más graves que se detectaron es el no tener respaldos de la información de red tanto en servidores y sistemas que utiliza el usuario final. Podrían existir daños en los servidores y esta generaría pérdida de la información la misma que ocasionaría una perdida para la empresa.

1.1.3 **Objetivo General**

Encontrar las vulnerabilidades existentes en la empresa SERVIHELP S.A para prevenir amenazas y pérdidas de información.

1.1.4 **Objetivo especifico**

Realizar un análisis de la estructura de la red con el propósito de alertar a la empresa de mal funcionamiento y riegos a correr.

Utilizar herramientas de redes y telecomunicaciones para evaluar la red y comprobar sus defensas ante amenazas.

Realizar informe sobre las recomendaciones para aplicar a la red para mejorar el uso y defensas de la misma y evitar amenazas para obtener una red confiable.

1.1.5 Alcance

Realizar todas las recomendaciones necesarias detallando cada problema que tiene la empresa con respecto amenazas informáticas y perimetrales con su respectiva solución para mejorar su red y se encuentre preparada para cualquier ataque o auditoria.

1.1.6 Justificación del proyecto

Con la realización del proyecto se pondrá en práctica los conocimientos obtenidos y nuestro nivel profesional para garantizar el buen funcionamiento de la estructura de red de la empresa SERVIHELP S.A.

Con este proyecto se espera que las actividades de la empresa SERVIHELP S.A tales como transmisión de datos, envío de correos y otros servicios se encuentren seguros, respaldados y confiables ante cualquier ataque o pérdida de información.

La realización del proyecto se lo hará con normas y estándares dispuestos en redes y telecomunicaciones.

1.2 Introducción Auditoria Informática

1.2.1 Concepto de Auditoria

“La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

De este modo la auditoria informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoria:

- Objetivos de protección de activos e integridad de datos
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software.

En muchos casos ya no es posible verificar manualmente los procedimientos informáticos que resumen, calculan y clasifican datos por lo que se deberá emplear software de auditoría y otras técnicas asistidas por computador

El auditor es responsable de revisar e informar a la dirección de la organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por el auditor informático:

- Participar en las revisiones durante y después del diseño, realización implantación y explotación de aplicaciones informáticas así como en las fases análogas de realización de cambios importantes.
- Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraude.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

1.2.2 Control interno y auditoria informática

Se puede definir el control interno como cualquier actividad o acción realizada manual y automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día en medida que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar procesos de aplicaciones y para gestionar los sistemas de información.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos otros son completamente manuales y muchos dependen de una combinación de elementos de software y procedimientos.

Históricamente los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- Controles preventivos: Para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- Controles detectivos: Cuando fallan los preventivos para tratar de conocer cuanto antes el evento
- Controles correctivos: Facilitan la vuelta a la normalidad cuando se han producido incidencias.

Como el concepto de controles se originó en la profesión de auditoría, resulta importante conocer la relación que existe entre los métodos de control, los objetivos de control y los objetivos de auditoría.

Los controles pueden implantarse a varios niveles diferentes. La evaluación de los controles de la tecnología de la información exige analizar diversos elementos interdependientes. Por ello es importante llegar a conocer bien la

configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implantarse los controles, así como para identificar posibles riesgos.

Para llegar a conocer la configuración del sistema es necesario documentar los detalles de red, así como los distintos niveles de control y elementos relacionados:

- **Entorno de red:** Consta de Esquema de la red, descripción de la configuración de hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los computadores y consideraciones relativas a la seguridad de la red.
- **Entorno de aplicaciones**: Procesos de transacciones, sistemas de gestión de base de datos.
- **Productos y herramientas**: Software para desarrollo de programas y para operaciones automáticas.
- **Seguridad del computador**: Identificar y verificar usuarios, control de acceso, registro de información, integridad del sistema, controles de supervisión
- **Administración del sistema**: Controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema incluyendo la administración de las redes.
- **Seguridad:** Incluye a las tres clases de controles fundamentales implantados en el software del sistema, integridad del sistema, confidencialidad y disponibilidad

1.2.3 Procedimientos

La opinión profesional, elemento esencial de la auditoria, se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma.

Como es natural cada una de las clases o tipos de auditoría posee sus propios procedimientos para alcanzar el fin previsto aun cuando puedan en muchos casos coincidir. El alcance de la auditoria, concepto de la vital importancia nos viene dado por los procedimientos. La amplitud y profundidad de los procedimientos que se apliquen nos definen su alcance.

En las auditorias altamente reglamentadas como la financiera es preceptivo “aplicar las Normas técnicas y decidir los procedimientos de auditoría”, “Cualquier limitación que impida la aplicación de lo dispuesto en las Normas técnicas debe ser considerada en el informe de auditoría como una reserva al alcance”

Se pretenden garantizar que se toman en consideración todos los aspectos, áreas, elementos, operaciones, circunstancias que sean significativas.

Para ello se establecen normas y procedimientos que en cuanto a la ejecución de la auditoria se resumen en que:

- El trabajo se planificara apropiadamente y se supervisara adecuadamente
- Se estudiara y evaluara el sistema de control interno
- Se obtendrá evidencia suficiente y adecuada

Estas tres normas se deducen claramente de la situación real actual de los riesgos que ha de afrontar el auditor.

1.2.4 **Auditoria informática en las Empresas PYMES**

El presente capitulo pretende ser una contribución que se sume el esfuerzo por conseguir una mayor rentabilidad de los sistemas de información en las empresas y concretamente denominadas PYMES (Pequeñas y Medianas Empresas)

La importancia de las PYMES viene dada ante todo por su número, más de dos millones de empresas que conformen el tejido empresarial así como su

potencial ya que constituyen la base del desarrollo empresarial. Es un hecho por fin asumido por todos los estamentos públicos y privados de la sociedad actual 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 abordar 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.

Es así mismo un hecho perfectamente demostrado que el Control Interno informático y su auditoria permite gestionar y rentabilizar los sistemas de información de la forma más eficiente, optimizando, en suma y resultados.

Por este hecho hemos creído de interés abordar en el presente capitulo la exposición de este método de Auditoria Informática expuesto de forma breve y directa en la convicción de que poniéndolo en práctica se lograra que los Sistemas de Información sean fiables como exactos y ante todo den el fruto que los empresarios esperan de ellos.

1.2.5 **Metodología de la Auditoria Informática**

Según el diccionario de la lengua de la real academia española, METODO es el “modo de decir o hacer con orden una cosa”, Asimismo define el diccionario la palabra METODOLOGIA como “conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal”, Esto significa que cualquier proceso científico debe estar sujeto a una disciplina de proceso definida con anterioridad que llamaremos METODOLOGIA. La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta el desarrollo del software y como no, la auditoria de los sistemas de información.

Las metodologías usadas por un profesional dicen mucho de su forma de entender su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de "acierto/error". Así mismo una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo, por lo que resulta habitual el uso de metodologías en las empresas auditoras profesionales desarrolladas por los más expertos, para conseguir resultados homogéneos en equipos de trabajo. La proliferación de metodologías en el mundo de la auditoria y el control informático se puede observar en los primeros años de la década de los ochenta paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas .Pero el uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas cuyo uso de las metodologías constituye una práctica habitual, una de ellas es la seguridad de los sistemas de información.

Si definimos la SEGURIDAD DE LOS SISTEMAS DE INFORMACION como la doctrina que trata de los riesgos informáticos o creados por la informática entonces la auditoria es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso.

Por tanto, el nivel de seguridad en una entidad es un objetivo a evaluar y estar directamente relacionado con la calidad y eficacia de un conjunto acciones y medidas destinadas a proteger y preservar la información de la entidad y sus medios de proceso.

La informática crea unos riesgos informáticos de los que hay que proteger y preservar en la entidad con un entramado de contramedidas y la calidad y eficacia de las mismas, es el objetivo a evaluar para poder identificar sus puntos débiles y mejorarlos.

Esta es una de las funciones de los auditores informáticos por tanto debemos profundizar más en entramado y contramedidas para ver qué papel tienen las metodologías y los auditores en el mismo. Para explicar este aspecto diremos que cualquier contramedida nace de la composición de varios factores:

- **La Normativa:** Define la forma clara y precisa todo que existir y ser cumplido, tanto desde el punto de vista conceptual como practico, desde lo general a lo particular. Debe inspirarse en estándares, políticas y normas de empresa, experiencia y práctica profesional.
- **La organización:** La integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa. Este es el aspecto más importante, dado que sin el nada es posible. Se pueden establecer controles sin alguno de los demás aspectos, pero nunca sin personas ya que no son estas las que realizan los procedimientos y desarrollan los planes.
- **Las Metodologías:** Son necesarias para desarrollar cualquier proyecto que nos propongamos de manera adecuada y eficaz.
- **Objetivos de control:** Los objetivos a cumplir en el control de procesos este concepto es el más importante después de la ORGANIZACIÓN y solamente de planteamiento correcto de los mismos saldrán procedimientos eficaces y realistas.
- **Procedimientos de control:** Son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada para la consecución de uno o varios objetivos de control
- **Tecnología de seguridad:** Están todos los elementos ya sean HARDWARE o SOFTWARE que ayudan a controlar un riesgo informático. Dentro de este concepto están los cifradores, autentificadores, equipos tolerantes al fallo y las herramientas de control.
- **Herramientas de control:** Son elementos software que permitan definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Todos estos factores están relacionados entre sí, así como la calidad de cada uno con la de los demás. Cuando se evalúa el nivel de seguridad de sistemas en una institución se están evaluando todos los factores y se plantea un plan de seguridad nuevo que mejore todos los factores.

Al finalizar el plan se habrá conseguido una situación nueva en la que el nivel de control sea superior al anterior.

Se llamara plan de seguridad a una estrategia planificada de acciones y productos que lleven a un sistema de información y sus centros de procesos de una situación inicial determinada y a mejorar a una situación mejorada.

Las metodologías que podemos encontrar en la auditoria informática son dos familias distintas:

- Auditorias de controles generales
- Metodológicas de auditores internos

El objetivo de las auditorias de controles generales es dar una opinión sobre la fiabilidad de los datos del computador. El resultado externo es un informe de la auditoria donde se destacan las vulnerabilidades encontradas. Están basadas en pequeños cuestionarios estándares que dan como resultados informes muy generalistas.

Tienen apartados por definir pruebas y anotar sus resultados, esta es una característica clara de la diferencia con las metodologías de evaluación de la consultoría como la de análisis de riesgos que no tienen estos apartados, aunque también tratan de identificar vulnerabilidades o falta de controles.

Esto es la realización de pruebas es consustancial a la auditoria, dado que tanto el trabajo de consultoría como el análisis de riesgos espera siempre la colaboración del analizado y por lo contrario la auditoria debe demostrar con pruebas todas sus afirmaciones y por ello siempre debe contener el apartado de las pruebas. Llegando al extremo de que hay auditorias que se basan solo en pruebas como la auditoria de integridad.

Estas metodologías están muy desprestigiadas pero no porque sean malas, sino porque dependen mucho de la experiencia de los profesionales que la usan y existe una práctica de utilizarlas profesionales sin ninguna experiencia.

Ninguna de estas metodologías usa ayudas de contramedidas llegándose a la aberración de que utilizan metodologías de análisis de riesgos para hacer auditorias.

Todas estas anomalías nacen de la dificultad que tiene un profesional sin experiencia que asume la función auditora y busca una fórmula fácil que le permita empezar su trabajo rápidamente.

El auditor informático necesita una larga experiencia y una gran formación tanto auditora como informática.

Llegamos al punto en el que es necesario decir que la metodología de auditor interno debe ser diseñada y desarrollada por el propio auditor y esta será la significación de su grado de experiencia y habilidad.

El esquema metodológico del auditor está definido por el plan del auditor.

1.2.6 **Plan del Auditor Informático**

Es el esquema metodológico más importante del auditor informático. En este documento se debe describir todo sobre esta función y el trabajo que se realiza en la entidad debe estar en sintonía con el plan del auditor del resto de auditores de la entidad.

Las partes de un auditor informático deben ser al menos las siguientes:

- **Funciones**: Ubicación de la figura en el organigrama de la empresa, debe existir una clara segregación de funciones con la informática y de control interno informático y debe ser auditado también. Deben describirse las funciones de forma precisa y la organización interna del departamento con todos sus recursos.
- **Procedimientos**: Para las distintas tareas de las auditorias, entre ellas están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría redacción de informe final, etc.

- **Tipo de auditorías**: Existen 3 tipos de auditoría:
    - Según su alcance
    - La full o completa de una área (por ejemplo control interno, informática, limitada a un aspecto)
    - La Correective Action Review (CAR) que es la comprobación de acciones correctivas de auditorías anteriores.
- **Sistema de Evaluación:** Independientemente de que exista un plan de acciones en el informe final debe hacerse el esfuerzo de definir varios aspectos a evaluar, como el nivel de gestión económica, gestión de recursos humanos, cumplimientos de normas, etc. Así como realizar una evaluación global de resumen para toda la auditoria. Esta evaluación final nos servirá para definir la fecha de repetición de la misma auditoria en el futuro según el nivel de exposición que se le haya dado a este tipo de auditoría en cuestión.

1.2.7 Metodología de Auditoria Informática en las empresas PYMES

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

- R.O.A (Risk Oriented Approach) Diseñada por Arthur Anderser
- CHECKLIST o cuestionarios.
- AUDITORIA DE PRODUCTOS (Por ejemplo, Red local, Windows, sistemas de gestión, paquetes de seguridad)

En si las tres metodologías están basadas en la minimización de los riegos que se conseguirá en función de que existen los controles y de que estos funcionen. En consecuencia el auditor deberá revisar estos controles y su funcionamiento.

De estas tres metodologías, la más adecuada a la Auditoria de las PYMES es a nuestro juicio la de la CHECKLIST por ser la más fácil utilización.

Según algunos autores, no resulta necesario tener conocimientos informáticos para realizar una auditoría informática mediante la técnica utilizada en esta

guía (CHECKLIST) No obstante creemos necesario un mínimo de formación específica para al menos saber qué es lo que se quiere analizar así como algunos conceptos no nos resulten excesivamente extraños. Fundamentalmente esos conocimientos serán de la índole de:

- Minicomputador
- Red Local
- PC
- Periféricos
- Software de base
- Eficacia de un servicio informático
- Seguridad lógica
- Seguridad física
- Etc.

Así mismo será necesario conocer en profundidad el organismo, composición y características principales así como los medios de que se disponen plantillas, datos técnicos, etc.

Por su puesto es deseable que se tengan unos conocimientos informáticos más exhaustivos, pues pueden ayudar a la ponderación de los controles, pero insistimos en que no son indispensables.

1.2.8 **Metodologías de referencia**

La metodología utilizada es la evaluación de riesgos R.O.A (Risk Oriented Approach) Enfoque orientado al riesgo, recomendada por ISACA (Information System Audit) Asociación de Auditores de sistema de información.

Esta evaluación de riesgos se desarrolla sobre determinadas áreas de aplicación 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 es debido a que dichos controles tienen incidencia independiente, en cada una y que se pretende poder analizar cada área independientemente es necesaria dicha repetición. Asimismo los controles generales y algunos controles de características especiales como pueden ser los de bases de datos, se aplicaran teniendo en cuenta las particularidades de cada entorno.

La autoguía se encuentra dividida en varias áreas de riesgo, concretamente seis que son:

- Riesgo en la continuidad del proceso
- Riesgo en la eficacia del servicio
- Riesgos económicos directos
- Riesgos de la seguridad lógica
- Riesgos de la seguridad física

Riesgo de 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 el análisis estricto de estos riesgos puesto que si bien otros podrían afectar relativamente a la empresa o bien causarles perjuicios de diverso tipo, estos podrían ocasionar un verdadero desastre. No pretendemos ser alarmistas y por supuesto no todos los riesgos analizados llevan a paralizar la empresa, pero insistimos en tener muy en cuenta el análisis exhaustivo de estos riesgos.

Riesgos en la eficacia del servicio informática: Entenderemos 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.

Riesgos en la eficiencia del servicio informática: Entenderemos como eficiencia del servicio la mayor forma de realizar los procesos o trabajos ya sea a nivel económico o técnico pretendiendo con el análisis de estos riesgos mejorar la calidad del 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.

Riesgos económicos directos: En cuanto a estos riesgos se analizaran aquellas posibilidades de desembolsos directos inadecuados, gastos varios que no deberían producirse e incluso aquellos gastos derivados de acciones ilegales con o sin el consentimiento de la empresa.

Riesgos de la seguridad lógica: Como riesgos de la seguridad lógica entenderemos todos aquellos que posibiliten accesos no autorizados a la información mecanizada mediante técnicas informáticas o de otros tipos. Incluiremos igualmente aquellos inherentes a transmisiones pese a que quizá en determinados ámbitos de aplicación podrían constituir un área independiente pero que se anexan con el fin de compactar el sistema de análisis.

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

Todas estas áreas están incluidas en cada ámbito de aplicación de acuerdo con la división que dimos al principio de minicomputadores, redes locales y PC.

1.2.9 **Resultados de la autoguia**

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

El primer sistema se responderá con SI No o N/A (NO APLICABLE) estos cuestionarios de respuesta directa tendrán un valor numérico de 1 a 10 a la pregunta que habrá que poner en lugar de respuesta.

Tabla 1.Resultados de la autoguia.

Controles	**SI**	**NO**	**N/A**
¿Posee la instalación equipos de continuidad en caso de cortes de energía como pueden ser los sistemas de alineación interrumpido?	7	4	

En el caso que dispusiera de UPS (Sistema de alineación interrumpida) se pondrá en la casilla del SI el valor de 7, En caso contrario pondríamos 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 guía 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 máximos por ejemplo:

Tabla 2.Resultados de la autoguia.

Controles	**SI**	**NO**	**N/A**
Evalué la carga de trabajo en época alta de proceso (Ponga el resultado en la casilla no) 1-30	7	4	

Como habrá observado también se le indicara en que casilla deberá incluir el resultado de su ponderación.

Por último existirán cuestiones que no tengan valoración sino que irán acompañadas de un asterisco. Estos controles son considerados de alto riesgo y 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. Por tanto estos controles deberán tenerse muy en cuenta a la hora de realizar la evaluación y en el caso de inexistencia dar primacía a su implantación.

Tabla 3.Sobre riesgo en la eficacia del servicio informático.

Controles	**SI**	**NO**	**N/A**
Existen planes a largo plazo para el departamento de informática			
Existen políticas para la planificación, control de 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.			
El D.I está separado orgánicamente en la estructura orgánica de la empresa.			
Es independientemente la ubicación de D.I de los otros departamentos de la empresa.			
Evalué la independencia de las funciones del personal entre las diferentes unidades.			
¿Existe una descripción por escrito (Manual de operaciones y procedimientos) de cada puesto en las diferentes unidades de D.I?			
Evalué la capacidad de los computadores disponibles para satisfacer la demanda en época alta			
Existe en calendario mantenimiento preventivo a los computadores			
¿Se verifica que dicho calendario no incluya revisiones en periodos de carga alta de trabajo?			
¿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?			
¿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?			
¿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 datos sensibles?			
¿Existe algún mecanismo de control que asegure una adecuada carga de la red especialmente en los periodos de trabajo crítico?			
¿Poseen todos los usuarios de la red especificaciones sobre disponibilidades, horarios, tiempo de respuesta, almacenamiento, respaldo y control operativo			
¿Existen planes formación para los usuarios de la red?			
¿Existen responsables que evalúen el correcto uso de la red por parte de los usuarios?			
Están perfectamente identificados todos los elementos físicos de la red (unidades de control, módems, cables etc.)			
¿Está asegurado en un tiempo prudencial la reparación o cambio de elementos físicos de la red?			
¿Se realiza por parte del 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 ha desarrollado o adquirido procedimientos automáticos para resolver o evitar cierres de sistemas en la red?			
Existen mecanismos que controlen los tiempos de respuesta de la red y la depuración de los fallos de operación de la misma			
¿Existe una rutina que se asegure que ningún proceso o dato de baja prioridad va a estar sin procesar en la red?			
¿Se controlan regularmente todos los procesadores de la red?			
¿Los sistemas Operativos que utilizan los computadores de usuarios son licenciados?			
¿Existe seguridad para el ingreso de utilización de los computadores?			

En cualquier caso siempre que se lleve a cabo una auditoria de empresa habrán de tenerse en cuenta como mínimo los siguientes controles generales:

Segregación de funciones, separación de los entornos de desarrollo y producción, control de programas, fuentes y objetivos, procedimientos, estándares o nomenclatura para toda clase de objetivos en el sistema de Información, plan de seguridad lógica y física (BACKUP o respaldo de datos y programas, etc.) y plan informático coordinado con el plan estratégico de la empresa.

Tanto atreves de la guía de autoevaluación como a través de la auditoria de los mencionados controles generales se puede alcanzar el objetivo de gestión y certificación de los datos logrando conseguir la calidad total de los Sistemas de Información, rentabilizando así las inversiones en Tecnología de la Información.

1.2.10 Herramientas y Técnicas para la Auditoria Informática

1.2.10.1 Cuestionarios

Las auditorias en informática se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamadas también evidencias.

Para esto, suele ser lo habitual comenzar solicitando la competición de cuestionarios pre impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación y muy cuidados en su fondo y forma.

1.2.10.2 Entrevistas

El auditor comienza a continuación con las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
- Mediante entrevistas en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
- Por medio de entrevistas en las que le auditor sigue un método preestablecido de antemano y busca finalidades concretas.

La entrevista es una de las actividades personales más importantes del auditor, en ellas este recoge más información y mejor matizada que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

1.2.10.3 **Checklist**

El auditor profesional y experto es aquel que reelabora muchas veces sus cuestionarios en función de escenarios auditados. Tiene claro lo que necesitaba saber y porque. Sus cuestionarios son vitales para el trabajo de análisis, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada. Muy por lo contrario el auditor conversara y hará preguntas normales que en realidad servirán para la completación sistemática de sus cuestionarios de sus Checklist.

Hay opiniones que descalifican el uso del Checklist ya que se consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalificada al auditor informático. Pero esto no es usar un Checklist es una evidente falta de profesionalismo.

El profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de Checklist, salvo excepciones las Checklist deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Los cuestionarios o Checklist responderán fundamentalmente a dos tipos de filosofía de calificación o evaluación:

- Checklist de rango:

  Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido

- Checklist Binaria:

  Es la que está constituida con respuestas única y excluyente: Si o No. Aritméticamente, equivalente a 1(uno) o 0(cero) respectivamente.

1.2.10.4 **Trazas o Huellas**

Con frecuencia, el auditor informático debe verificar que los programas tanto de los sistemas como de usuario, realizan exactamente las funciones previstas y no otras. Para ello se apoya en productos Software muy potentes y modulares que entre otras funciones, rastrean los caminos que siguen los datos atreves del programa.

Muy especialmente estas trazas se utilizan para comprobar la ejecución de las validaciones de datos.

Las mencionadas trazas no deben modificar en absoluto el sistema. No obstante la utilidad de las trazas, ha de repetirse lo expuesto en la descripción de la auditoria informática de sistemas, el auditor informático emplea preferentemente la amplia información que proporciona el propio sistema.”(Piattini & del Peso Navarro, 1997)

1.3 Seguridad Informática

Se enfoca en la protección de la infraestructura computacional y de la información. La seguridad informática se encarga de proteger información, esta información protegida se conoce como privilegiada o confidencial, para la seguridad informática existe pilares que nos ayudan a mantener protegida la empresa los cuales son:

- Confidencialidad
- Integridad
- Disponibilidad
- Autenticidad

1.3.1 **Confidencialidad**

Quiere decir que la información que maneja solo puede tener acceso personas autorizadas.

Como medida para que nuestra información sea confidencial podemos utilizar cifrados y encriptación en la información el cual consiste en transformar la información dejándola ilegible en forma que solo el receptor pueda entenderla al momento de recibirla para lo cual necesitaría realizar un proceso de autentificación para acceder a la información.

1.3.2 **Integridad**

Quiere decir que la información no puede ser alterada en el trascurso del camino hasta llegar a su destino, para cual los sistemas de seguridad informática no deben permitir que la información se duplique y sea manipulada por usuarios no autorizados.

1.3.3 **Disponibilidad**

Nos indica que la información debe encontrarse funcionando correctamente y estar disponible para acceder a esa información solamente personas autorizadas.

1.3.4 **Autenticidad**

Asegura la identidad con respecto al origen de la información enviada, esto quiere decir que la información es enviada por la identidad que dice ser más no una suplantación por lo cual se utiliza una autentificación.

1.3.4.1 **Autentificación:**

Esta encargada de verificar la identidad de una persona que necesite acceder a un recurso, una autentificación va acompañada de una seguridad como las que se detallan a continuación:

- Mediante una contraseña segura
- Mediante un dispositivo
- Mediante un dispositivo Biométrico

1.3.4.2 **Contraseña segura:**

Una contraseña segura debe cumplir estos requisitos:

- Tener ocho caracteres como mínimo.
- No debe contener el nombre de usuario, el nombre real o el nombre de la empresa.
- No debe contener una palabra completa.
- Está compuesta por caracteres de cada una de las siguientes cuatro categorías:

Tabla 4.Contraseñas seguras

Categoría de caracteres	Ejemplos
Letras mayúsculas	A, B, C
Letras minúsculas	a, b, c
Números	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Símbolos	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' <> , . ? /

Para crear una contraseña segura se debe mezclar letras números símbolos en diferente orden.

1.4 Problemas de Seguridad Informática

1.4.1 **Ataques Informáticos**

Un ataque es un intento de una persona en este caso llamada (Hacker) quien busca los agujeros o vulnerabilidades para realizar daño a un sistema informático.

- **Hacker**: Son personas que tiene amplios conocimientos en el área de informática capaces de acceder a sistemas no autorizados.

Los objetivos de los hacker es buscar las vulnerabilidades existentes de la red con el fin de demostrar que no existe seguridad a la que ellos no puedan acceder.

1.4.2 **Amenazas Informáticas**

Una amenaza son programas informáticos, virus, gusanos etc. Que tienen como propósito alterar el funcionamiento de la red llevando infecciones al sistema operativo, estas infecciones pueden llegar al usuario por varios medios como se va a detallar a continuación:

- Dispositivos de almacenamiento extraíbles
- Navegación en Internet
- Compartición de archivos en red

1.4.3 **Vulnerabilidad Informática**

Esto quiere decir que un sistema se encuentra propenso a ser atacado ya que en el existen errores por los cuales pueden acceder para causar problemas en la red.

1.4.4 **Riesgo Informático**

Es un posible suceso ante una amenaza a información, recurso o sistema esto quiere decir que no es suficientemente seguro con la protección de datos y esto puede causar daños a la empresa.

2 Capítulo II Levantamiento de la información.

2.1 Estado de la información

Según el levantamiento realizado a la empresa SERVIHELP S.A se pudo verificar que el cableado estructurado ya es antiguo. También se verifico que el tráfico de las redes de telefonía y datos trabajan por el mismo cable de red es decir no se encuentran separados por segmentos.

Adicional poseen un rack abierto en el cual se encuentran los equipos activos de la empresa este rack no cuenta con ventilación ya que este se encuentra ubicado en un área abierta.

2.1.1 **Elaboración del diagrama de red de SERVIHELP**

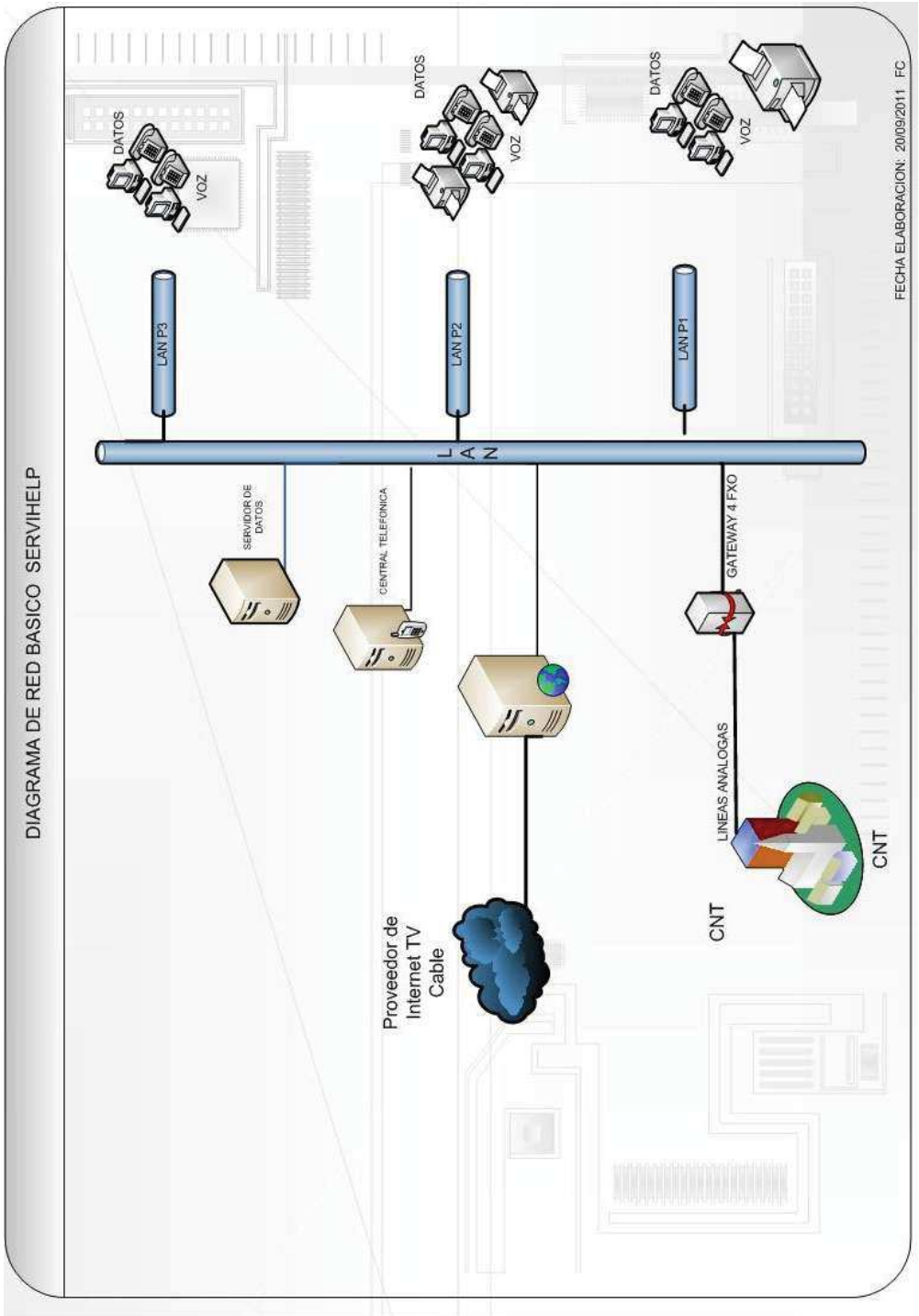


Figura: 1 Diagrama de red de la empresa SERVIHEL S.A.

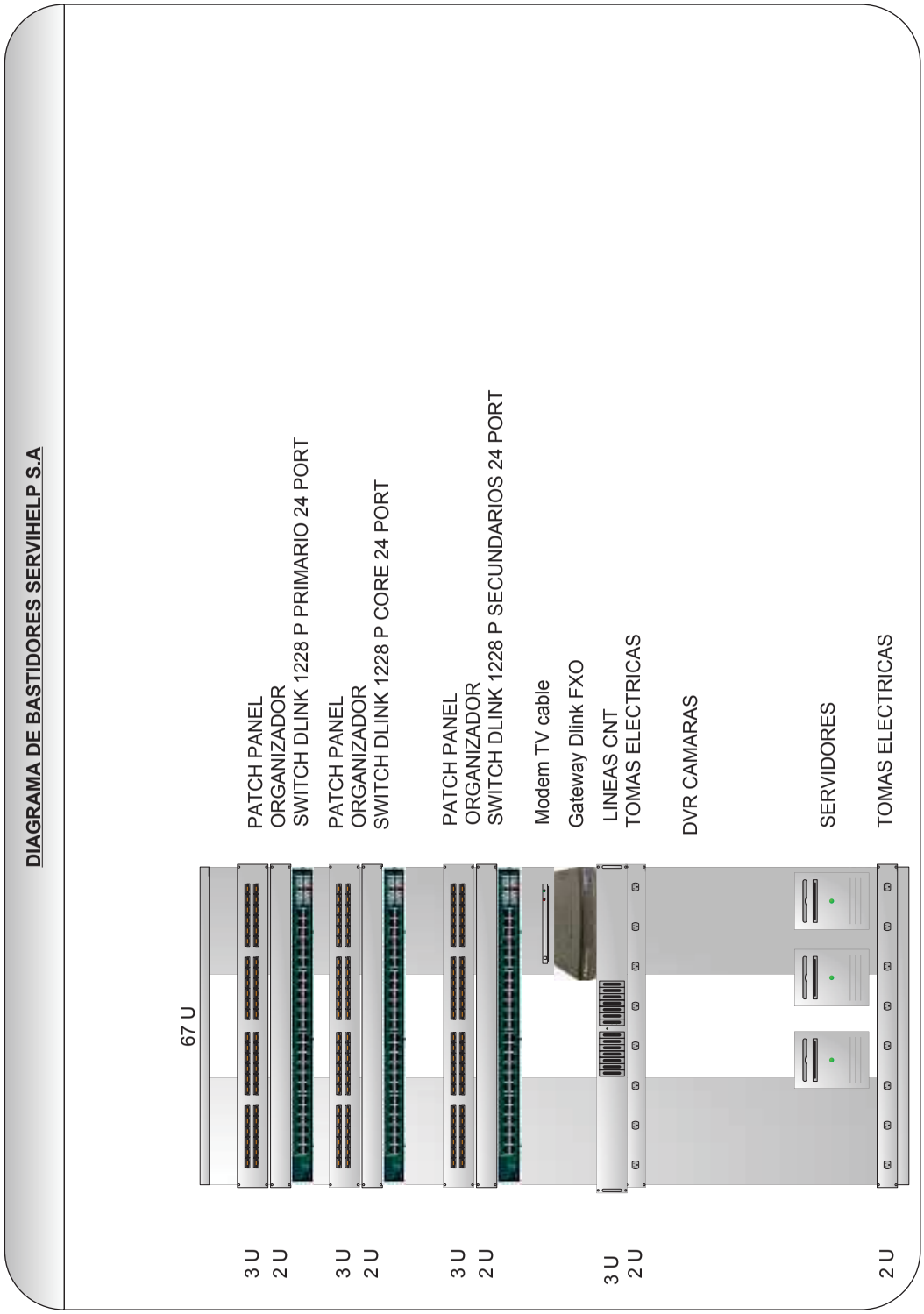


Figura: 2 Diagrama de Bastidores de la empresa SERVIHELP S.A.

2.1.2 Tipos de servidores

Servidor de Archivos

La función que cumple es el almacenamiento de archivos en un servidor los cuales se pueden compartir en una red LAN a través de protocolos o puertos específicos, el acceso a los archivos es mediante políticas de acceso basadas en usuario y/o grupos. Este servidor usa la aplicación Samba server la cual permite compartir archivos alojados en un servidor Linux a usuarios Microsoft sin necesidad de una interfaz adicional o propietaria.

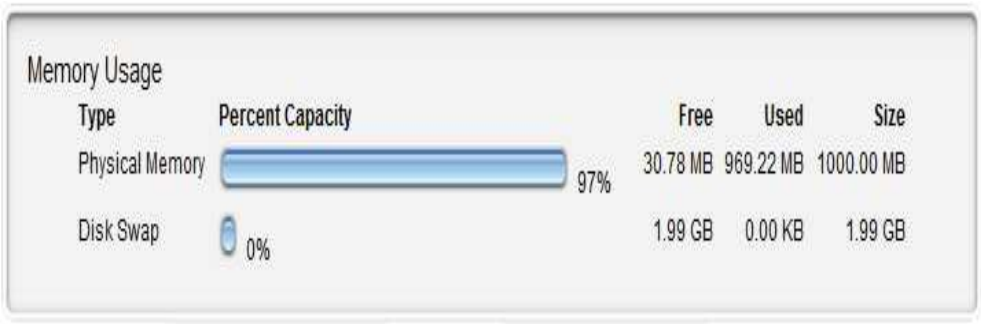


Figura: 3 Recursos Servidor archivos

Recursos:

Sistema Operativo:

- Red hat
- Samba server
- Clark connect versión 4.0

Características:

- Intel DG41RQ
- Procesador Intel® Core2 Dual
- Memoria RAM 2GB
- Disco duro Sata 1 Tera
- Tarjeta de red Dlink 10/100 Mbps

Servidor de internet

Este servidor realiza la función de distribuir el servicio de internet y de proporcionar el direccionamiento IP, actúa como servidor DHCP así como también de Firewall.

En este servidor se encuentra el proxy el cual crea los filtros y perfiles para la utilización de usuario final.

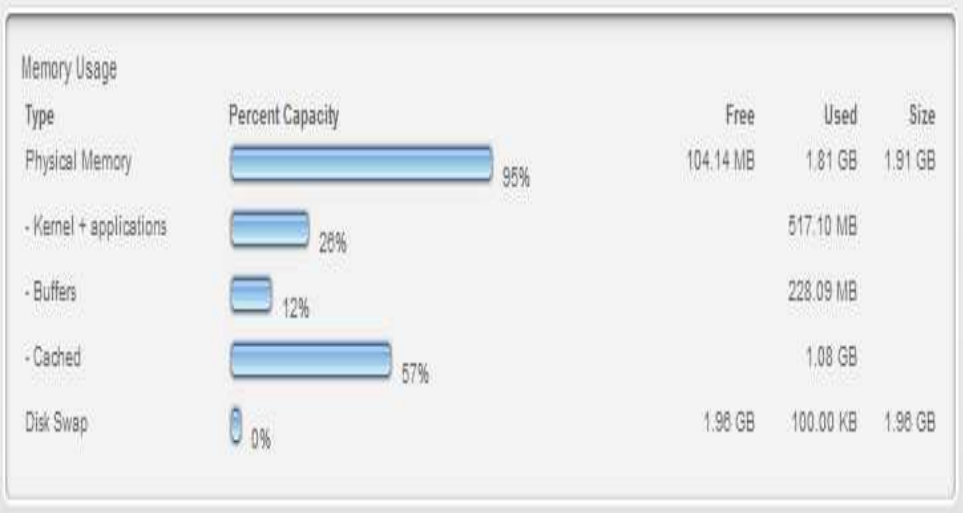


Figura: 4 Recursos Servidor Internet

Recursos:

Sistema Operativo:

- Red hat
- Clear OS versión 5.2

Características:

- Intel DG41RQ
- Procesador Intel® Core 2 Dual
- Memoria RAM 2Gb
- Disco duro Sata 160 GB
- 2 Tarjetas de red Dlink 10/100 Mbps

Servidor de Telefonía

Este servidor es el encargado de distribuir la telefonía interna y llamadas externas aquí se encuentran alojadas las líneas telefónicas para que se distribuya al usuario final como también la comunicación interna entre los usuarios.

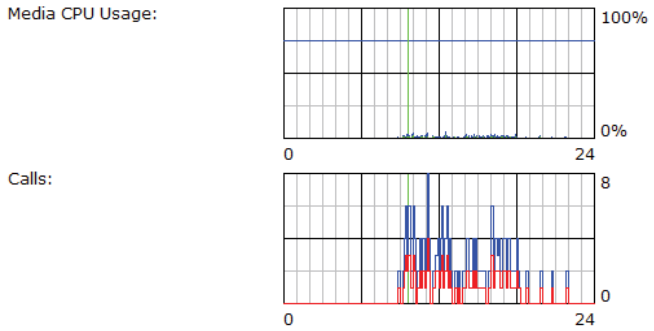


Figura: 5 Recursos Servidor Telefonía

Recursos:

Sistema Operativo

- Centos 5.0
- Software Masterbox IP propietario de SERVIHELP

Características:

- Intel DG41RQ
- Procesador Intel® Core 2 Dual
- Memoria RAM 2GB
- Disco duro Sata 160 GB
- 2 Tarjeta de red Dlink 10/100 Mbps

2.1.3 Infraestructura

Cableado

La empresa cuenta con cableado estructurado categoría 5 llega a la estación de trabajo con terminación faceplate doble.

Figura: 6 Faceplate Doble (Electrisistemas del Caribe)

La empresa cuenta con 54 puntos de red, 27 puntos para datos y 27 puntos para telefonía el cual es distribuido de la siguiente manera:

Planta baja

Área de Bodega

- 1 Punto de red de Voz
- 1 Punto de red de Datos

Área de Adquisiciones

- 1 Punto de red de Voz
- 1 Punto de red de Datos

Recepción

- 1 Punto de red de Voz
- 1 Punto de red de Datos

Área de Nuevas Tecnologías

- 5 Puntos de red de Voz
- 5 Puntos de red de Datos

Área de Ventas

- 2 Puntos de red de Voz
- 2 Puntos de red de Datos

Segundo Piso

Área de Gerencia

- 1 Punto de red de Voz
- 1 Punto de red de Datos

Área Administrativa

- 1 Punto de red de Voz
- 1 Punto de red de Datos

Área de Contabilidad

- 3 Punto de red de Voz
- 3 Punto de red de Datos

Área de Compras publicas

- 1 Punto de red de Voz
- 1 Punto de red de Datos

Área de Recursos Humanos

- 2 Punto de red de Voz
- 2 Punto de red de Datos

Sala de Reuniones

- 3 Punto de red de Voz

- 3 Punto de red de Datos

Área de Proyectos

- 6 Puntos de red de Voz
- 6 Puntos de red de Datos

No poseen cuarto de equipos tienen un Rack de piso de 40 u abierto

Switchs

La empresa SERVIHELP posee 3 equipos Switch con las siguientes características:

- Marca Dlink
- Modelo 1228P
- 24 Puertos 10/100
- 4 Puertos 10/100/1000
- 2 Puertos SFP
- Soporta 802.1q (Vlan)
- Soporta QoS (Calidad de servicio)
- Soporta 24 puertos Ethernet POE(Power Over Ethernet)

Estos switch se encuentran interconectados en entre sí, además realizan la interconexión de los equipos terminales como también se encuentran conectados los servidores de diferentes servicios.

Estos equipos switch se encuentran trabajando en la Vlan 01 (defecto). En la cual trabajan las redes de datos y telefonía

2.1.4 Equipos terminales

La empresa SERVIHELP S.A dispone de 49 equipos terminales los se distribuyen de la siguiente manera:

- 20 computadores de escritorio

- 5 computadores portátiles.
- 20 teléfonos IP
- 4 impresoras de red

El 90% de los computadores poseen el sistema operativo Windows XP Services pack 2 y el 10 % utilizan el sistema operativo Windows 7ultímate.

Cada equipo terminal posee una cuenta de usuario de Administrador y un usuario con cuenta limitada, el 100% de las cuentas como administrador poseen una contraseña segura pero el 50% de las cuentas limitadas no poseen una contraseña segura.

En los equipos terminales de encuentran instalado el Antivirus Avast que lo poseen el 100% de los equipos este antivirus se encuentra con vigencia hasta el 2018 ya que cuenta con licencia crack

El direccionamiento que utiliza la empresa para la red de datos es por DHCP de Clase C no utiliza subredes.

La Empresa SERVIHELP S.A cuenta con 20 teléfonos IP los cuales son utilizados para el ingreso o salida de llamadas. Estos teléfonos utilizan una dirección IP en la red de telefonía

El direccionamiento utilizado para la red de telefonía es de clase B subneteada para 254 host.

La topología de red que utiliza la empresa SERVIHELP es de tipo estrella.

3 Capítulo III Auditoria

3.1 Evaluación de Antivirus

La empresa SERVIHELP S.A se encuentra trabajando con el antivirus AVAST el mismo que procederemos a evaluar con una serie de pruebas para comprobar el funcionamiento y protección en lo equipos.

Para realizar esta evaluación se ha utilizado la herramienta EICAR como gestor de pruebas hacia el antivirus.

EICAR: Es una herramienta de test de antivirus desarrollada por el Instituto Europeo para la investigación de antivirus informáticos y por la organización de investigación de antivirus informáticos para probar la respuesta del funcionamiento de los antivirus en los equipos.

La razón de la herramienta EICAR es permitir a las personas, empresas, programadores de antivirus probar su software sin tener que utilizar un verdadero virus que pueda causar un daño real al no responder el antivirus correctamente.

Primera Prueba

La primera prueba consiste en ingresar a la página de EICAR y realizar una descarga de un archivo que posee la extencion.com el cual está compuesto por una serie de códigos, ya que esta cadena de códigos representa un virus perjudicial. Al momento de realizar la descarga del archivo nuestro antivirus debe informar que ha encontrado una amenaza en el caso de que esté funcionando correctamente.

En el caso de no responder significa que nuestro antivirus no se encuentra protegiendo a los equipos y no representan una seguridad a los usuarios.

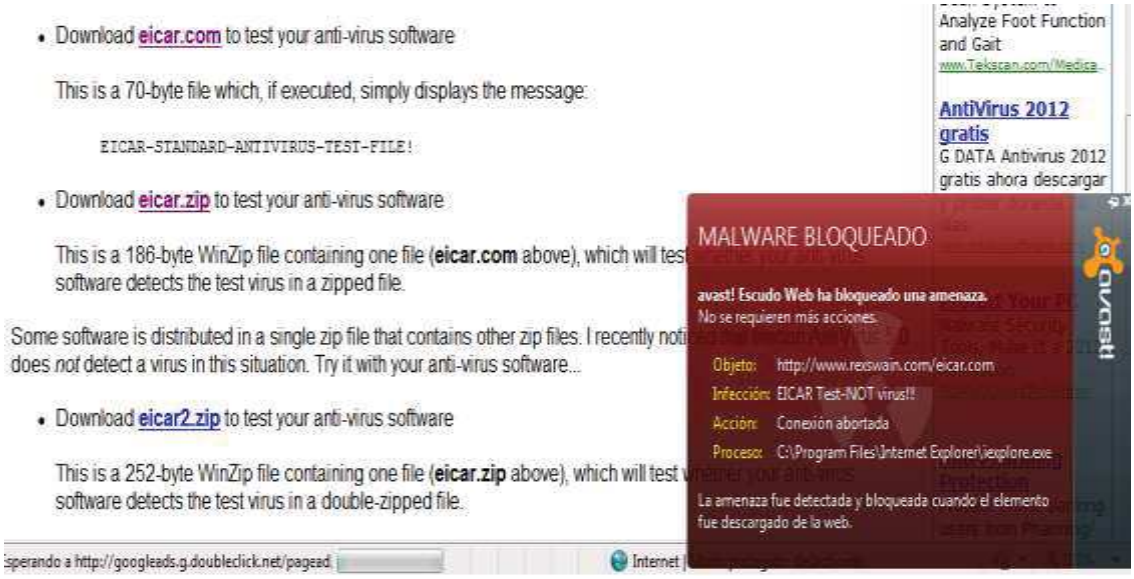


Figura: 7 Pruebas EICAR

Segunda Prueba

Es realizando una descarga de un archivo infectado con la extencion.zip que se encuentra comprimido, el antivirus tendrá que detectar el virus que se encuentra oculto dentro de esta carpeta.

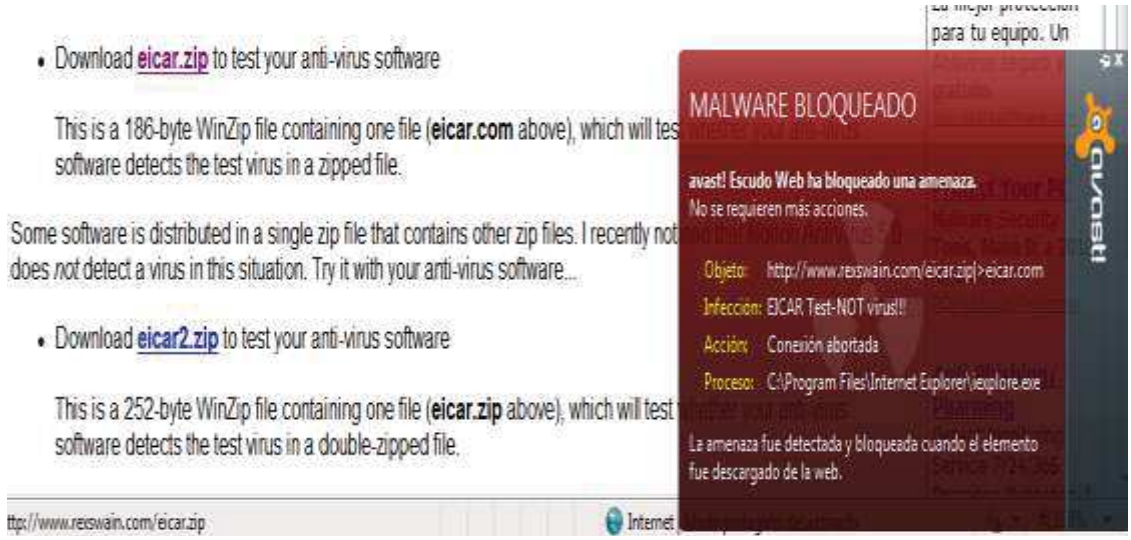


Figura: 8 Prueba EICAR

3.2 Evaluación Servidor de Correo

La empresa SERVIHELP S.A no posee un servidor de correo localmente ya que la empresa cuenta con un dominio que se encuentra alojado en los servidores de Google.

El correo electrónico es el medio de comunicación más utilizado a nivel mundial para realizar él envió y recepción de información por lo que se va a realizar las siguientes evaluaciones:

- Detección de correos infectados (SPAM)
- Test de Open Relay

Detección de correos infectados

Para evaluar si nuestro servidor de correo esta prevenido ante un SPAM o virus se realizó la siguiente prueba con EICAR el cual manda información infectada a nuestra dirección de correo en este caso se utilizó la dirección tecnico3@servihelp.net , el servidor tiene que detectar y eliminar si la información viene infectada.

Esta prueba se realizó desde la dirección http://www.vsantivirus.com/eicar-test.htm (vsantivirus, 2003)

En la figura 9ingresamos la dirección de correo electrónico a la cual se va a mandar la información, también podemos seleccionar 1 o más archivos infectados para poder comprobar la seguridad de nuestro correo

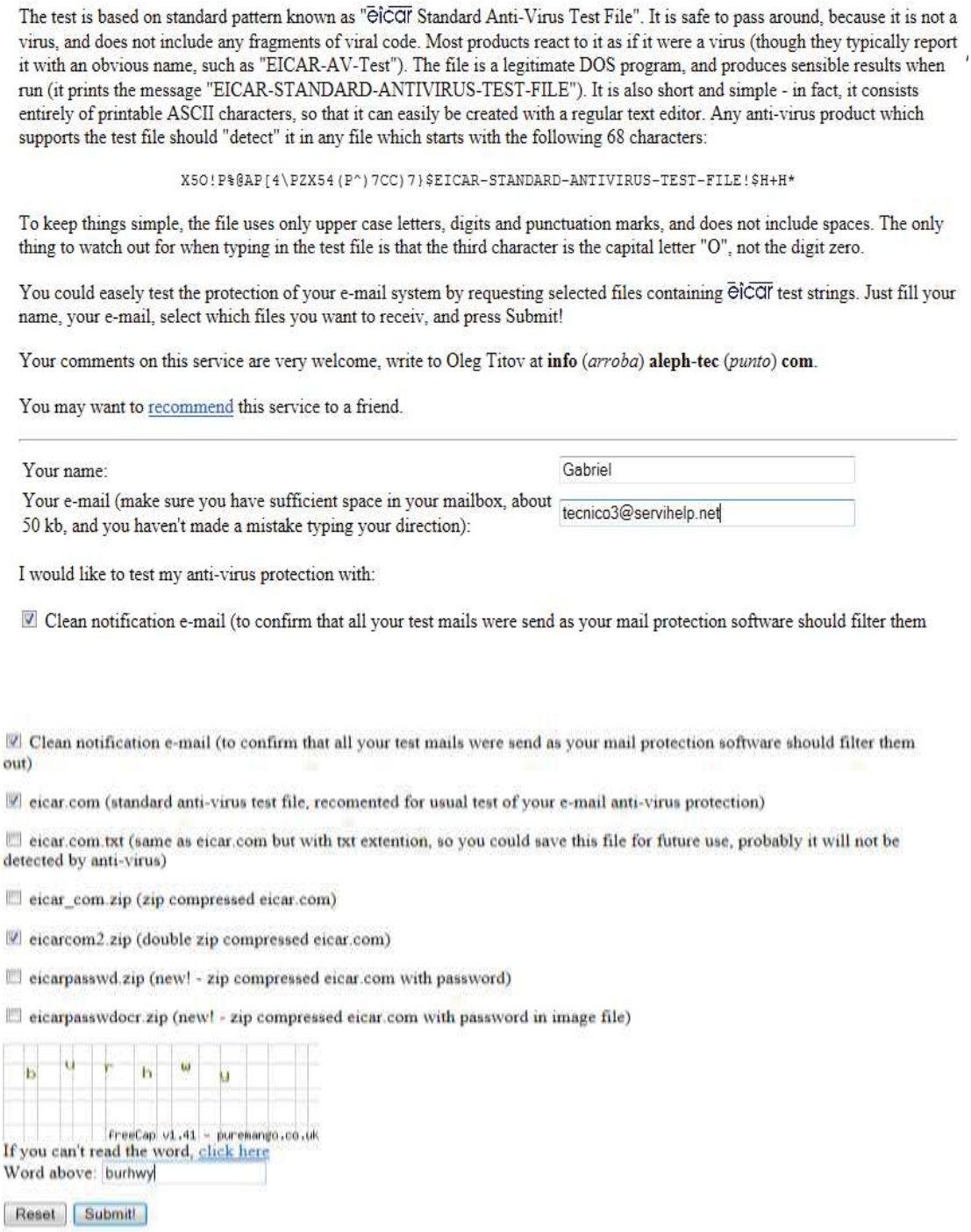


Figura: 9 Pruebas Servidor de correo

Como nos indica la Figura10se puede observar que los archivos fueron enviados correctamente

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

Home > EICAR
Gabriel, we have send to your e-mail address **tecnico3@servihelp.net** following files:

Array ([name] => Gabriel [email] => tecnico3@servihelp.net [eicar] => Array ([0] => clean [1] => eicar.com [4] => eicarcom2.zip) [word] => burhwy [action] => Submit!)

1. Sending clean... 1 OK!
2. Sending eicar.com... 1 OK!
3. Sending eicarcom2.zip... 1 OK!

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

Figura: 10 Pruebas Servidor de correo

En la figura 10 nos indica que está correo infectado, enviado desde la página de EICAR al servidor de correo lo reconoció como correo infectado y procedió a bloquearlo.

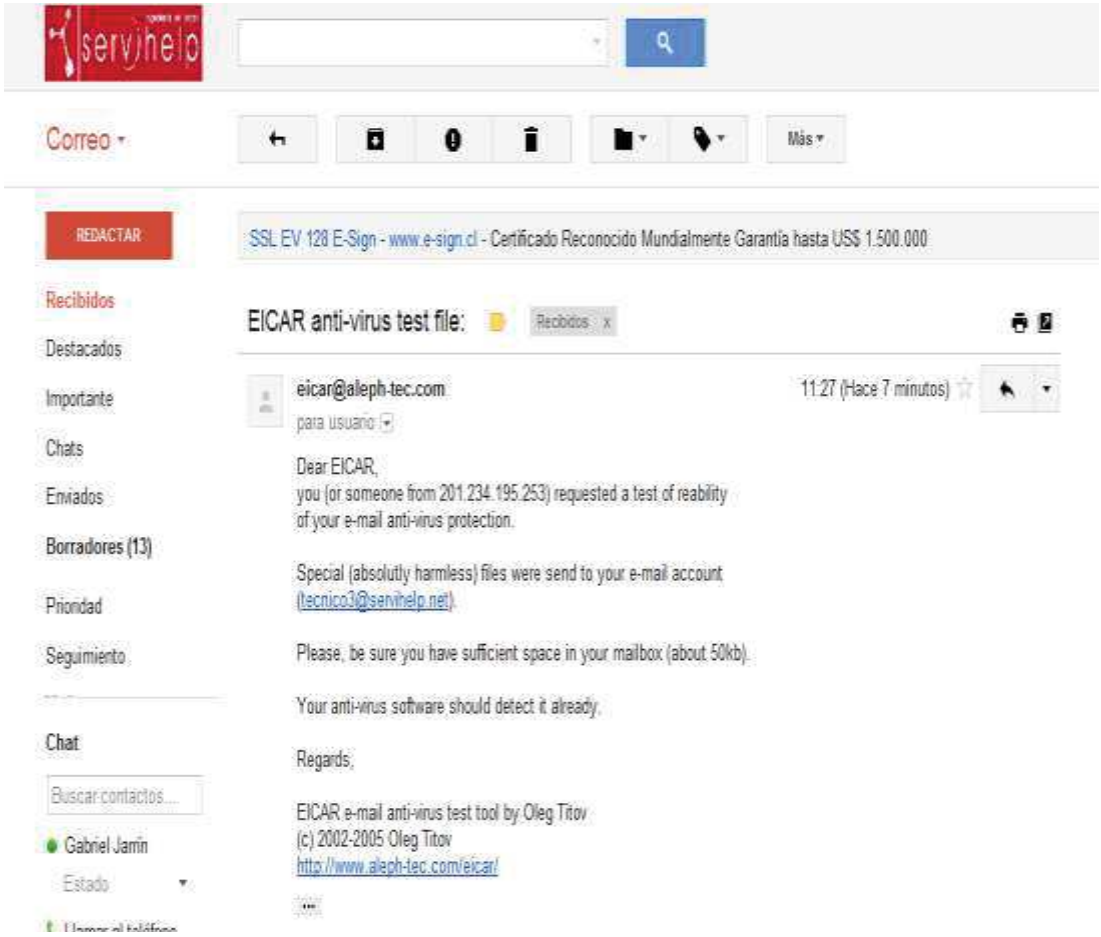


Figura: 11 Pruebas Servidor de correo

Open Relay Test

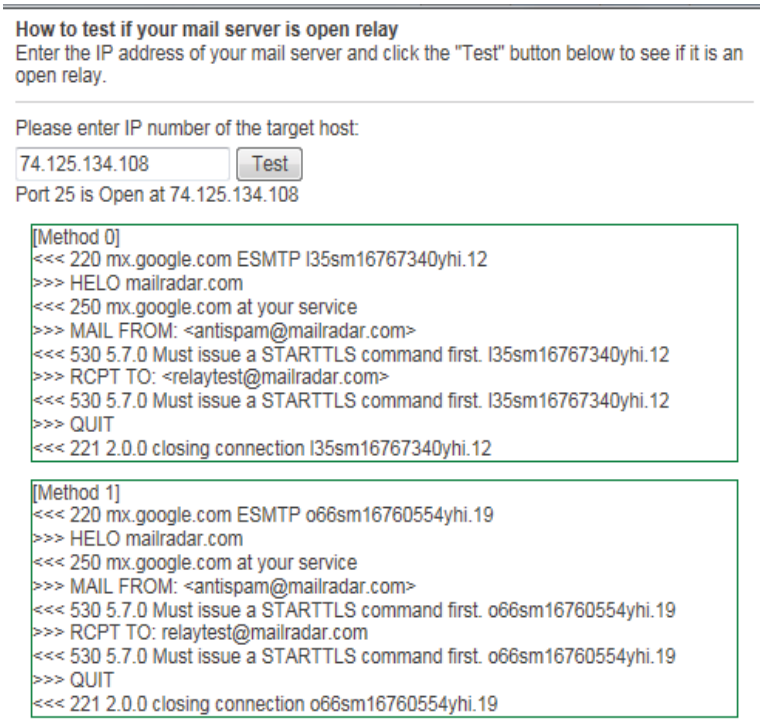
Es un servidor que se utiliza para realizar ataques de correo el cual no verifica la retrasmisión estos servidores utilizan el mecanismo MTA (Agente de transporte de correo).

Para realizar esta prueba la vamos a realizar con la dirección IP Publica donde tenemos alojado nuestro dominio que en este caso sería:

IP Pública 74.125.134.108

Ahora procedemos a ingresar la IP en la página web que vamos a utilizar para realizar esta pruebahttp://www.mailradar.com/openrelay/ (MailRadar, 2007)

En la figura 12 ingresamos la IP pública con la cual trabaja el servidor de correo



```
[Method 2]
<<< 220 mx.google.com ESMTP z11sm15132443anj.13
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam>
<<< 530 5.7.0 Must issue a STARTTLS command first. z11sm15132443anj.13
>>> RCPT TO: <relaytest@mailradar.com>
<<< 530 5.7.0 Must issue a STARTTLS command first. z11sm15132443anj.13
>>> QUIT
<<< 221 2.0.0 closing connection z11sm15132443anj.13
```

```
[Method 3]
<<< 220 mx.google.com ESMTP g6sm15144895ani.5
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <>
<<< 530 5.7.0 Must issue a STARTTLS command first. g6sm15144895ani.5
>>> RCPT TO: <relaytest@mailradar.com>
<<< 530 5.7.0 Must issue a STARTTLS command first. g6sm15144895ani.5
>>> QUIT
<<< 221 2.0.0 closing connection g6sm15144895ani.5
```

```
[Method 4]
<<< 220 mx.google.com ESMTP s21sm16775404yhb.5
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. s21sm16775404yhb.5
>>> RCPT TO: <relaytest@mailradar.com>
<<< 530 5.7.0 Must issue a STARTTLS command first. s21sm16775404yhb.5
>>> QUIT
<<< 221 2.0.0 closing connection s21sm16775404yhb.5
```

```
[Method 5]
<<< 220 mx.google.com ESMTP s21sm16775602yhb.5
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. s21sm16775602yhb.5
>>> RCPT TO: <relaytest%mailradar.com@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. s21sm16775602yhb.5
>>> QUIT
<<< 221 2.0.0 closing connection s21sm16775602yhb.5
```

```
[Method 6]
<<< 220 mx.google.com ESMTP u11sm15137049ane.11
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. u11sm15137049ane.11
>>> RCPT TO: <relaytest%mailradar.com.com@[gg-in-f108.1e100.net]>
<<< 530 5.7.0 Must issue a STARTTLS command first. u11sm15137049ane.11
>>> QUIT
<<< 221 2.0.0 closing connection u11sm15137049ane.11
```

```
[Method 7]
<<< 220 mx.google.com ESMTP z11sm15132759anj.13
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. z11sm15132759anj.13
>>> RCPT TO: <"relaytest@mailradar.com">
<<< 530 5.7.0 Must issue a STARTTLS command first. z11sm15132759anj.13
>>> QUIT
<<< 221 2.0.0 closing connection z11sm15132759anj.13
```

```
[Method 8]
<<< 220 mx.google.com ESMTP m51sm16765059yhh.16
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. m51sm16765059yhh.16
>>> RCPT TO: <"relaytest%mailradar.com">
<<< 530 5.7.0 Must issue a STARTTLS command first. m51sm16765059yhh.16
>>> QUIT
<<< 221 2.0.0 closing connection m51sm16765059yhh.16
```

```
[Method 9]
<<< 220 mx.google.com ESMTP e24sm16775284yhh.4
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. e24sm16775284yhh.4
>>> RCPT TO: <relaytest@mailradar.com@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. e24sm16775284yhh.4
>>> QUIT
<<< 221 2.0.0 closing connection e24sm16775284yhh.4
```

```
[Method 10]
<<< 220 mx.google.com ESMTP s1sm15144729anj.1
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. s1sm15144729anj.1
>>> RCPT TO: <"relaytest@mailradar.com"@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. s1sm15144729anj.1
>>> QUIT
<<< 221 2.0.0 closing connection s1sm15144729anj.1
```

```
[Method 11]
<<< 220 mx.google.com ESMTP e18sm16779890yhi.0
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. e18sm16779890yhi.0
>>> RCPT TO: <relaytest@mailradar.com@gg-in-f108.1e100.net>
<<< 530 5.7.0 Must issue a STARTTLS command first. e18sm16779890yhi.0
>>> QUIT
<<< 221 2.0.0 closing connection e18sm16779890yhi.0
```

```
[Method 12]
<<< 220 mx.google.com ESMTP z28sm16773576yhh.7
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. z28sm16773576yhh.7
>>> RCPT TO: <@[74.125.134.108]:relaytest@mailradar.com>
<<< 530 5.7.0 Must issue a STARTTLS command first. z28sm16773576yhh.7
>>> QUIT
<<< 221 2.0.0 closing connection z28sm16773576yhh.7
```

```
[Method 13]
<<< 220 mx.google.com ESMTP o66sm16761361yhi.19
>>> HELO mailradar.com
<<< 250 mx.google.com at your service
>>> MAIL FROM: <antispam@[74.125.134.108]>
<<< 530 5.7.0 Must issue a STARTTLS command first. o66sm16761361yhi.19
>>> RCPT TO: <@[gg-in-f108.1e100.net]:relaytest@mailradar.com>
<<< 530 5.7.0 Must issue a STARTTLS command first. o66sm16761361yhi.19
>>> QUIT
<<< 221 2.0.0 closing connection o66sm16761361yhi.19
```

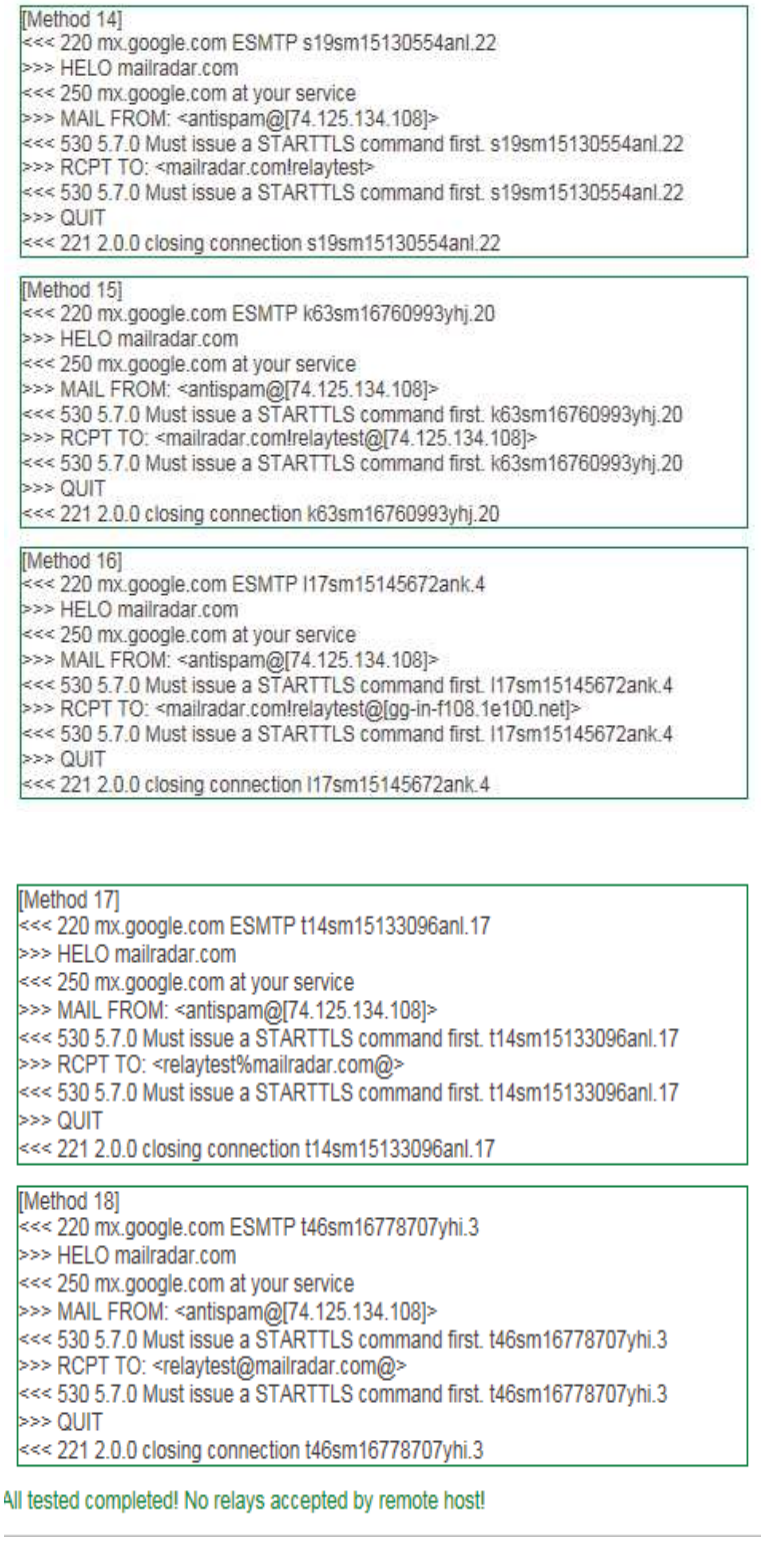


Figura: 12 Pruebas Open Replay

En la figura 12nos indica que se ha completado el test y que el servidor no acepto ralays.

3.3 Evaluación Listas Negras

Para poder realizar una evaluación de listas negras hemos utilizado 2 sitios web los mismo que brindan como servicio la verificación si nuestro servidor de correo se encuentra en listas negras.

Sitio web más utilizados:

- http://whatismyipaddress.com/blacklist-check
- http://mxtoolbox.com/blacklists.aspx

Para poder realizar la verificación si nuestra IP pública con la cual estamos saliendo hacia el internet se encuentra en listas negras tenemos que saber qué dirección estamos utilizando. En el caso de no saber la IP pública tenemos sitios web los cuales nos ayudan con esta información como:

- http://whatismyipaddress.com
- http://network-tools.com

En estos sitios Web encontramos la IP que estamos utilizando para la salida al internet, después de realizar la verificación procedemos a ingresar al sitio web que nos ayudara a realizar la verificación si nos encontramos en listas negras.

A continuación se procederá a realizar la verificación de listas negras en los sitios web mencionados.

Primera Prueba

Para esta prueba procederemos a utilizar el siguiente sitio web:

- http://whatismyipaddress.com

Para poder realizar esta prueba vamos a ingresar la IP pública que estamos utilizando en nuestro servidor

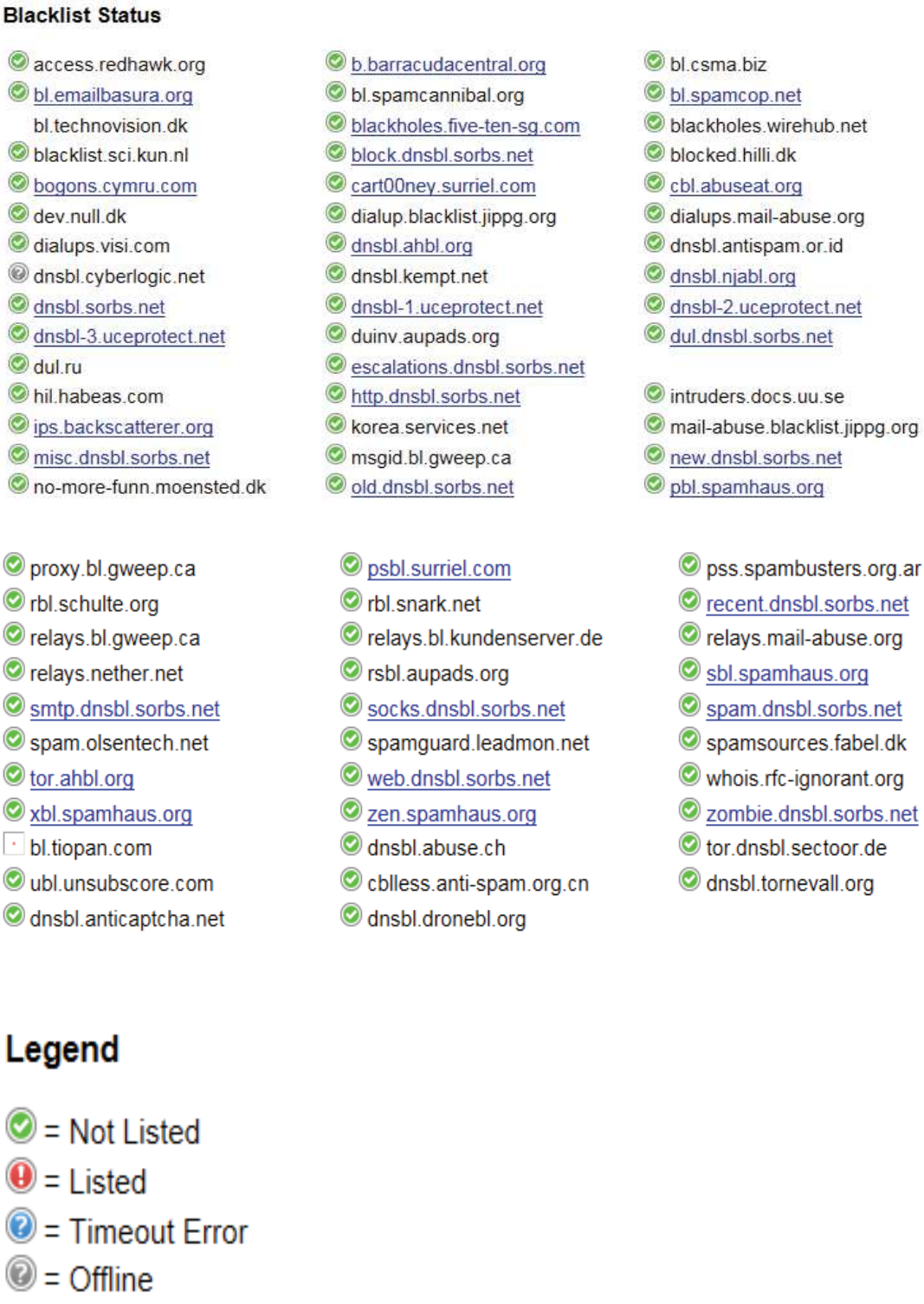


Figura: 13 Pruebas Listas Negras

En la figura 13 nos indica de acuerdo al test que se realizamos que IP Publica que utiliza el servidor se encuentra fuera de Listas negras.

Segunda prueba

Para esta prueba procederemos a utilizar el siguiente sitio web:

- http://mxtoolbox.com/blacklists.aspx

En el segundo test que realizamos podemos verificar que tampoco la IP Publica que utiliza el servidor se encuentra en Listas negras.

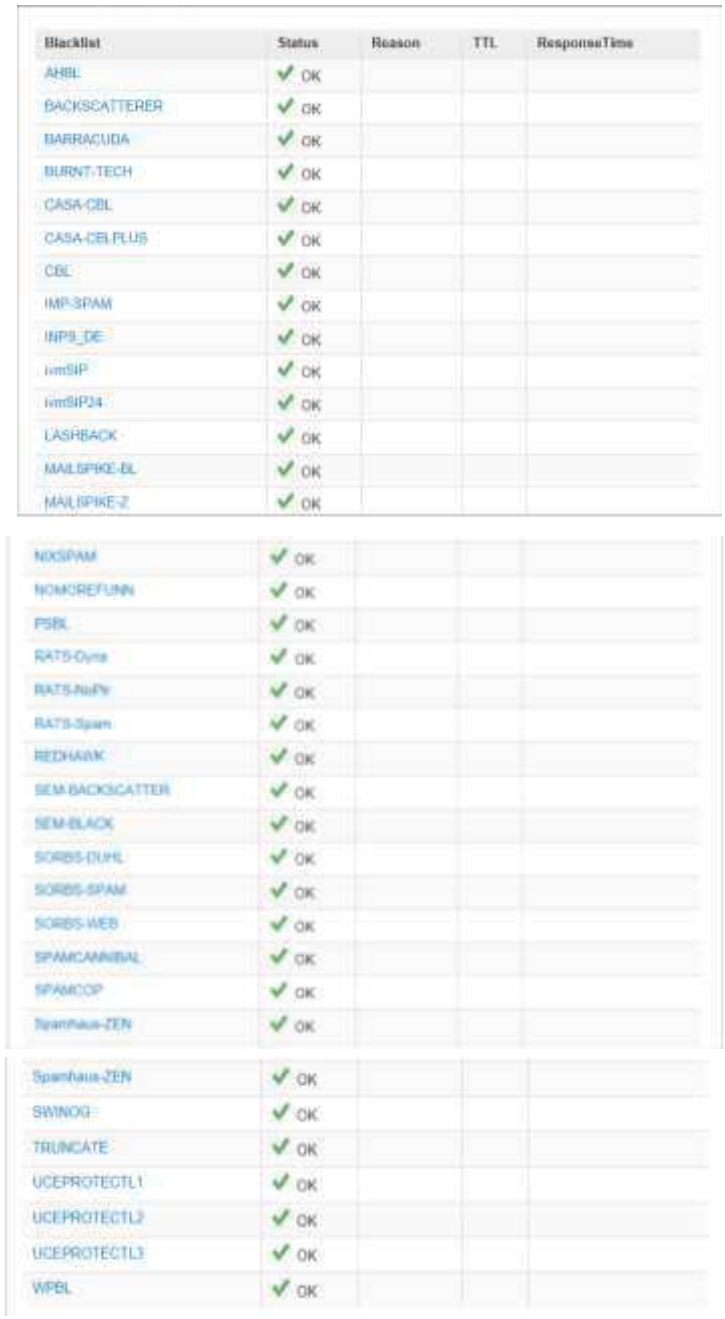


Figura: 14 Pruebas Listas Negras

3.4 Evaluación del servidor proxy

En esta evaluación vamos a comprobar si las reglas y políticas establecidas en el servidor proxy se encuentran funcionando correctamente.

En la empresa SERVIHELP S.A se encuentran bloqueados sitios para ocio del personal, A continuación vamos a ingresar a algunos sitios para verificar su funcionamiento.

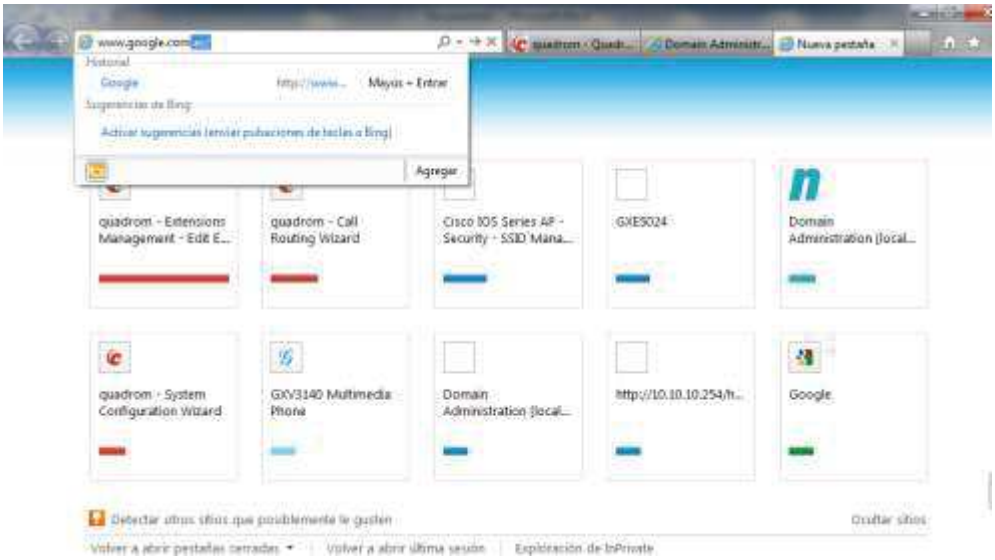


Figura: 15 Ingreso a sitio web Google

En la figura 16 se verifica que se puede ingresar al sitio www.google.com

Figura: 16 Ingreso al sitio web Google

La siguiente prueba será ingresando a un sitio web de ocio en este caso www.facebook.com

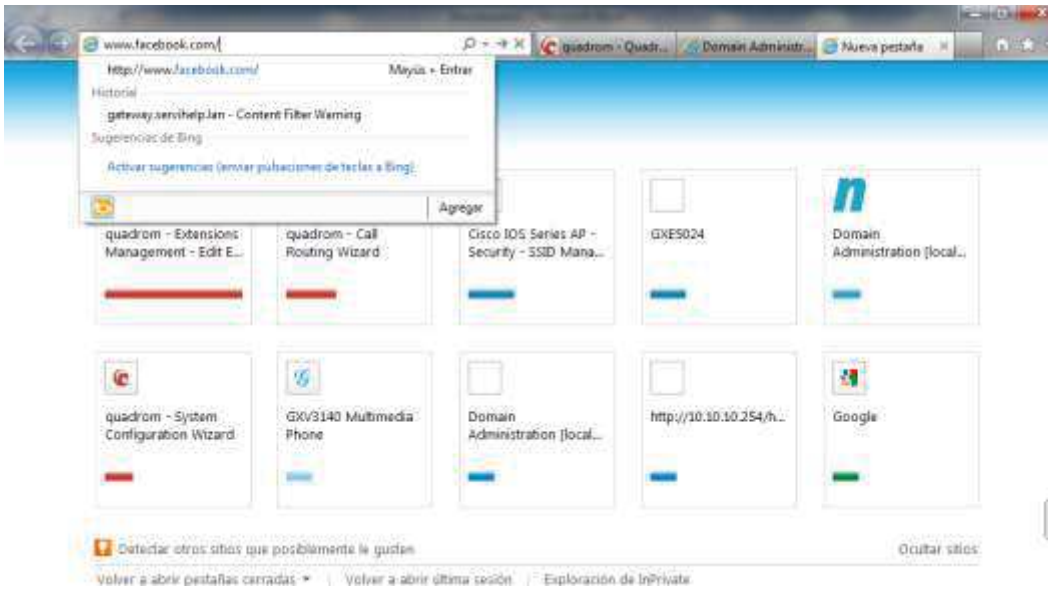


Figura: 17 Ingreso al sitio web Facebook

En la figura 18 se puede observar que este sitio se encuentra restringido por el servidor proxy y se puede comprobar que se están cumpliendo las reglas y políticas establecidas por políticas de la empresa.

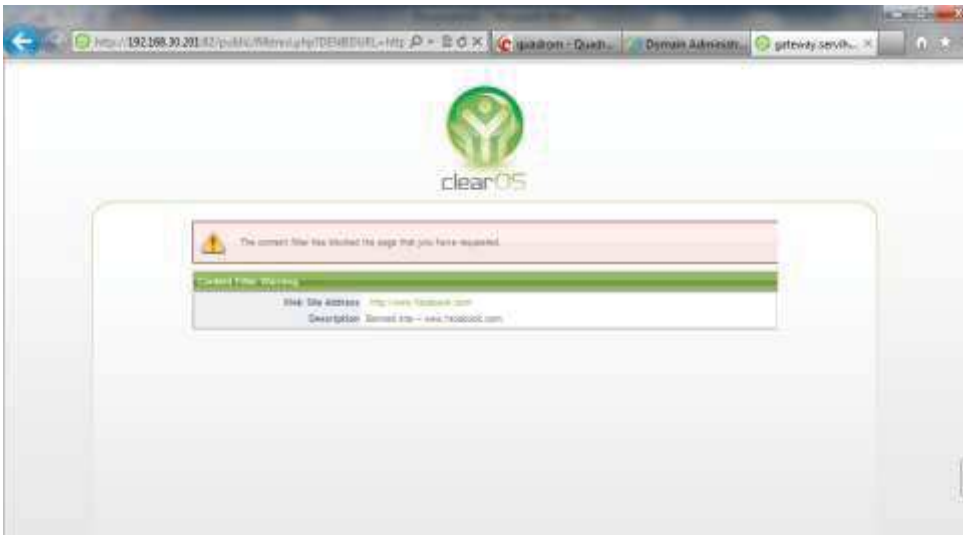


Figura: 18 El ingreso al sitio web Facebook se encuentra bloqueada

También vamos a intentar acceder al sitio web www.hotmail.com

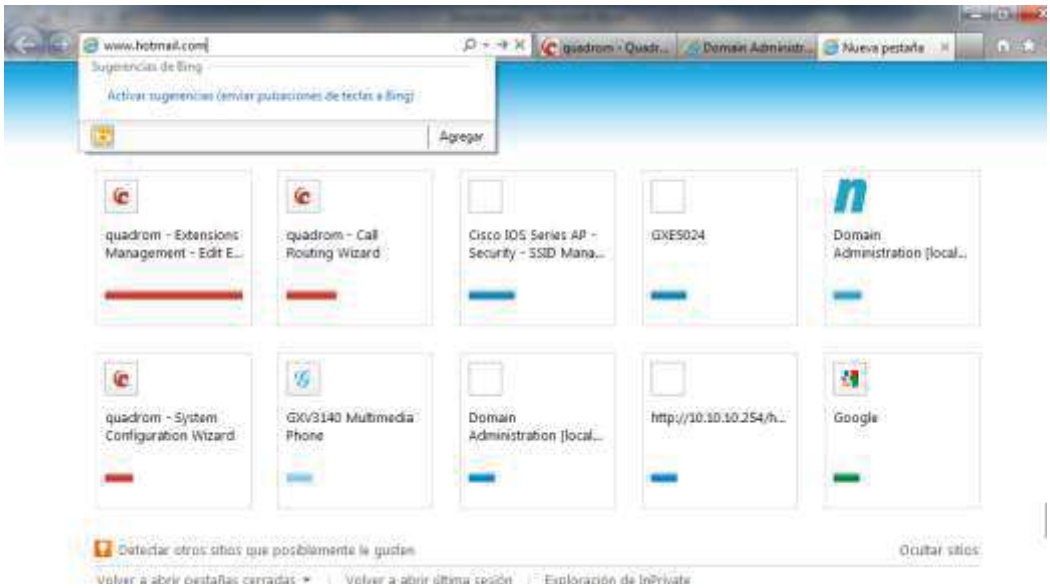


Figura: 19 Ingreso a sitio Hotmail

En la figura 20 se puede observar que este sitio se encuentra bloqueado de acuerdo las reglas y políticas establecidas por el servidor proxy.

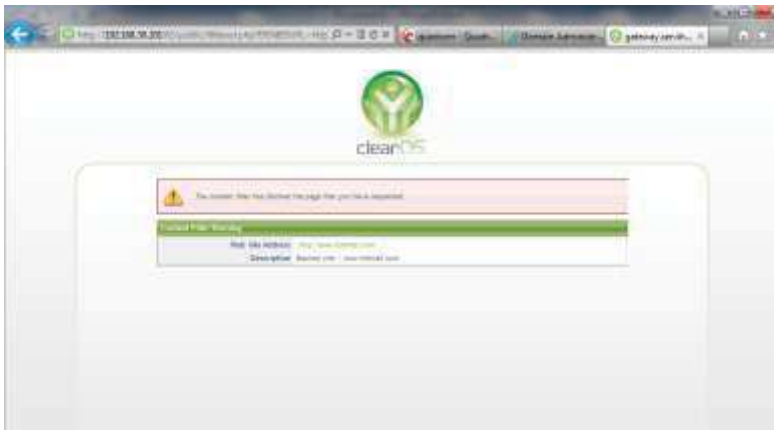


Figura: 20 El ingreso al sitio web se encuentra bloqueado

Existen proxy anónimos que permiten el ingreso a las páginas bloqueadas desde otro servidor que se encuentran alojados en la nube de internet, en esta prueba vamos a verificar si podemos ingresar a los sitios bloqueados desde algún servidor proxy.

Figura: 21 Búsqueda de proxy anonymous

Se puede observar en la figura 22 que el servidor proxy no permite realiza la búsqueda ya que se encuentra habilitada la seguridad en el servidor para no acceder a esos sitios.

Figura: 22 Acceso negado a la búsqueda de proxy anonymous

Se realizó la búsqueda de proxy con diferentes palabras y se encontró varios sitios que dan el servicio de proxy anónimo como se muestra en la figura 23

Figura: 23 Búsqueda proxy anónimos con diferentes palabras

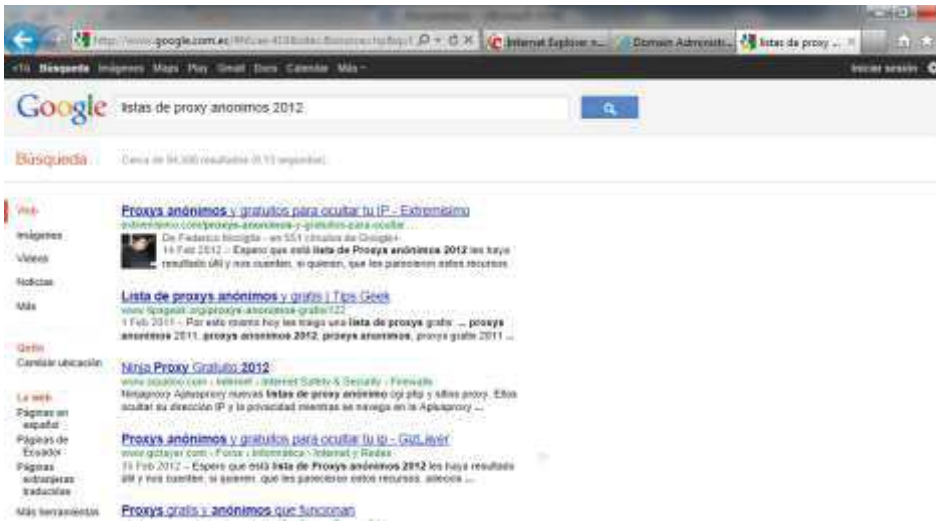


Figura: 24 Resultados de la búsqueda

Se intentó ingresar a los sitios pero el servidor no permite el acceso y los bloquea.

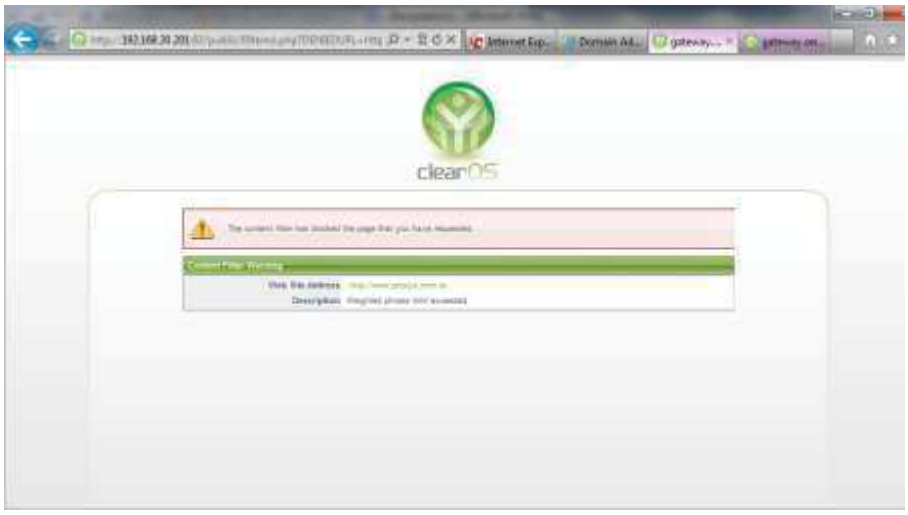


Figura: 25 Intento de ingreso a un sitio proxy y lo bloquea

Se realizó la búsqueda de más sitios para intentar evadir la seguridad del servidor proxy y se puede observar en la figura 26 y 27 que realizo la búsqueda a varios sitios proxy, ahora procederemos intentar acceder a estos sitios.

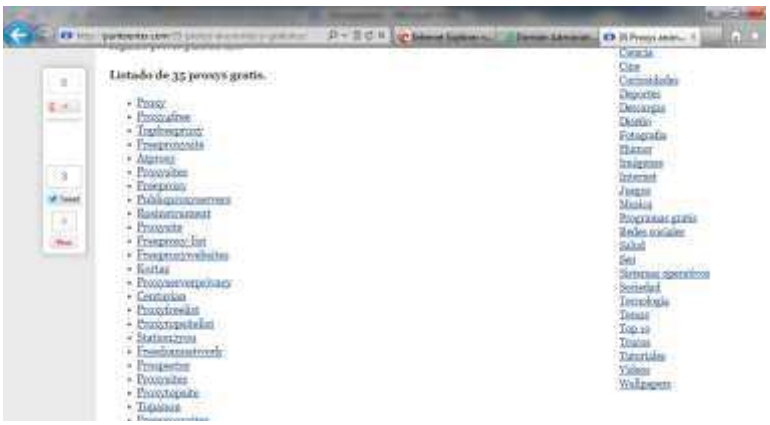


Figura: 26 Lista de sitios proxy

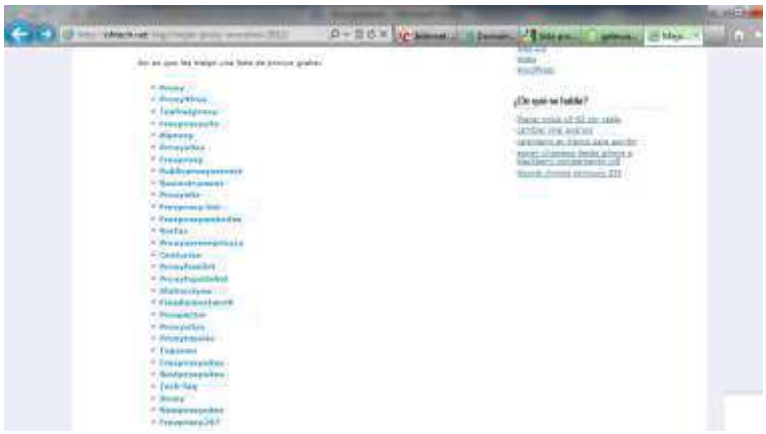


Figura: 27 Lista de sitios proxy

Figura: 28 Bloqueo de intento de acceso a un sitio proxy anonymous

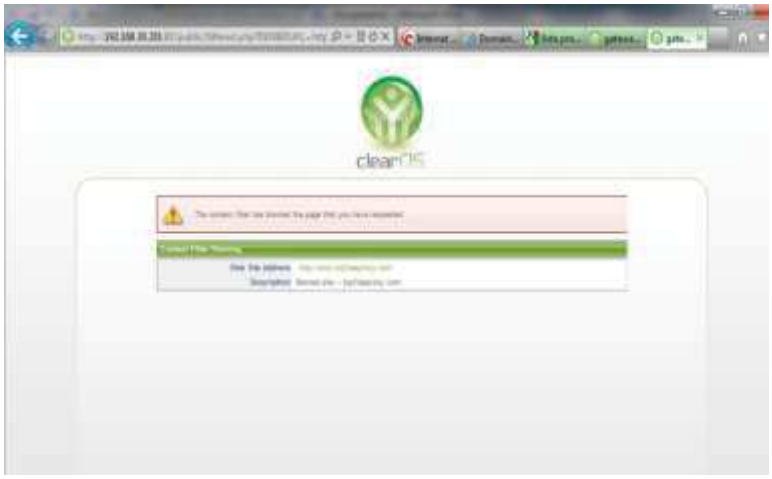


Figura: 29 Bloqueo de intento de acceso a un sitio proxy anonymous

Como se puede observar en las Figuras 28 y 29 no permite acceder a ninguno de estos sitios y se puede comprobar que la seguridad del servidor proxy se encuentra funcionando correctamente ya que en todos los intentos de ingreso hacia un proxy automáticamente nos bloqueó el acceso al sitio.

3.5 Evaluación de Escaneo de Puertos Abiertos

En esta evaluación se realiza un análisis del servidor proxy, el cual nos permite saber que puertos se encuentran abiertos o cerrados.

Se deben tomar en cuenta los puertos abiertos ya que por esos puertos podemos recibir ataques a nuestra red.

Para realizar este análisis de puertos abiertos se utilizó el siguiente sitio web:http://www.t1shopper.com/

En la figura 30 En esta página web automáticamente nos reconoce la IP publica que estamos utilizando en el servidor proxy y aquí escogemos los puertos que queremos verificar si están abiertos.

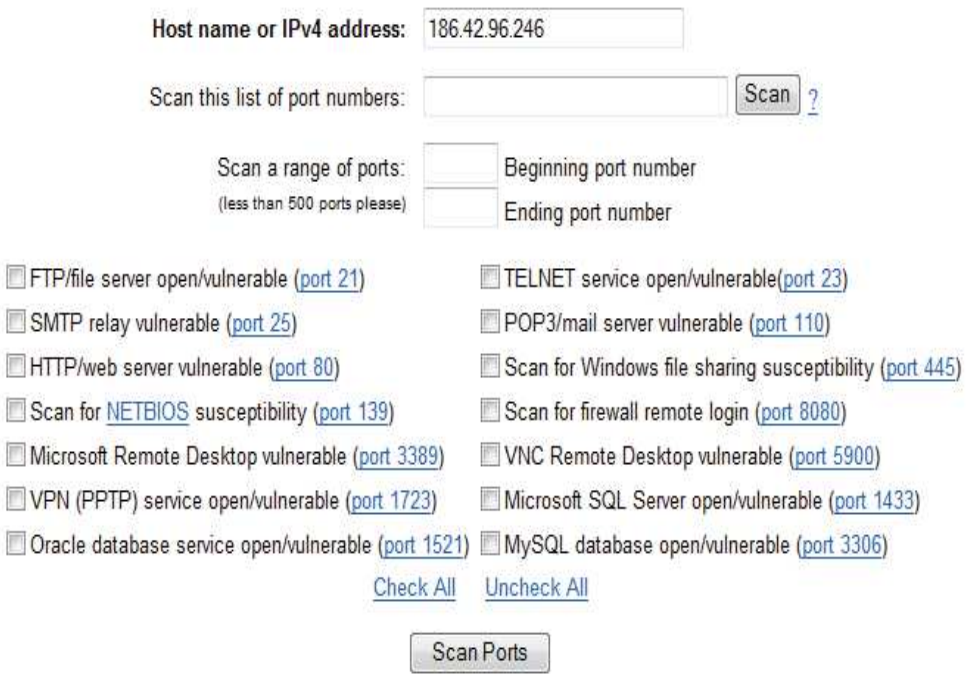


Figura: 30 Selección de puertos a Escanear

En la figura 31 Nos indica que ha encontrado que tenemos abiertos 2 puertos

- Puerto 21 FTP
- Puerto 80 HTTP

Se debe realizar la verificación si es necesario que estos puertos se encuentren abiertos ya que esto puede producir vulnerabilidad a la red de la empresa SERVIHELP S.A.

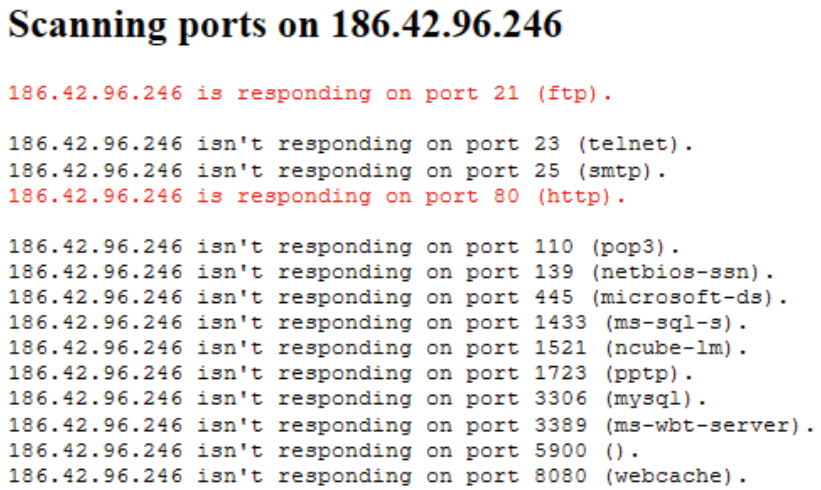


Figura: 31 Resultados de los puertos abiertos en el servidor proxy

3.6 Evaluación de las contraseñas de los equipos activos

Ahora se evaluaran las contraseñas de seguridad de los equipos activos para lo cual se procederá a verificar si los equipos se encuentran sin contraseñas o con contraseñas conocidas como:

- admin
- user
- en blanco

Adicional se va utilizar la siguiente página web http://www.passwordmeter.com/ (The password Meter)en donde se encontrara una aplicación para verificar el porcentaje de seguridad de la contraseña que se están utilizando.

A continuación se procederá a realizar la verificación de la seguridad de los equipos que conforman la red de la empresa SERVIHELP S.A.

Servidor Proxy y Servidor de archivos

Debido a que el servidor proxy y servidor de archivos poseen la misma configuración de seguridad y el mismo sistema operativo se procederá a realizar las siguientes pruebas

Se realizaron pruebas de ingreso en los servidores. Se ingresó un usuario y contraseña con los datos:

- Usuario: admin
- Contraseña: admin, user y en blanco

Figura: 32 Intento de acceso con usuario y contraseñas conocidas

Figura 33 Intento de acceso con usuario y contraseñas conocidas

Se puede verificar en la Figura 32 y 33 que no accede con los datos ingresados esto quiere decir que la seguridad del equipo se encuentra segura. Adicional se realizó una captura con el software Wireshark el cual nos ayuda a capturar todo el tráfico que realizamos, en esta prueba no se obtuvo resultados ya que el servidor está utilizando el protocolo HTTPS el mismo que se utiliza para una conexión segura. Por ende no aparece en las capturas realizadas por el wireshark.

Para revisar qué porcentaje de seguridad cumple la contraseña utilizada vamos a utilizar el siguiente web http://www.passwordmeter.com/ .

En la figura 34 ingresamos la contraseña correspondiente al servidor y procedemos a evaluar su seguridad

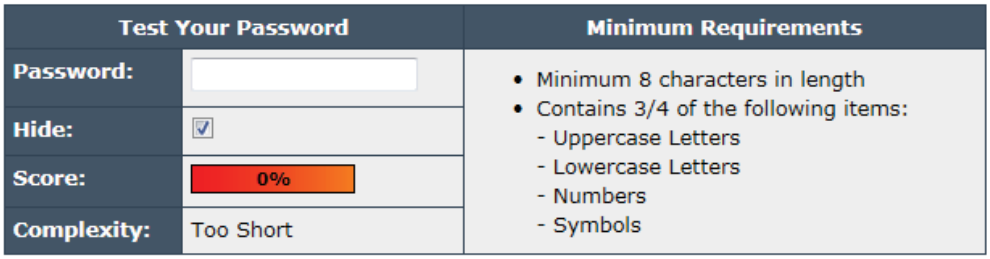


Figura: 34 Evaluación de contraseñas

En la figura 35 se puede verificar el porcentaje con respecto a la seguridad de la contraseña y como resultado nos indica que la contraseña que se utiliza es MUY FUERTE.

Servidor telefonía

Se realizaron pruebas de ingreso en el servidor de telefonía con los siguientes datos:

- Usuario: admin
- Contraseña: admin, user y en blanco

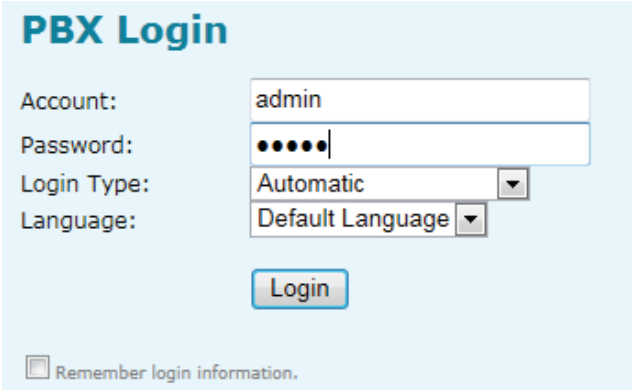


Figura: 35 Evaluación de contraseña de servidor telefonía

Se puede verificar en la figura 35 que no accede con los datos ingresados esto indica que la seguridad del equipo funciona correctamente.

Para saber si la seguridad que posee la contraseña es fuerte realizamos una prueba de ingreso y se realizó una captura con el software Wireshark con el cual se pudo verificar que aparecen los caracteres de la contraseña que están con letras y números y los que se encuentran con símbolos se encuentran cifrados.

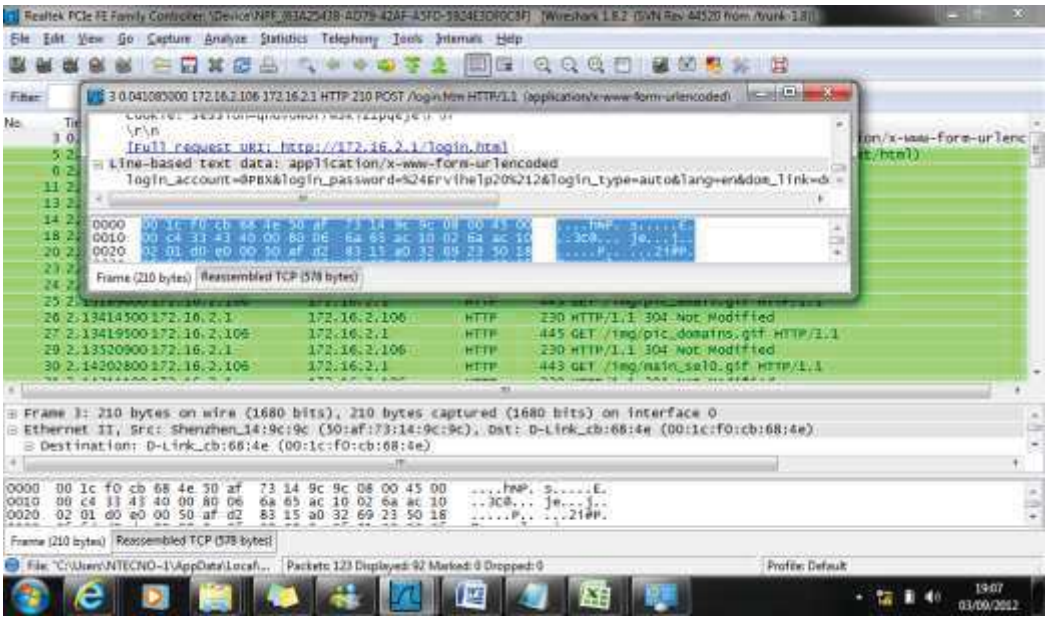


Figura: 36 Captura Wireshark

En esta prueba se verifica que la contraseña es segura para el acceso al equipo.

Adicional se realizó un análisis sobre la contraseña con la cual se encuentra trabajando el servidor, como se puede observar en la figura 37 indica que posee un 100% de porcentaje en su seguridad esto quiero decir que la contraseña es MUY FUERTE.

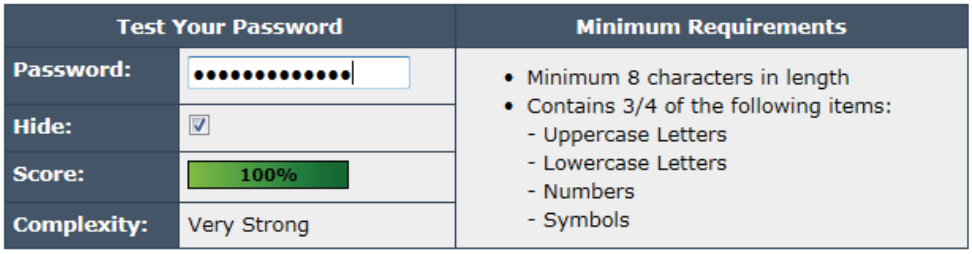


Figura: 37 Análisis de contraseña

Equipos Switch Dlink 1228

Se realizaron pruebas de ingreso de usuario con los siguientes datos

- Usuario: admin
- Contraseña: admin, user y en blanco

Figura: 38 Ingreso a Switch

Figura: 39 Acceso a configuración switch

Esta prueba se realizó en los 3 equipos switch que poseen las mismas características

Como se puede observar en las figuras 38 y 39 se pudo ingresar a las configuraciones de los equipos con las contraseñas que se ingresaron por defecto.

Adicional se realizó una captura con el software wireshark para saber la seguridad de la contraseña que se ingresó y como resultado se pudo verificar en la figura 40 que en la captura realizada se pudo saber cuál es el nombre de usuario y contraseña (admin) que se ingresó, esto quiere decir que la contraseña no es segura ya que no se encuentra cifrada.

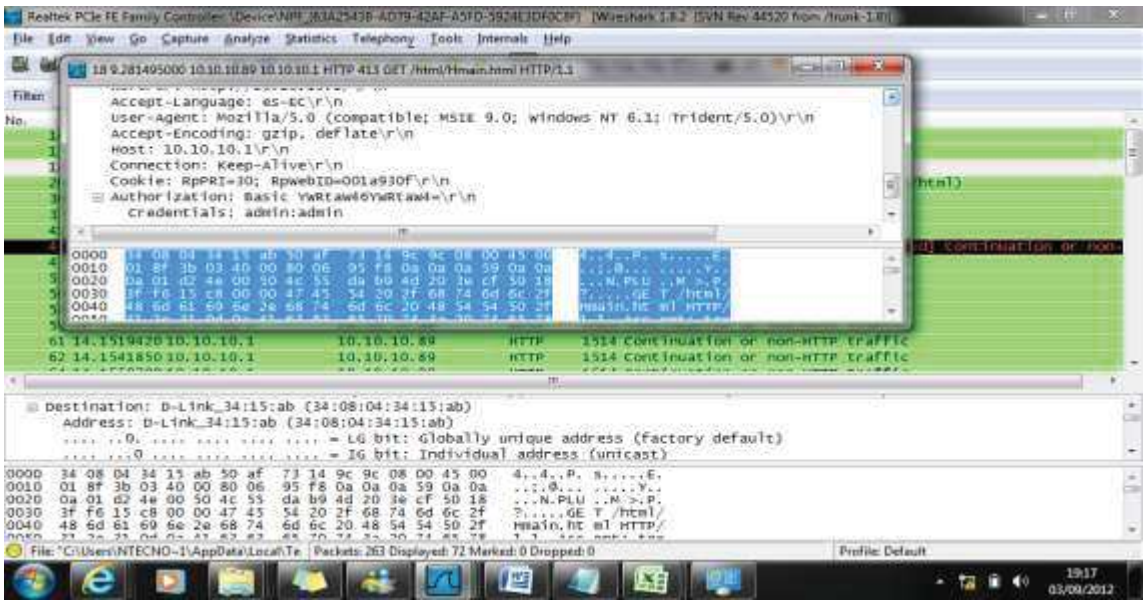


Figura 40 Captura con wireshark Switchs

También se verifico el porcentaje de seguridad para la clave que se ingresó en los equipos switchs.

Como se puede observar en la figura 41 nos indica que la contraseña utilizada es muy débil.

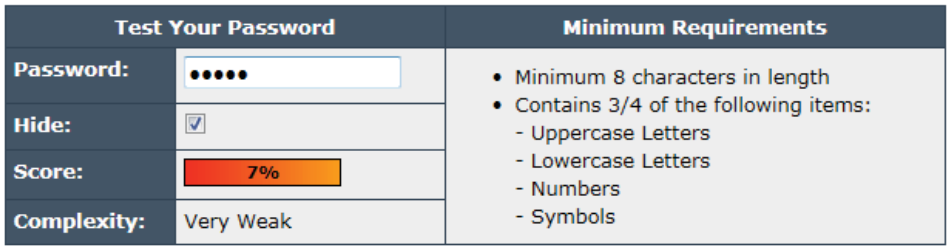


Figura: 41 Análisis de contraseña de los Switchs

En esta figura 41se puede verificar que para obtener una clave segura se debe mezclar y símbolos letras y número ya que así las contraseñas se cifran y son difíciles de descifrar.

4 Capítulo IV Resultados de la auditoria

4.1 Presentación de resultados

Para la presentación de resultados con respecto a la auditoría realizada a la empresa SERVIHELP S.A se realizaron cuadros comparativos en los cuales se verá el resultado final de la auditoría, para ello se recopiló la información de cada prueba ejecutada como también se pudo ocupar como referencia la metodología Checklist para recopilar información..

4.1.1 Sistemas Operativos

En esta evaluación verificamos el porcentaje de los sistemas operativos usados en la empresa el cual se puede observar en la figura 42

Adicional los sistemas que la empresa SERVIHELP no poseen licenciamiento original

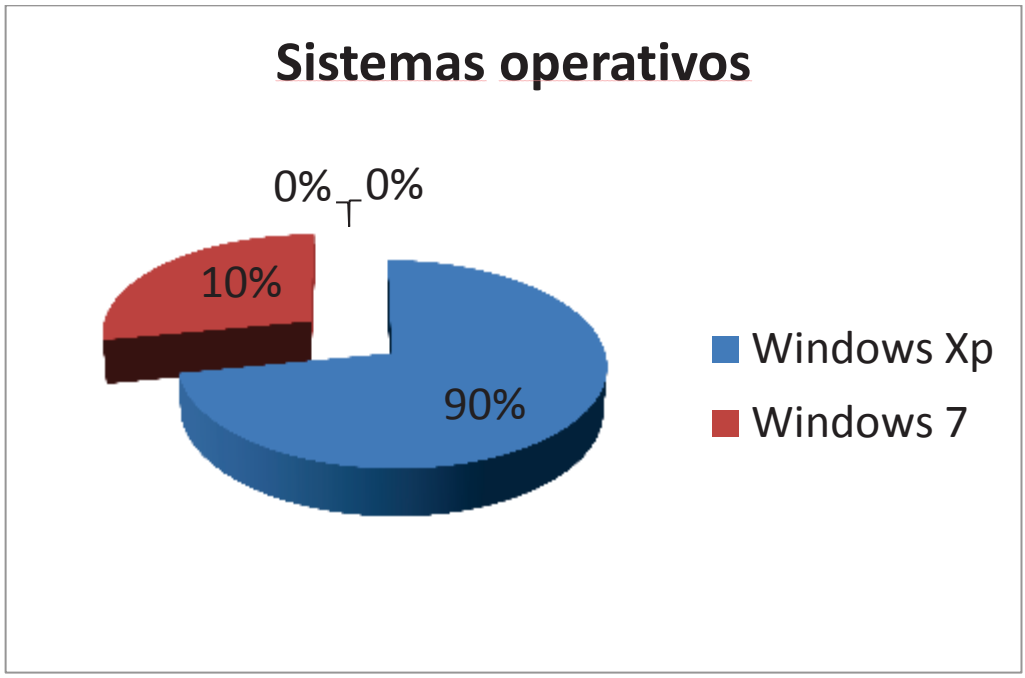


Figura: 42 Porcentaje de sistemas operativos en la Empresa SERVIHELP S.A

4.1.2 **Análisis de contraseñas en los usuarios**

En esta prueba se analizó la seguridad de la contraseña que manejan los usuarios en los ordenadores.

Se analizó las contraseñas de los usuarios creados en los ordenadores:

- Administrador
- Usuarios

Contraseñas	Contraseñas
Administrador	Usuarios
100 % SEGURA	50% SEGURA 50 % INSEGURA

Figura: 43 Análisis de contraseñas de los usuarios

La contraseña de Administrador es generada por el departamento de Nuevas tecnologías por lo tanto es un estándar en la empresa, por otro lado las contraseñas de los usuarios son inseguras ya que son creadas por ellos y por lo general suelen poner en sus contraseñas los nombres de las personas que ocupan los ordenadores y así se vuelven vulnerables.

4.1.3 **Análisis Antivirus**

La empresa utiliza el antivirus Avast el cual se encuentra instalado en un 100% en todos los ordenadores. Su licencia se encuentra con una vigencia de 6 años.

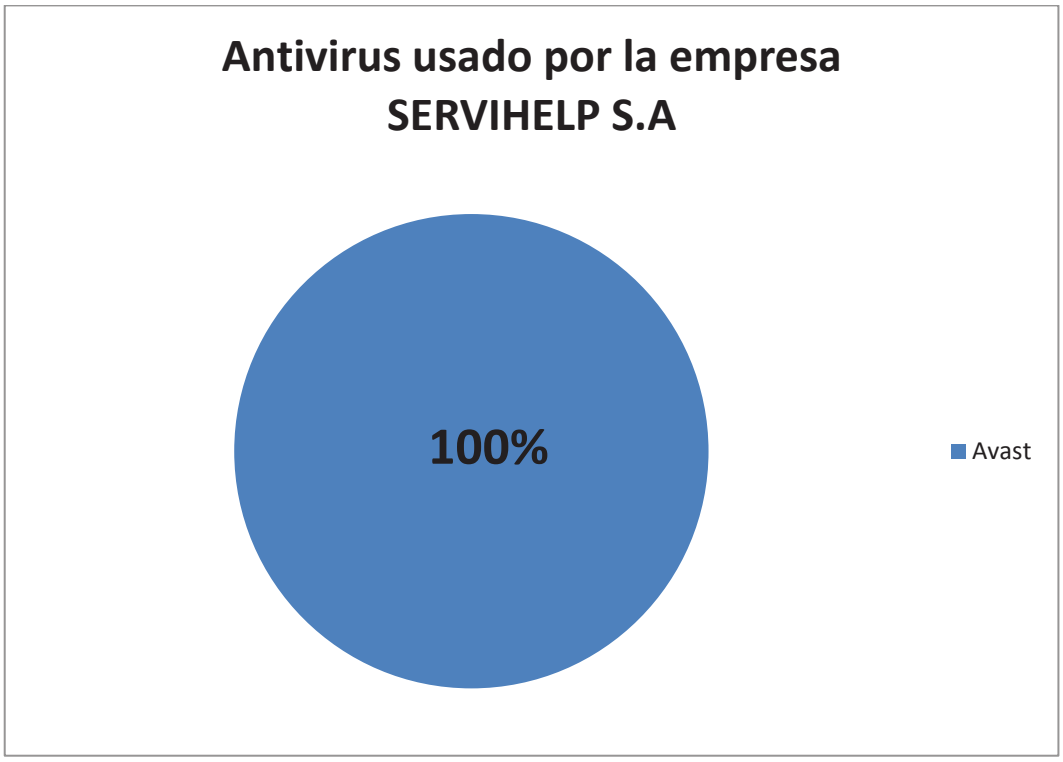


Figura: 44 Porcentaje de uso de antivirus

4.1.4 Contraseñas de equipos y dispositivos

Las contraseñas que se utilizan en los equipos y dispositivos que posee la empresa SERVIHELP se procederá a clasificar según las evaluaciones realizadas anteriormente en:

- Robustas
- Vulnerables

Tabla 5. Análisis de contraseñas en los usuarios.

	CONTRASEÑAS	
EQUIPOS Y DISPOSITIVOS	**ROBUSTAS**	**VULNERABLES**
Computadoras	50%	50%
Switch	0%	100%
Servidores	90%	10%

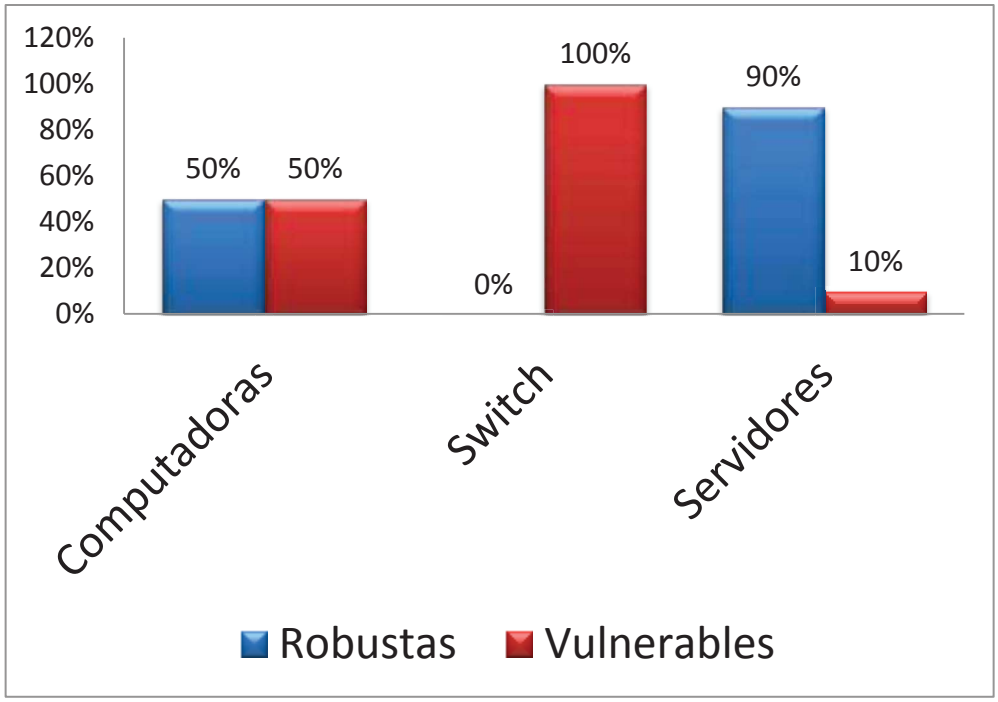


Figura: 45 Porcentaje de seguridad en contraseñas

4.1.5 **Checklist de la Empresa SERVIHELP S.A**

Tablas 6. Sobre riesgo en la eficacia del servicio informático.

Controles	SI	NO	N/A
Existen planes a largo plazo para el departamento de informática	*		
Existen políticas para la planificación, control de 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.		*	
El D.I está separado orgánicamente en la estructura orgánica de la empresa.		*	

Es independientemente la ubicación de D.I de los otros departamentos de la empresa.	*		
Evalué la independencia de las funciones del personal entre las diferentes unidades.	*		
¿Existe una descripción por escrito (Manual de operaciones y procedimientos) de cada puesto en las diferentes unidades de D.I?		*	
Evalué la capacidad de los computadores disponibles para satisfacer la demanda en época alta	*		
Existe en calendario mantenimiento preventivo a los computadores		*	
¿Se verifica que dicho calendario no incluya revisiones en periodos de carga alta de trabajo?		*	
¿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?	*		
¿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?	*		
¿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 datos sensibles?	*		
¿Existe algún mecanismo de control que asegure una adecuada carga de la red especialmente en los periodos de trabajo crítico?		*	

Poseen todos los usuarios de la red especificaciones sobre disponibilidades, horarios, tiempo de respuesta, almacenamiento, respaldo y control operativo		*	
¿Existen planes de formación para los usuarios de la red?		*	
¿Existen responsables que evalúen el correcto uso de la red por parte de los usuarios?		*	
Están perfectamente identificados todos los elementos físicos de la red (unidades de control, módems, cables etc.)		*	
¿Está asegurado en un tiempo prudencial la reparación o cambio de elementos físicos de la red?	*		
¿Se realiza por parte del 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 ha desarrollado o adquirido procedimientos automáticos para resolver o evitar cierres de sistemas en la red?		*	
Existen mecanismos que controlen los tiempos de respuesta de la red y la depuración de los fallos de operación de la misma		*	
¿Existe una rutina que se asegure que ningún proceso o dato de baja prioridad va a estar sin procesar en la red?	*		
¿Se controlan regularmente todos los procesadores de la red?		*	
¿Los sistemas Operativos que utilizan los computadores de usuarios son licenciados?		*	
¿Existe seguridad para el ingreso de utilización de los computadores?		*	

5 Conclusiones y Recomendaciones

5.1 Conclusiones

- La Empresa SERVIHELP S.A que trabaja en el ámbito de telecomunicaciones se pudo verificar que cuentan con equipos aptos para establecer una buena infraestructura como también una buena seguridad en la red.
- El problema que poseen es que no están utilizando los equipos activos al 100% como separar las redes de telefonía y datos en segmentos de Vlan para obtener una red con calidad
- También se debe implementar licencias originales en sistemas operativos e antivirus ya que al no poseerlas genera inconvenientes en el funcionamiento de los mismos.
- Se pudo verificar que la IP Publica asignada a la empresa SERVIHELP no consta en listas negras esto quiere decir que el correo no está enviando SPAM.
- Adicional existen equipos que no poseen buena seguridad para su autenticación el cual afecta que sea vulnerable al ingreso a la administración del equipo y se puedan efectuar cambios que provoquen errores en la red.
- Se pudo comprobar que para el ingreso a los servidores de archivos, proxy y telefonía cuentan con buena seguridad de acceso.
- Con respecto al antivirus que se encuentra utilizando se pudo observar que está respondiendo a las amenazas e infecciones pero se recomienda utilizar un antivirus pagado ya que posee más beneficios y seguridades para la empresa.
- Se comprobó que el servidor proxy se encuentra funcionando correctamente ya que las políticas y reglas establecidas por la empresa están activas dejando una buena seguridad para la restricción de ingreso de sitios web.
- En el Checklist realizado se pudo determinar que en la empresa SERVIHELP S.A no existe procesos a seguir en los departamentos,

como también no existe una capacitación sobre procedimientos y operaciones en el departamento informático hacia los usuarios.

5.2 Recomendaciones

- La empresa SERVIHELP S.A cuenta con equipos óptimos para tener una buena infraestructura, como también SERVIHELP S.A trabaja en el área de telecomunicaciones lo cual para la empresa es más fácil adquirir e implementar software original el mismo que dará más beneficios y mayor seguridad con respecto a la seguridad informática.

- Se recomienda reforzar la seguridad en las contraseñas de los equipos y dispositivos utilizando combinaciones de números letras y símbolos para obtener una contraseña robusta.

- La información que maneja la empresa SERVIHELP S.A es de suma importancia la misma que se debe realizar un respaldo del servidor de archivos así en el caso de sufrir algún daño tener la información respaldada.

- Se recomienda realizar una mantenimiento preventivo mensual a los computadores con esto se reforzara la seguridad y rendimiento a la información de la empresa SERVIHELP S.A.

- Es importante realizar una capacitación a los usuarios del correcto funcionamiento de la red en cada departamento de la empresa como también realizar manuales con procedimientos a seguir con el fin de mantener un correcto manejo de la información.

- Como recomendación para mejorar el tráfico en la red se puede realizar la implementación de Redes Virtuales (VLAN) para esto se realizó la siguiente implementación a realizar en los equipos switch para mejorar el tráfico en segmentos en la red de SERVIHELP S.A

Implementación Redes Virtuales (Vlan)

El propósito de implementar Vlan ayudara a separar el tráfico de la red de datos y telefonía como también la organización de ingreso de servicios de proveedores.

Para esto vamos a utilizar los equipos Switch Dlink 1228 para poder realizar la implementación.

Se necesita la creación de las siguientes VLAN:

- VLAN 10: TELEFONIA
- VLAN 20: RED_DATOS
- VLAN 30: IP_PUBLICAS

Para la distribución de las Vlan de telefonía y datos tenemos 2 modos que nos permiten realizar este servicio.

- Modo Tagged: En este modo necesitaremos un equipo físico el mismo que soporte Vlan (Protocolo 802.1q).
- Modo Access: Para este modo solo enviaremos la información ya que no es necesario un equipo físico que soporte Vlan.

VLAN 10

Por medio de esta VLAN va a trabajar el tráfico de TELEFONIA para esto vamos a realizar la configuración de la vlan en cada uno de los teléfonos IP de SERVIHELP.

VLAN 20

Por medio de esta VLAN va a trabajar el tráfico de internet y datos.

VLAN 30

En esta VLAN se encuentran la IP Publicas que entrega en proveedor de internet con lo cual cuenta la empresa.

EQUIPOS SWITCHS ACTIVOS

SWITCH DE CORE

- MODELO: DLINK 1228 P
- NAME: CORE

SWITCH PRIMARIO

- MODELO: DLINK 1228 P
- NAME: PRIMARIO

SWITCH SECUNDARIO

- MODELO: DLINK 1228 P
- NAME: SECUNDARIO

ASIGNACION DE PUERTOS Y CONFIGURACION

SWITCH DE CORE 1228P

- VLAN 10: TELEFONIA
- VLAN 20: RED_DATOS
- VLAN 30: IP_PUBLICAS

Tabla 7. Asignación de puertos y configuración.

PUERTO	DESCRIPCION	VLAN	MODO PUERTO
27	UPLINK 1228P PRIMARIO	10,20	TAGGED
28	UPLINK 1228 P SECUNDARIO	10,20	TAGGED
24	WAN SERVIDOR INTERNET	30	UNTAGGED
23	LAN SERVIDOR DATOS	20	UNTAGGED

22	LAN SERVIDOR TELEFONIA	10	UNTAGGED
21	WAN GATEWAY TELEFONIA	10	UNTAGGED
20	LAN SERVIDOR INTERNET	20	UNTAGGED
19	ADMINISTRACION PBX	20	UNTAGGED
18	ADMINISTRACION PBX	20	UNTAGGED
17	MODEN TV-CABLE IP PUBLICAS	30	UNTAGGED
16	IP PÚBLICAS	30	UNTAGGED
15	IP PÚBLICAS	30	UNTAGGED
14	IP PÚBLICAS	30	UNTAGGED
1 AL 13	RED TELEFONIA Y RED DATOS	10,20	VLAN 10 TAGGED VLAN 20 UNTAGGED

SWITCH PRIMARIO 1228P

- VLAN 10: TELEFONIA
- VLAN 20: RED_DATOS

Tabla 8. Asignación de puertos y configuración.

PUERTO	DESCRIPCION	VLAN	MODO PUERTO
27	UPLINK 1228P CORE	10,20	TAGGED
28	ADMINISTRACION SWITCH	1	UNTAGGED
1 AL 24	RED TELEFONIA Y RED DATOS	10,20	VLAN 10 TAGGED VLAN 20 UNTAGGED

SWITCH SECUNDARIO 1228P

- VLAN 10: TELEFONIA

- VLAN 20: RED_DATOS

Tabla 9. Asignación de puertos y configuración.

PUERTO	DESCRIPCION	VLAN	MODO PUERTO
27	UPLINK 1228P CORE	10,20	TAGGED
28	ADMINISTRACION SWITCH	1	UNTAGGED
1 AL 24	RED TELEFONIA Y RED DATOS	10,20	VLAN 10 TAGGED VLAN 20 UNTAGGED

6 Referencias

Electrisistemas del Caribe. (s.f.). Recuperado el 2013, de https://sitegoogle.com/site/electrisistemasdelcaribe/productos/materiales-electricos

MailRadar. (2007). Recuperado el 2013, de http://www.mailradar.com/openrelay/

Mxtoolbox. (2012). Recuperado el 2013, de http://mxtoolbox.com/blacklists.aspx

Network-tools. (2012). Recuperado el 2013, de http://network-tools.com

Piattini, M. G., & del Peso Navarro, E. (1997). *Auditoria Informatica Un enfoque practico.*

t1shopper. (2012). Recuperado el 2013, de http://www.t1shopper.com/

The password Meter. (s.f.). Recuperado el 2013, de http://www.passwordmeter.com/

vsantivirus. (2003). Recuperado el 2013, de http://www.vsantivirus.com/eicar-test.htm

Whatismyipaddress. (2012). Recuperado el 2013, de http://whatismyipaddress.com/blacklist-check