FACULTAD DE INGENIERIA Y CIENCIAS AGROPECUARIAS

AUDITORÍA DE SEGURIDAD INFORMÁTICA INTERNA Y PERIMETRAL DE LA FILIAL EN ECUADOR DE UNA EMPRESA MULTINACIONAL

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

Profesor Guía
Ing. Paulo Rodríguez

Autor
Danny Gabriel Ayala Chiliquinga

Año
2012

DECLARACIÓN DEL PROFESOR GUÍA

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

_____

Paulo Rodríguez

Ingeniero

CI. 1712032463

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"

_____

Danny Gabriel Ayala Chiliquinga

CI. 1713389946

AGRADECIMIENTO

Agradezco a DIOS por darme la sabiduría necesaria para la realización de este trabajo.

A mis maestros que gracias a su guía hicieron posible la culminación de mi carrera.

Por último y no menos importante al Ing. Juan Cruz por brindarme la oportunidad para dar este paso importante en mi desarrollo profesional.

DEDICATORIA

A mi madre y hermana por su apoyo incondicional en todo momento.

A mi padre, que a pesar de estar lejos ha estado siempre pendiente de mí.

RESUMEN

Este documento muestra el planeamiento, levantamiento de información y ejecución del proceso de auditoría informática interna y perimetral de la filial en Ecuador de una empresa multinacional, teniendo como principal objetivo que el administrador de la infraestructura pueda conocer las vulnerabilidades potenciales de la red y elaborar un plan acción.

ABSTRACT

This document describes the planning, information gathering and implementation of internal IT audit process and perimeter of the subsidiary in Ecuador of a multinational company, having as main objective the network administrator can know the potential vulnerabilities and identify an action plan.

INDICE

INTRODUCCION

Hoy en día, en un mundo globalizado y con un vertiginoso avance tecnológico, las organizaciones han tenido que cambiar su manera de pensar en cuanto a la seguridad en el manejo de sistemas automatizados, interconectados entre sí y con el mundo. Los mismos que deben proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Así mismo las redes de telecomunicaciones se han convertido en el punto neural para la interacción de la sociedad moderna; desde la aparición de Internet, se han dado permanentes cambios, producidos por un lado gracias a los avances en el desarrollo de paquetes de software, tecnología, mercadotecnia por lo que se hace necesario ofrecer servicios confiables y seguros para satisfacer las necesidades de los usuarios.

Sin embargo, las infraestructuras independientemente de su escala no son cien por ciento inmunes a ataques, los mismos que pueden tener diversas causas o finalidades y ponen en riesgo los objetivos o metas de las organizaciones en su labor diaria.

Para minimizar los riesgos sería ideal facilitar al o a los administradores un informe del estado de la seguridad de la red, y así mismo sugerencias para aumentar la seguridad de los sistemas informáticos.

En nuestra área, el concepto de seguridad informática se aborda de manera más práctica, ya que las tareas que se deben realizar son mucho más activas e involucran acción constante y proactiva de los responsables de la administración. En base a los conocimientos generados se pueden realizar planes de acción específicos en caso de que se encuentren vulnerabilidades.

CAPITULO I

1.1. Definición del tema

1.1.1. Antecedentes

Actualmente la filial cuenta con una infraestructura de cableado estructurado categoría 5 y red inalámbrica mediante puntos de acceso con contraseña WEP dinámica.

Existe instalada y en producción una solución de respaldo de datos calendarizado.

Se encuentra en producción una sola VLAN ya que la cantidad de nodos o equipos interconectados no sobrepasa el número de direcciones de red disponibles.

Las licencias de software se administran desde la matriz hacia todas las filiales.

El antivirus y parches de seguridad se manejan de forma centralizada con una consola y un servidor de actualizaciones.

La navegación hacia internet se realiza a través de un proxy con filtrado de contenidos y control de acceso basado en usuarios de directorio activo.

El servidor de correo electrónico cuenta con protección en tiempo real de correo basura.

Los servidores WEB y de aplicaciones corporativas se manejan de forma centralizada fuera del país.

1.1.2. Formulación del problema

Toda la infraestructura funciona y se administra de forma centralizada, lo cual evidencia un único punto de falla para la comunicación entre filiales ya que no existe un centro de datos y comunicaciones de contingencia.

No existe escalabilidad a futuro al tener una sola VLAN tanto para usuarios

como para servidores.

La red inalámbrica está expuesta a ataques y accesos no autorizados ya que el cifrado WEP posee vulnerabilidades.

La infraestructura no cuenta con un control de acceso adicional o de detección de intrusos que complemente las políticas ya establecidas.

1.1.3. Objetivos

1.1.3.1. Objetivo General

Realizar la auditoria de seguridad informática interna y perimetral de la filial en Ecuador de una empresa multinacional, de tal forma que el administrador de la infraestructura pueda conocer las vulnerabilidades potenciales de la red y elaborar un plan acción.

1.1.3.2. Objetivos Específicos

Revisar la seguridad del entorno físico del centro de datos y cableado estructurado.

Evaluar la seguridad de los entornos de software de clientes y servidores.

Evaluar la posibilidad de acceder a la red interna cableada e inalámbrica de forma no autorizada.

Elaborar un informe acerca de la situación actual y recomendaciones para reforzar el sistema en caso de encontrar vulnerabilidades.

1.1.4. Alcance

Se realizará un levantamiento de información de los entornos de hardware, esto es servidores y equipos de comunicación del centro de datos y se analizará que tan probable es llegar a ellos de forma no autorizada.

Se evaluará el estado del cableado estructurado y red inalámbrica, sus características y factibilidad de realizar conexiones no autorizadas.

Se revisará el nivel de seguridad de los equipos de usuarios frente a ataques informáticos ya sea de correos maliciosos o virus informáticos.

No se ejecutarán acciones que puedan poner en riesgo la confidencialidad de la filial o datos críticos del negocio, tampoco se aplicarán o implementarán acciones que puedan poner en riesgo la continuidad de las operaciones.

1.1.5. Justificación del Proyecto

A pesar del avance y evolución en la tecnología informática y de comunicaciones, las redes computacionales no están inmunes a intrusiones, ataques y accesos no autorizados, inclusive con un detallado esquema de arquitectura de red y sofisticados sistemas de seguridad no se pueden detectar muchos de los riesgos a los cuales está expuesta la información, sobre todo si se pasa por alto una periódica evaluación del estado de seguridad de la red.

Por lo indicado anteriormente, surge la necesidad de evaluar el estado de seguridad informática de la filial en Ecuador de una empresa multinacional, tal evaluación contribuye a la detección de vulnerabilidades, aumentando así la autenticidad, integridad, confiabilidad y disponibilidad de los recursos tecnológicos.

1.1.6. Metodología

La metodología a utilizar es la de Evaluación de Riesgos (ROA Risk Oriented Approach) bajo técnicas de CHECKLIST mediante la cual se revisa y verifica los controles con la ayuda de una lista de preguntas o ítems a verificar. (Piatinni y del Peso, 2001, p.568)

Esta metodología se basa en un procesamiento interno de información con el fin de obtener respuestas que permitan una correcta descripción de puntos débiles y fuertes. (Universidad de Belgrano, 2012, http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm).

1.1.6.1. Checklist de rango

Lista de verificación que contiene aspectos que el auditor debe puntuar dentro de un rango preestablecido.

Por ejemplo: En el análisis del control de acceso a un cuarto de equipos se verifica que tipo de control existe sobre el ingreso del personal y se puede tener la siguiente valoración:

1. Bueno
2. Regular
3. Malo

1.1.6.2. Checklist binario

Esta lista de verificación se caracteriza por que su respuesta es única y excluyente. Si o No.

Por ejemplo: En el análisis de utilización de recursos de red por parte de los usuarios, se utilizan contraseñas de acceso.

1. Si
2. No

1.2. Marco teórico

1.2.1. Auditoría informática

Auditoría informática es un proceso que consiste en recolección de datos y evaluación de evidencias con el fin de determinar si un sistema de información cumple las condiciones necesarias para garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos. (Piatinni y del Peso, 2001, p.28)

- Confidencialidad: Propiedad de la información mediante la cual se garantiza que será accesada únicamente por quienes tengan la debida autorización. (Piatinni y del Peso, 2001, p.398)

- Integridad: Propiedad de la información mediante la cual se garantiza que los datos sean correctos, completos sin ningún tipo de alteración. (Piatinni y del Peso, 2001, p.399)

- Disponibilidad: Se refiere a la accesibilidad de la información el momento que se requiera. (Piatinni y del Peso, 2001, p.399)

- Autenticidad: Propiedad que permite identificar a quien genera la información, y asegura que se esté suplantando al mismo. (Piatinni y del Peso, 2001, p.399)

El proceso de auditoría debe regirse a una metodología, aplicarse con formalidad y mediante una planificación oportuna, con el objetivo de optimizar los recursos informáticos.

1.2.2. Tipos de metodología

Las metodologías existentes se agrupan en dos clases:

1.2.2.1. Cuantitativas

Se asignan valores numéricos a las listas para su respectiva comparación, proporcionan datos de probabilidad de eventos o de riesgos. (Piatinni y del Peso, 2001, p.51)

1.2.2.2. Cualitativas

Basado en criterios en base a experiencias, en este tipo de metodologías se corre el riesgo de pasar por alto riesgos desconocidos por la misma falta de experiencia del profesional. (Piatinni y del Peso, 2001, p.52)

Las metodologías de auditoría informática son de tipo cualitativo ya que se apoyan en la experiencia y formación de los profesionales, existen dos familias distintas de metodología de auditoría informática:

- Auditorías de controles generales, definen políticas y procedimientos que se aplican a los sistemas de información e infraestructuras de TI

procurando obtener un correcto funcionamiento y cuyo objetivo es dar una opinión sobre la fiabilidad de dichos sistemas. (Piatinni y del Peso, 2001, p.63)

- Metodologías de auditores internos, estas se estructuran en base a las recomendaciones del plan de trabajo y el proceso a seguir, además define el objetivo de la misma, describe la auditoría en forma de cuestionarios basados en los controles a verificar. (Piatinni y del Peso, 2001, p.63)

1.2.3. Fases de la auditoria informática

- Identificación de los objetivos y delimitación del alcance.
- Identificación de fuentes y recopilación de información.
- Determinación del plan de trabajo.
- Adaptación de cuestionarios, listas de verificación y herramientas.
- Realización de entrevistas y pruebas.
- Análisis de resultados y valoración de riesgos.
- Presentación del informe. (Piatinni y del Peso, 2001, p.399)

1.2.4. Informe de auditoría

El informe constituye el producto del proceso de auditoría y es el documento que se entrega al cliente concluido el trabajo. En el informe se deben incluir los antecedentes, objetivos y el alcance.

En cada punto debe explicarse los incumplimientos o debilidades encontradas y sus respectivas recomendaciones. (Piatinni y del Peso, 2001, p.638)

1.2.5. Seguridad informática

La seguridad informática es una rama de la tecnología aplicada a

computadores y redes, cuyo objetivo se enfoca en la protección de la infraestructura e información contenida en esta, para lo cual utiliza una serie de procesos y mecanismos concebidos para minimizar los posibles riesgos o vulnerabilidades que pueden afectar la infraestructura o la información.

Dentro de los objetivos primordiales de la seguridad informática tenemos:

Proteger la información por ser el activo más valioso dentro de una organización, evitando que usuarios externos, no autorizados o malintencionados puedan hacer uso de esta.

Garantizar el funcionamiento adecuado de los equipos informáticos y prever con antelación planes de acción en caso de que existiese algún tipo de falla en los mismos u ocurran acontecimientos que provoquen su operación incorrecta.

Establecer normas o reglas a los usuarios que minimicen los riesgos a la información o infraestructura informática.

1.2.5.1. Amenazas

Las amenazas son circunstancias que pueden afectar tanto a los datos como a los equipos y suelen ser imprevisibles, estas pueden estar ligadas a factores informáticos (programas maliciosos, virus informáticos, gusanos informáticos, troyanos) destinados a perjudicar a los usuarios, sustraer información o a hacer un mal uso de los recursos del sistema. Existen amenazas en las que el factor humano es determinante ya sea por negligencia, o desconocimiento.

Amenazas internas se presentan debido a esquemas de seguridad inapropiados o ineficientes en las compañías, ya que no existe planificación adecuada que proteja los recursos informáticos frente a estas.

Amenazas externas a la red local, generalmente ocasionados por atacantes que buscan la forma de infiltrarse sin ser detectados.

1.2.5.2. Vulnerabilidades

“Las vulnerabilidades son errores que permiten realizar tanto interna o

externamente actos sin consentimiento o conocimiento del administrador de la red, suplantar usuarios, con fines ilícitos." (Wikilibros, 2012, http://es.wikibooks.org/wiki/Seguridad_informatica/Vulnerabilidad).

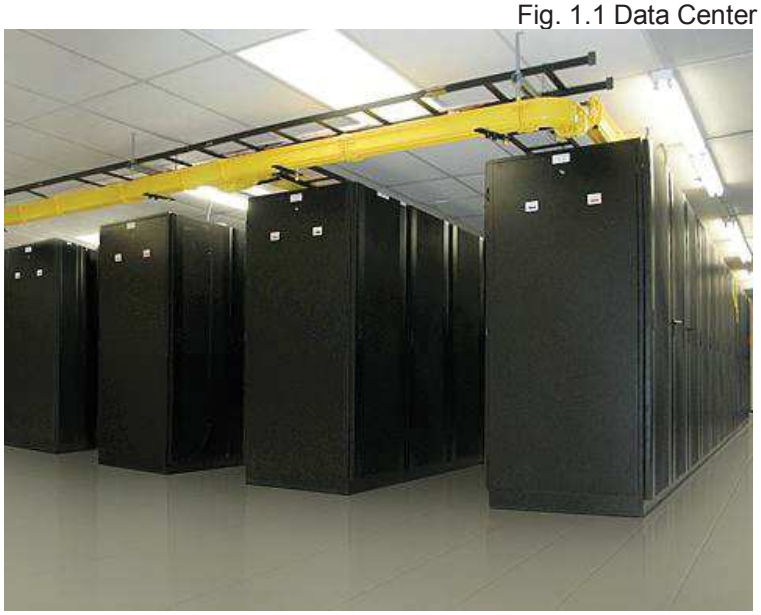
1.2.6. Mecanismos o técnicas de seguridad informática

Existen diversos recursos, mecanismos o técnicas para proteger sistemas informáticos:

1.2.6.1. Centro de datos o de cómputo

La localidad donde se concentran los recursos computacionales o informáticos y de telecomunicaciones de una organización, dicha localidad debe contar con todas las características que permitan la continuidad y alta disponibilidad de las operaciones. (Fig. 1.1)

Fig. 1.1 Data Center



Fuente: http://www.digitalone.com/us-data-center.html

1.2.6.2. Suministro ininterrumpido de energía

Conocidos por sus siglas en inglés UPS (Uninterrupted Power Suply) es un dispositivo que posee baterías que se están cargando constantemente y provee energía eléctrica por un lapso de tiempo prudencial a los equipos que se encuentran directamente conectados a él en caso de que la alimentación

proveniente del proveedor de electricidad falle. (Fig. 1.2)

Fig. 1.2 Equipos UPS

Fuente: http://electroprotecciones.com.ec

1.2.6.3. Generador de energía

Es una planta generadora de corriente que puede ser alimentada por combustible, la misma que suple la falta de electricidad por parte del proveedor del servicio público.

1.2.6.4. Sistema de refrigeración de equipamiento informático

Son sistemas que previenen problemas causados por altas temperaturas en los centros de equipos manteniendo una temperatura adecuada para su normal operación.

1.2.6.5. Extintores de incendios

Son artefactos diseñados para apagar fuego, pero en nuestro caso extinguir incendios que se presenten en el cuarto de equipos, existen varios tipos:

- Extintores de polvos universales para fuegos ABC
- Extintores de polvo químico seco para combatir fuegos de clase BC
- Extintores de CO2,
- Extintores para metales.

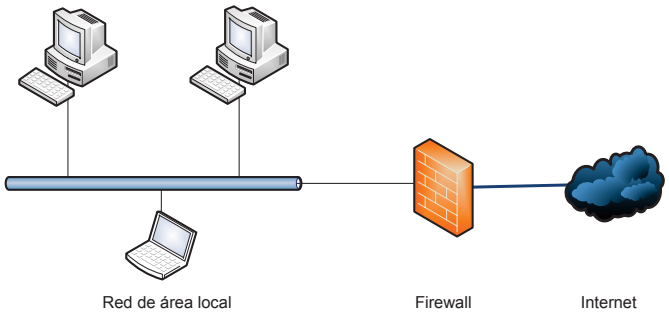
Fig. 1.3 Extintor

Fuente: http://es.wikipedia.org

1.2.6.6. Firewall

Firewall es un sistema de software o hardware que se ubica entre dos redes, (la red pública y una red de área local) para limitar el tipo de tráfico entre estas. (Fig. 1.4)

Fig. 1.4 Esquema lógico de red con Firewall

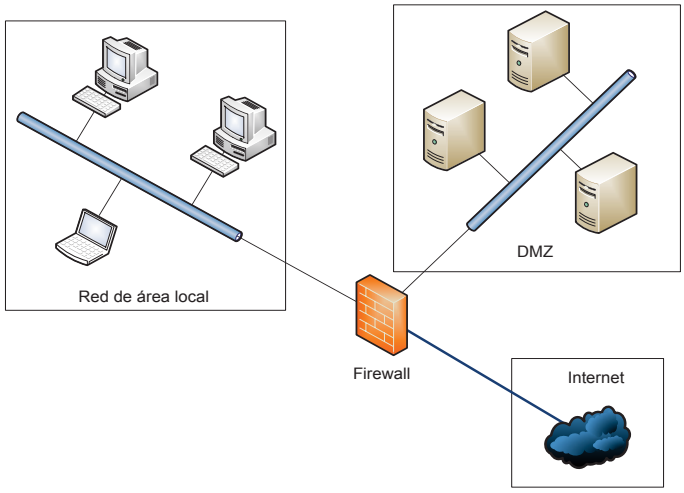


Fuente: Autor

1.2.6.7. Zona desmilitarizada (DMZ)

Red separada de una compañía a la que se puede acceder tanto desde la red interna como desde una red externa (generalmente servidores web) con el objetivo de no comprometer la seguridad. (Fig. 1.5)

Fig. 1.5 Esquema lógico de una red con DMZ



Fuente: Autor

1.2.6.8. Antivirus

Un antivirus es un programa de software desarrollado con el objetivo de detectar, prevenir o eliminar virus informáticos para lo cual se mantiene ejecutándose en el equipo al que se necesita proteger.

- **Virus informático**

Es un programa o software desarrollado o creado con fines maliciosos cuyos objetivos pueden ser varios:

- Alterar el normal funcionamiento del equipo informático.
- Robar información.
- Suplantar la identidad del usuario frente a los sistemas computacionales.

Hay diversos tipos de virus y entre los más comunes están:

Troyanos, se caracterizan por introducirse en los ordenadores como programas inofensivos pero con el objetivo de proporcionar el control del mismo a usuarios remotos.

Gusanos, tienen la característica de duplicarse a sí mismos ocasionando problemas de rendimiento.

Bombas lógicas son programas maliciosos que permanecen ocultos e

inactivos hasta llegar un determinado período de tiempo programado, en el cual ejecutan las acciones para los que fueron creados.

1.2.6.9. Antispam

Antispam es una técnica utilizada para prevenir el correo electrónico considerado basura, o no deseado, (generalmente publicidad). Se pueden aplicar a los servidores de correo electrónico o a los programas clientes de correo de usuarios finales.

1.2.6.10. Servidores de actualizaciones

Servidores que se encargan de descargar automáticamente los parches de seguridad y actualizaciones para los clientes en la red.

1.2.6.11. Respaldos de seguridad

Es importante disponer de sistemas de respaldos o de backups que protejan la información frente a fallas de equipos, incendios, robo, desastres naturales entre otros. Estos sistemas permiten una recuperación relativamente rápida ante estos acontecimientos.

1.2.6.12. Políticas de seguridad

Es importante para cada compañía elaborar políticas con las que se aseguren un adecuado uso de los equipos informáticos, herramientas e información contenida en los mismos.

Algunas políticas pueden ser:

- Utilización de un directorio activo y unidades organizativas.
- Cambio periódico de claves de usuario.
- Complejidad de contraseñas.
- Permisos de navegación hacia determinados sitios.
- Permisos del usuario sobre los equipos de escritorio.

CAPITULO II
LEVANTAMIENTO DE INFORMACIÓN

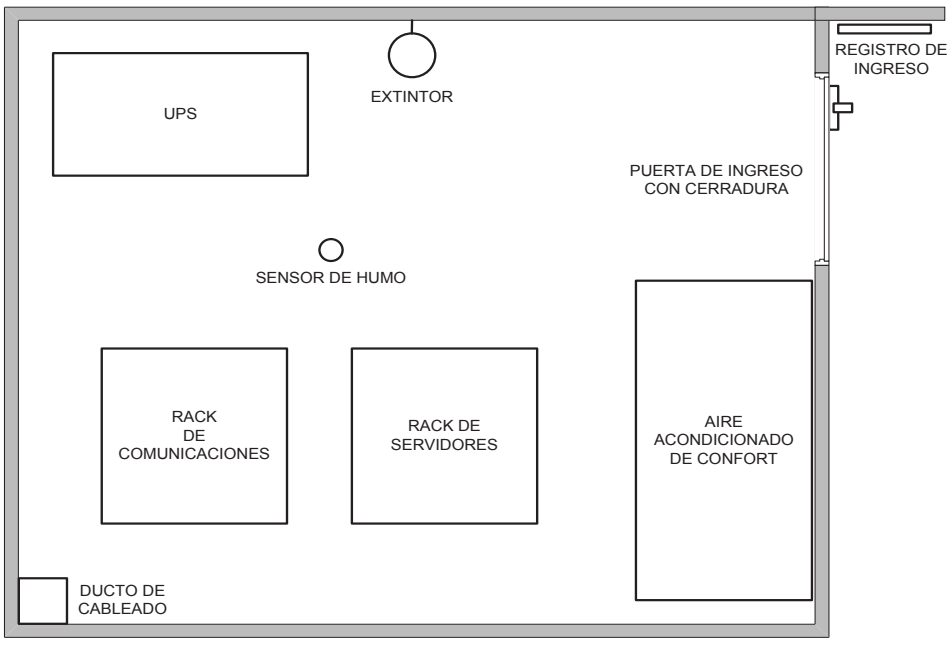
La infraestructura tecnológica actualmente es la base de cualquier empresa la cual permite el máximo aprovechamiento de los recursos, aumento del valor de la empresa y una respuesta más rápida frente a las exigencias del mercado.

Esta etapa se realizará con la colaboración del administrador de la red, el cual proporcionará la información pertinente pero que no comprometa la confidencialidad de la filial.

2.1. Mecanismos y técnicas de seguridad del centro de datos

El centro de datos alberga sistemas informáticos y equipos de telecomunicaciones por medio de los cuales se realiza el proceso de comunicación interna y externa de la filial. La figura 2.1 muestra la disposición física de los elementos en el centro de datos.

Fig. 2.1 Disposición de equipos y dispositivos en el centro de datos



Fuente: Autor

La tabla 2.1 muestra las características de los sistemas de seguridad utilizados en el centro de datos, los datos y características de los sistemas se obtienen mediante observación.

Tabla 2.1 Mecanismos de seguridad del centro de datos

MECANISMO / TECNICA	CARACTERISTICAS
PUERTA DE INGRESO	• Aislamiento térmico y acústico. • Señalización.
CERRADURA	• Teclado para digitar la clave de acceso • Alimentación por medio de baterías • La llave se la guarda en una caja fuerte bajo el cargo del administrador de activos.
REGISTRO DE INGRESO	• Documento físico donde se registra nombre, fecha, hora y trabajo a realizar de las personas que ingresan. • Se registra el nombre de la persona que autoriza el ingreso.
AIRE ACONDICIONADO	• De confort.
PISO	• De baldosa
SISTEMA DE ALIMENTACIÓN DE ENERGÍA	• UPS 15 KVA • Generador de energía alimentado por combustible.
SISTEMAS DE SEGURIDAD	• Extintor de incendios de polvo químico universal ABC. • Sensores de humo.

Fuente: Autor

2.2. Infraestructura de comunicaciones y cableado estructurado

Por medio de los equipos de telecomunicaciones se realiza el proceso de comunicación interna y externa de la filial. Los equipos se ubican en el rack de comunicaciones de acuerdo a lo que se muestra en la tabla 2.2

Tabla. 2.2 Equipos de comunicaciones

EQUIPO	MARCA/MODELO	CARACTERISTICAS / OBSERVACIONES
Router	Cisco 2600	• Administrado por el proveedor de internet
Router	Cisco 1800	• Administrado localmente
Switch	3COM 3824	• 24 puertos • Administrable
Switch	D-LINK 1024R+	• 24 puertos • No administrable
Patch Panel	48 puertos	
Switch	D-LINK 3226L	• 24 puertos • Administrable
Switch	Allied Telesyn AT-FS724i	• 24 puertos • No administrable
Patch Panel	48 puertos	
Switch	Allied Telesyn FS7241i	• 24 puertos • No administrable
Switch	D-LINK 1024R+	• 24 puertos • No administrable
Patch Panel	48 puertos	
Switch Fibra Optica	N/D	• Administrado por el proveedor
Dispositivo de Seguridad	Cisco ASA 5510	• Administrado desde Matriz
Switch	3COM 2024	• 24 puertos • No administrable

Fuente: Autor

- Todos los puntos de red de los pisos se concentran en el rack de comunicaciones del centro de datos.

2.3. Infraestructura de red inalámbrica

Las instalaciones cuentan con red inalámbrica, los dispositivos se listan en la tabla 2.3

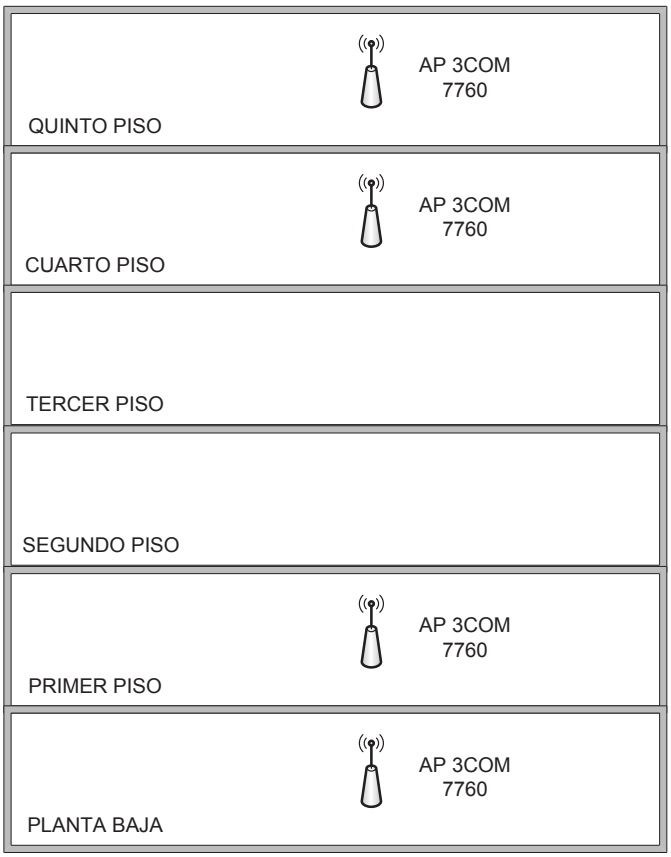
Tabla 2.3 Dispositivos de red inalámbrica

EQUIPO	MARCA/MODELO	CANTIDAD	CARACTERISTICAS / OBSERVACIONES
Access Point	3Com 7760	4	• SSID oculto • Contraseña cifrado WEP

Fuente: Autor

La ubicación de los dispositivos en el edificio se muestra en la figura 2.2.

Fig. 2.2 Distribución de puntos de acceso en el edificio



Fuente: Autor

- El nombre de red oculto y la contraseña solo se proporciona a los

usuarios mediante autorización de su supervisor y del responsable del área de sistemas.

- El cifrado de seguridad es de tipo WEP de 64bits, se renueva cada mes.

2.4. Infraestructura de servidores

El centro de datos alberga los equipos que brindan servicios a las estaciones de trabajo o clientes de la red.

Al tratarse de la filial una empresa multinacional, los servicios básicos de red se proveen localmente, mientras que los servidores de aplicaciones, bases de datos y servidores web se encuentran en la matriz de la empresa, esto es fuera del país.

En la tabla 2.4 se resume los servidores instalados y sus características esenciales.

Tabla 2.4 Servidores

TIPO DE SERVIDOR	CARACTERISTICAS
Servidor DNS externo	• Servidor de DNS externo
Firewall y Servidor Proxy	• S.O. Windows Server 2003 • ISA Server 2006
Servidor de Correo y Antispam	• S.O. Windows Server 2003 • Exchange Server 2003 • Antigen for Exchange
Servidor DNS primario	• S.O. Windows Server 2003 • Directorio Activo
Servidor DNS secundario	• S.O. Windows Server 2003 • Directorio Activo
Servidor de DHCP	• S.O. Windows Server 2003
Servidor de archivos e impresión	• S.O. Windows Server 2003 • HP Web Jet Admin

TIPO DE SERVIDOR	CARACTERISTICAS
Servidor de Actualizaciones	• S.O. Windows Server 2003 • WSUS • Consola antivirus Forefront
Sistema de copias de seguridad a cinta	• S.O. Windows Server 2003 • HP Data Protector

Fuente: Autor

- Todas las licencias de software se administran desde la matriz hacia todas las filiales.

2.5. Clientes o equipos de red

En la tabla 2.5 se muestra los equipos y sus características concernientes a las políticas de seguridad.

Tabla 2.5 Clientes de red

TIPO DE CLIENTE	CARACTERISTICAS	NUMERO DE EQUIPOS
Equipo terminal	• Windows XP SP3 • Antivirus Microsoft Forefront • Isa Server 2006 Client Security	86
Impresora	• Administración desde el servidor de impresión	5

Fuente: Autor

2.6. Distribución de usuarios con acceso a recursos tecnológicos

La filial cuenta con 88 empleados, distribuidos en los pisos de acuerdo a lo que se muestra en la tabla 2.6

Tabla 2.6 Distribución de usuarios

UBICACION	AREA	NUMERO DE USUARIOS
Planta baja	Sistemas / Recepción	22
Primer piso	Financiero / Administrativo	11

UBICACION	AREA	NUMERO DE USUARIOS
Tercer piso	Operativo	22
Cuarto piso	Comercial	12
Quinto piso	Operativo	21

Fuente: Autor

De la totalidad de empleados 86 personas tienen acceso a los recursos de la red.

64 usuarios tienen derechos de administración local de su respectivo equipo, lo que equivale al 74,4% de la población.

2.7. Políticas de seguridad en las contraseñas de acceso de usuarios

- Las contraseñas deben estar formadas por un mínimo de 7 caracteres, entre mayúsculas, minúsculas y caracteres especiales. (Anexo 2).
- La contraseña inicial emitida a un nuevo usuario debe ser cambiada en el primer ingreso a la red.
- La contraseña deben ser renovada cada 60 días por el usuario. (Anexo 2).
- Luego de tres ingresos erróneos de la contraseña, la cuenta será bloqueada, y solo podrá ser desbloqueada por el personal de soporte bajo solicitud del usuario afectado. (Anexo 2).

2.8. Resumen

En la figura 2.3 se muestra el diagrama lógico de la red a ser auditada.

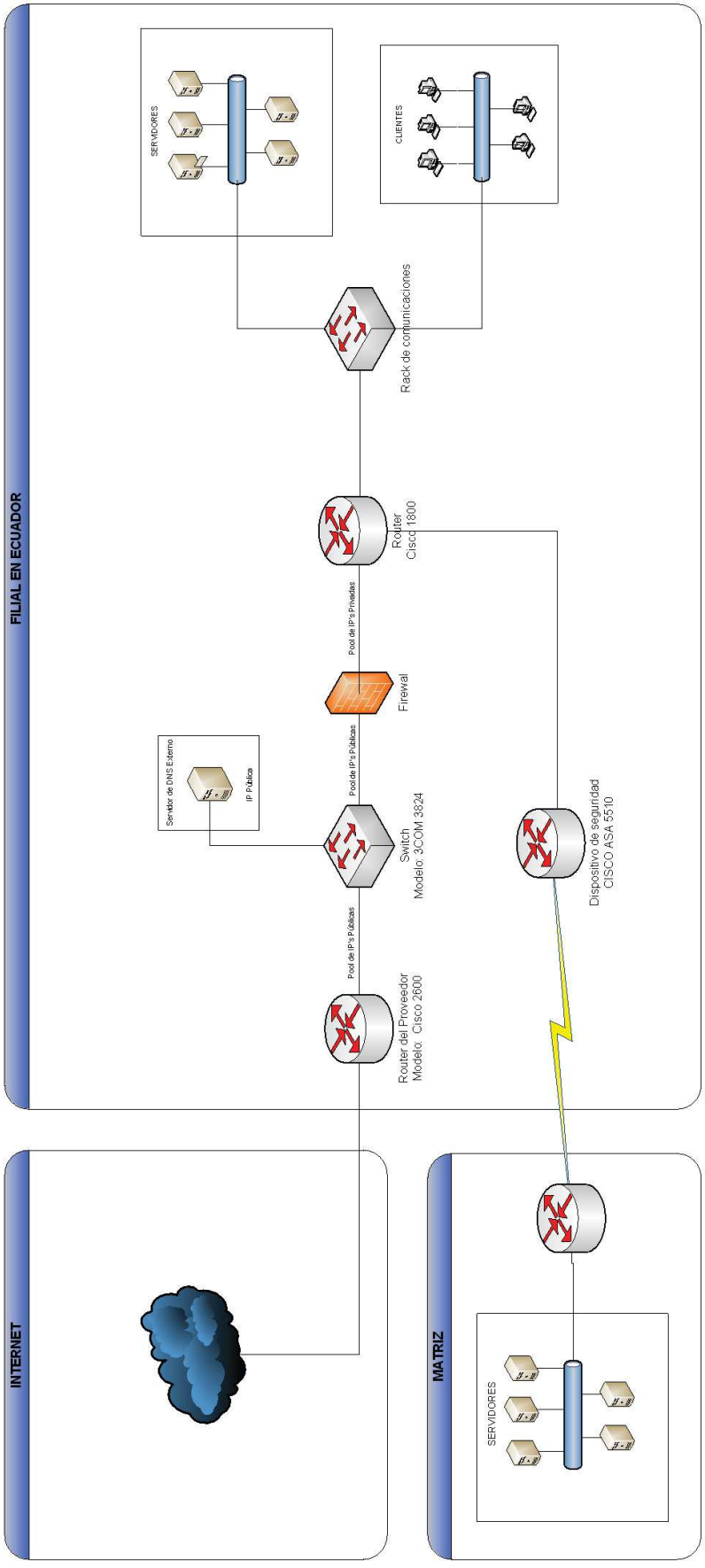


Fig. 2.3 Diagrama lógico de red

Fuente: Autor

CAPITULO III
ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1. Identificación de recursos

Con el objetivo de elaborar un informe de auditoría se realizará el levantamiento de la información, mediante listas de verificación (Checklist) se analizarán los mecanismos y sistemas de seguridad implementados.

Esta etapa se realizará con la colaboración del administrador de la red, para lo cual se solicita autorización para obtener capturas de pantalla para demostrar las pruebas de los sistemas. Se concede dicha autorización siempre y cuando las capturas de pantalla no revelen usuarios, contraseñas o comprometan la confidencialidad de la filial; además de que no se apliquen acciones que puedan poner en riesgo la continuidad de las operaciones.

3.1.1. Verificación y análisis de técnicas y mecanismos de seguridad del centro de datos

Para la tabulación de resultados se realizará una escala subjetiva de valores, esencialmente buena, regular o mala dependiendo de las características y las recomendaciones para los mecanismos. (Ver Tabla 3.1)

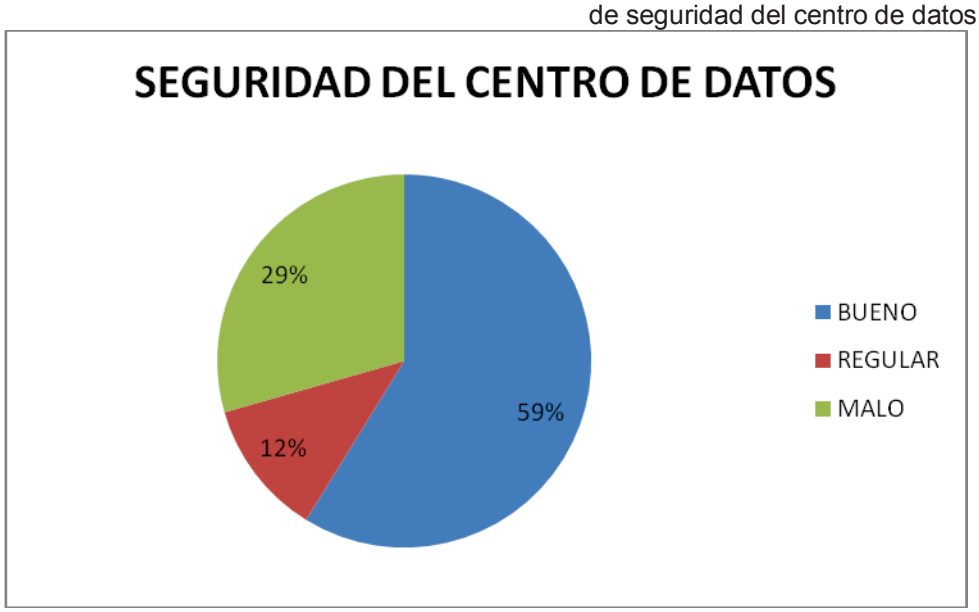
Tabla 3.1 Verificación de los mecanismos y técnicas de seguridad del centro de datos

MECANISMO / TECNICA	OBSERVACION	VALORACION		
		BUENO	REGULAR	MALO
Puerta de ingreso	Aislamiento térmico	✓		
	Aislamiento acústico	✓		
	Señalización	✓		
Cerradura electrónica y con llave	Teclado para digitar la clave de acceso	✓		
	Cambio periódico de la clave de acceso			✓
	Alimentación por medio de baterías.		✓	

MECANISMO / TECNICA	OBSERVACION	VALORACION		
		BUENO	REGULAR	MALO
Cerradura electrónica y con llave	Registro de reemplazo de baterías.			✓
	La llave se guarda en un lugar seguro.	✓		
Registro de ingreso al centro de datos	Documento físico donde se registra nombre, fecha, hora y trabajo a realizar de las personas que ingresan.	✓		
	Se registra el nombre de la persona que autoriza el ingreso	✓		
Aire acondicionado	De confort			✓
	Sensores de humedad y temperatura			✓
Piso	Antiestático			✓
Sistemas de alimentación de energía	UPS 15 KVA	✓		
	Generador de energía alimentado por combustible	✓		
Sistemas de seguridad	Extintor de incendios de polvo químico universal ABC		✓	
	Sensores de humo	✓		

Fuente: Autor

Grafico 3.1 Tabulación de resultados de verificación de los mecanismos y técnicas de seguridad del centro de datos



Fuente: Autor

Observaciones

- La puerta de ingreso con aislamiento térmico y acústico busca mantener una temperatura adecuada en el centro de datos, y que el ruido de los equipos en funcionamiento no incomoden a los empleados.
- La señalización permite la identificación del lugar y advierte el acceso limitado solo para personal autorizado que son los administradores de red.
- La cerradura con teclado para digitar clave de acceso previene el acceso a personas no autorizadas que no conozcan la clave de seguridad.
- No existen registros de cambios de clave para ingresar al centro de datos.
- No existen registros de reemplazo de baterías de la cerradura electrónica.
- El registro de ingreso al centro de datos permite documentar el control de qué persona ingresa, la fecha, la hora y la tarea a realizar en el centro de datos además de que persona autoriza dicho ingreso.

- El aire acondicionado instalado no cumple con las características de precisión y de nivel de temperatura recomendadas para un centro de datos.

- No se observan instalados sensores de humedad y temperatura del ambiente.

- El piso del centro de datos no cumple con las características recomendadas contra descargas electroestáticas.

- En caso de producirse un incendio, no se utiliza un extintor de polvo químico para centros de datos, el mismo podría afectar el funcionamiento de los equipos electrónicos.

3.1.2. Verificación y análisis de seguridad del cableado estructurado y equipos de comunicaciones

Para la tabulación de resultados se realizará una escala de valores, esencialmente buena, regular o mala dependiendo de las características y las recomendaciones para los mecanismos. (Ver tabla 3.2)

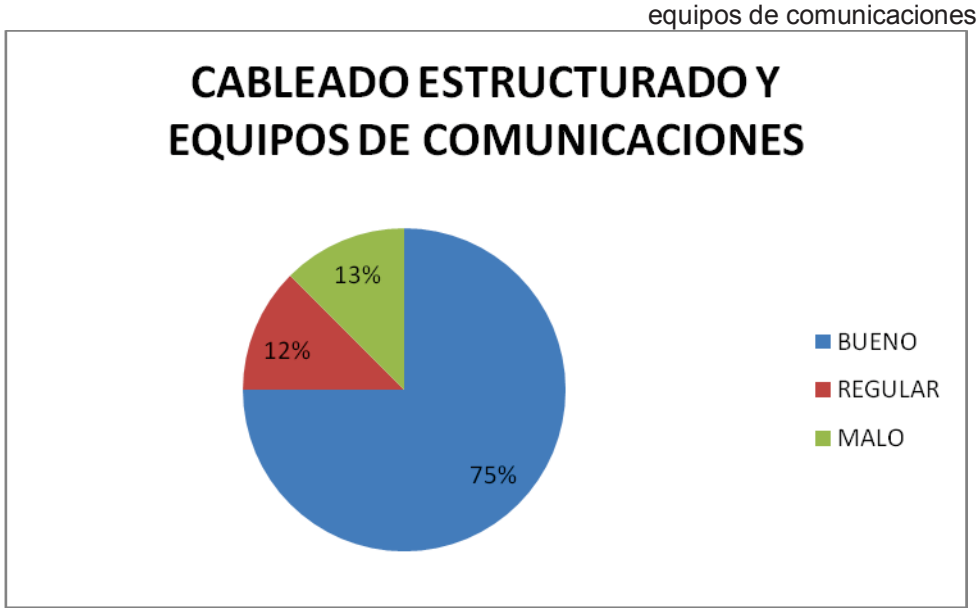
Tabla 3.2 Verificación de los mecanismos y técnicas de seguridad de cableado estructurado y equipos de comunicaciones

EQUIPO / ELEMENTO	VERIFICACION / PRUEBA	VALORACION		
		BUENO	REGULAR	MALO
Cableado del rack de comunicaciones	Verificación de organización deficiente del cableado en el rack			✓
	Edad del cableado menor a 5 años		✓	
	Todos los puntos de red se centralizan en el rack de comunicaciones			✓
	Puntos de red identificados		✓	
Router de proveedor Cisco 2600	Administrado por el proveedor de internet	✓		
Router de borde Cisco 1800	Se ha modificado usuario y contraseña colocado por el fabricante (Fig. 3.1)	✓		
Switch administrable 3COM 3824	Se ha modificado usuario y contraseña colocado por el fabricante (Fig. 3.2)	✓		
Switch D-LINK 1024R+	Equipo no administrable	✓		
Switch D-LINK 3226L	Se ha modificado usuario y contraseña colocado por el fabricante (Fig. 3.3)	✓		

EQUIPO / ELEMENTO	VERIFICACION / PRUEBA	VALORACION		
		BUENO	REGULAR	MALO
Switch Allied Telesyn AT-FS724i	Equipo no administrable	✓		
Switch Allied Telesyn FS7241i	Equipo no administrable	✓		
Switch D-LINK 1024R+	Equipo no administrable	✓		
Switch Fibra Optica	Administrado por el proveedor	✓		
Dispositivo de Seguridad Cisco ASA 5510	Administrado desde Matriz	✓		
Switch 3COM 2024	Equipo no administrable	✓		
Access point 3COM 7760	Se ha modificado usuario y contraseña colocado por el fabricante en los 4 equipos (Fig. 3.4)	✓		

Fuente. Autor

Grafico 3.2 Tabulación de resultados de verificación de cableado estructurado y equipos de comunicaciones

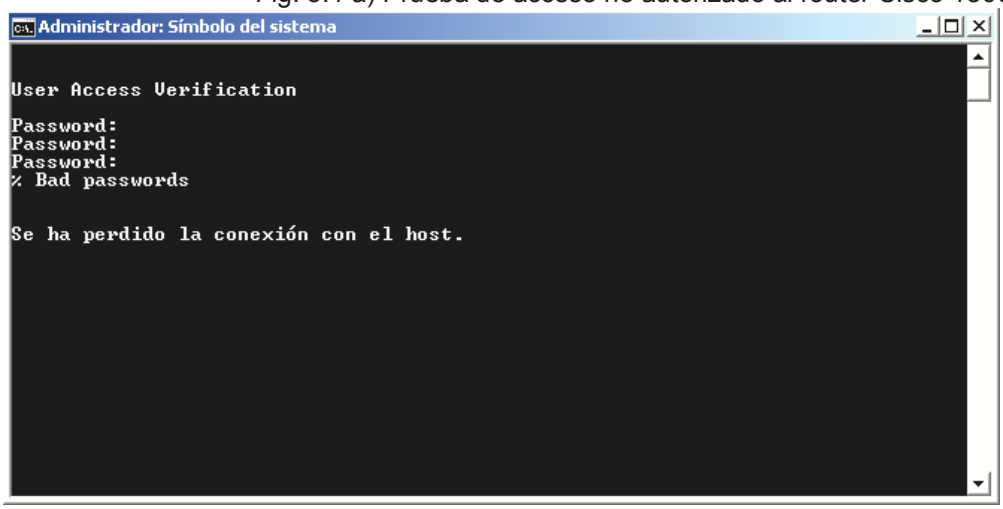


Fuente: Autor

Observaciones

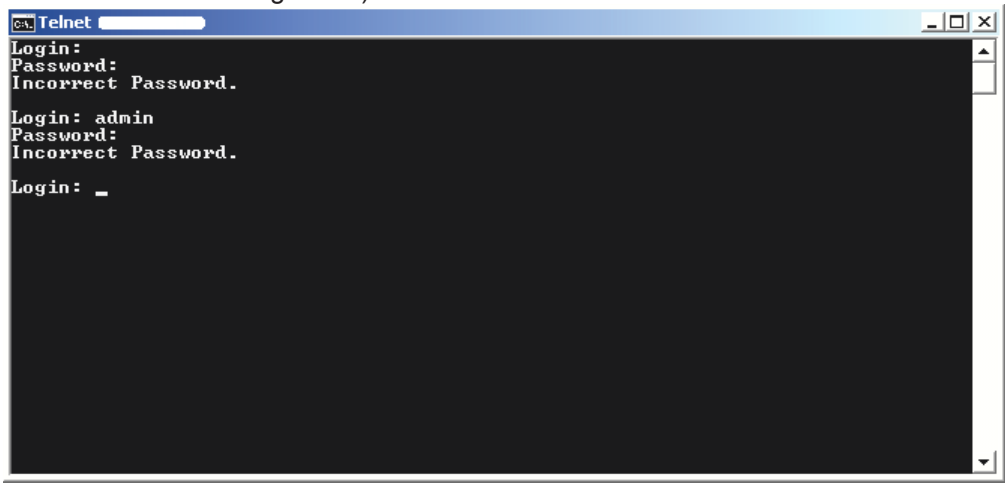
- Se verifica que la organización de los cables del rack de comunicaciones es deficiente como resultado de que todos los puntos de la red confluyen hacia él.
- Varios puntos de red no se encuentran identificados, lo que dificultaría la resolución de problemas de conectividad.
- Los equipos de comunicaciones administrables tienen configurado usuario y contraseña diferente a la colocada por el fabricante. Tomando en cuenta el anexo 2 en donde se encuentran fragmentos de la documentación técnica de los dispositivos se muestran capturas de pantalla de los intentos de ingreso a la interfaz de administración de los equipos. (Fig. 3.1)

Fig. 3.1 a) Prueba de acceso no autorizado al router Cisco 1800



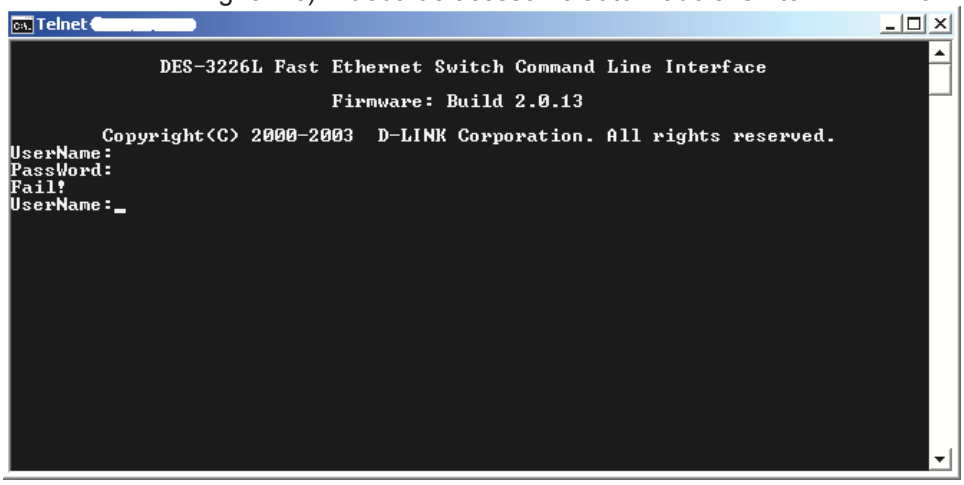
Fuente: Autor

Fig. 3.1 b) Prueba de acceso no autorizado al switch 3Com 3824



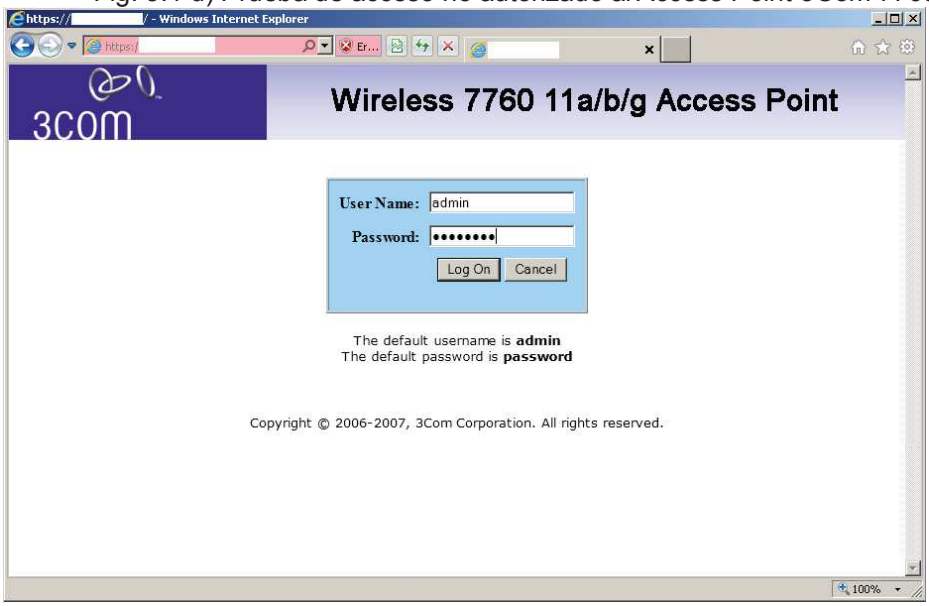
Fuente: Autor

Fig. 3.1 c) Prueba de acceso no autorizado al switch D-LINK 3226L



Fuente: Autor

Fig. 3.1 d) Prueba de acceso no autorizado al Access Point 3Com 7760



Fuente: Autor

3.1.3. Verificación y análisis de seguridad de la red inalámbrica

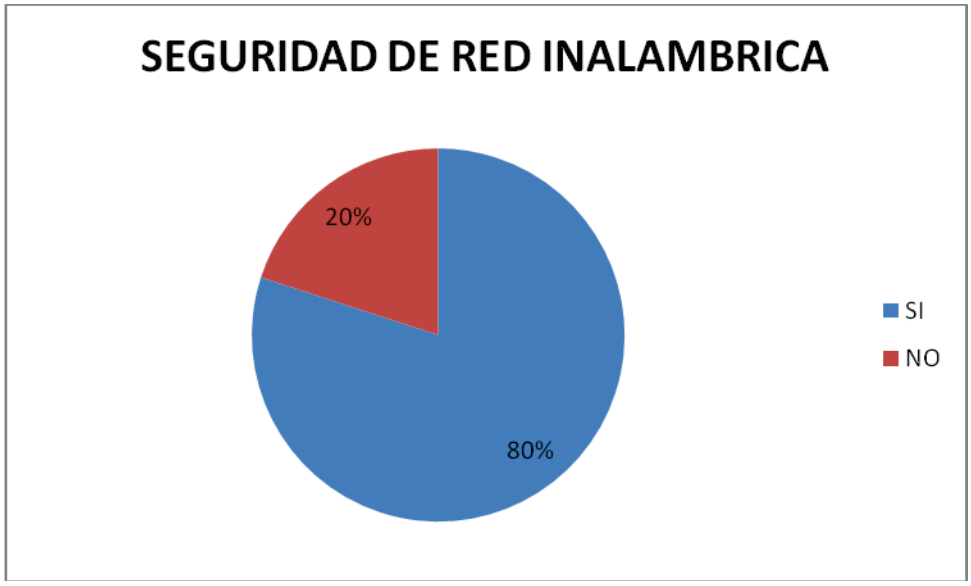
Para la tabulación de resultados se realizará una valoración de SI o NO dependiendo de la característica y las recomendaciones para el mecanismo utilizado. (Ver tabla 3.3)

Tabla 3.3 Verificación y análisis de seguridad de la red inalámbrica

VERIFICACION	RESULTADO	
	SI	NO
Nombre de la red inalámbrica oculto	✓	
Se utiliza contraseña de red inalámbrica con cifrado robusto		✓
Se cambia la contraseña periódicamente	✓	
Navegación por la red inalámbrica es limitada	✓	
Se utiliza mecanismos de autenticación a nivel de usuario	✓	

Fuente: Autor

Gráfico 3.3 Tabulación de resultados de verificación y análisis de seguridad de la red inalámbrica



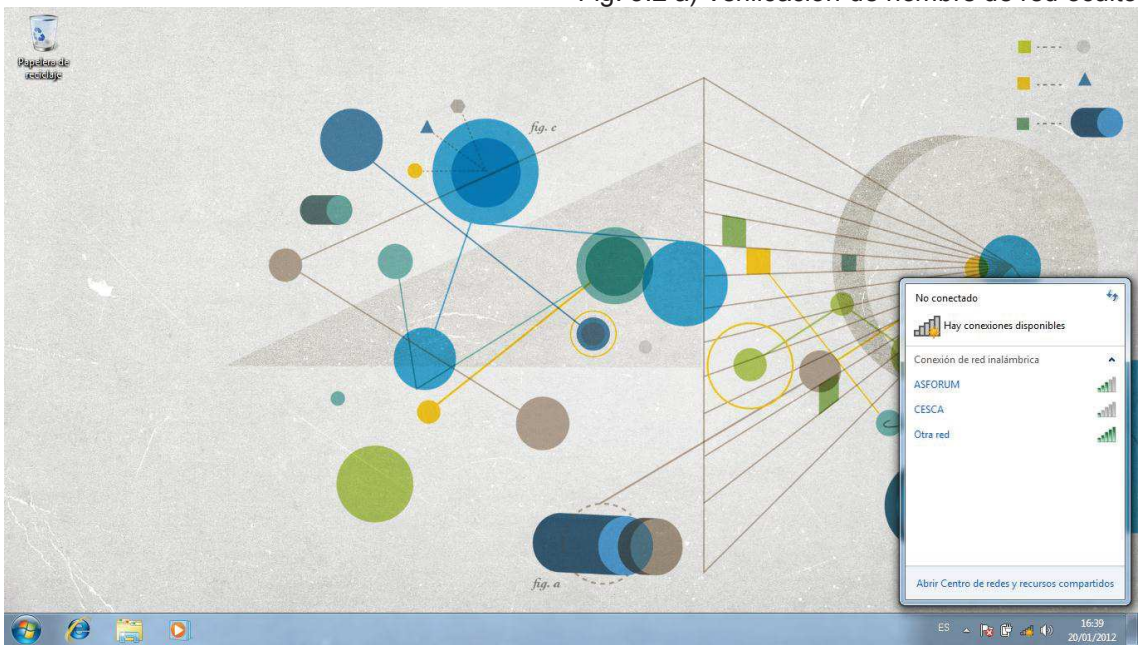
Fuente: Autor

Observaciones

- La red inalámbrica tiene configurado un nombre de red oculto, las pruebas demuestran que a menos que no se conozca el nombre de la red se complica la conexión a la misma.

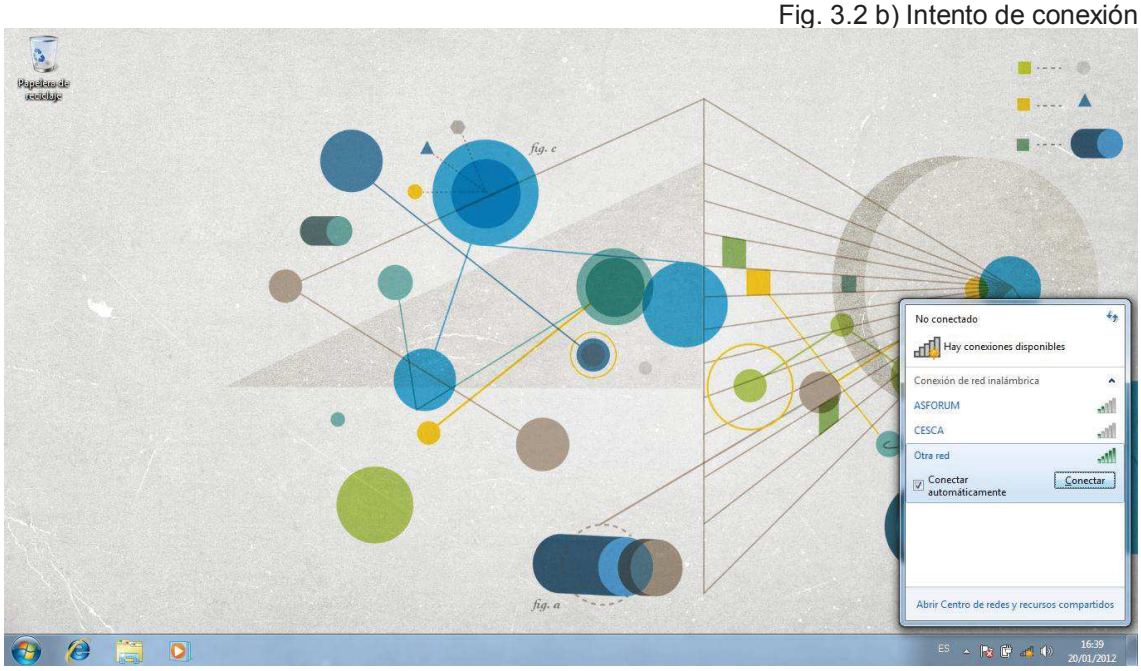
- Las pruebas se realizan con un equipo que no pertenece a la organización. (Ver Fig.3.2)

Fig. 3.2 a) Verificación de nombre de red oculto



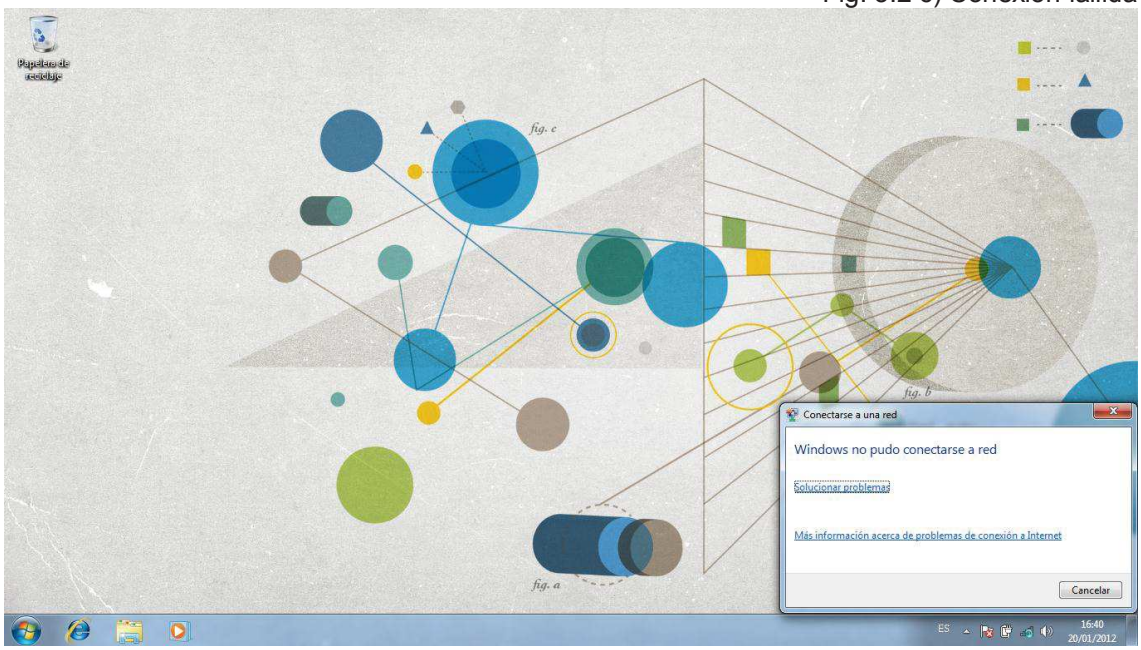
Fuente: Autor

Fig. 3.2 b) Intento de conexión



Fuente: Autor

Fig. 3.2 c) Conexión fallida



Fuente: Autor

3.1.4. Verificación y análisis de seguridad de la infraestructura de servidores

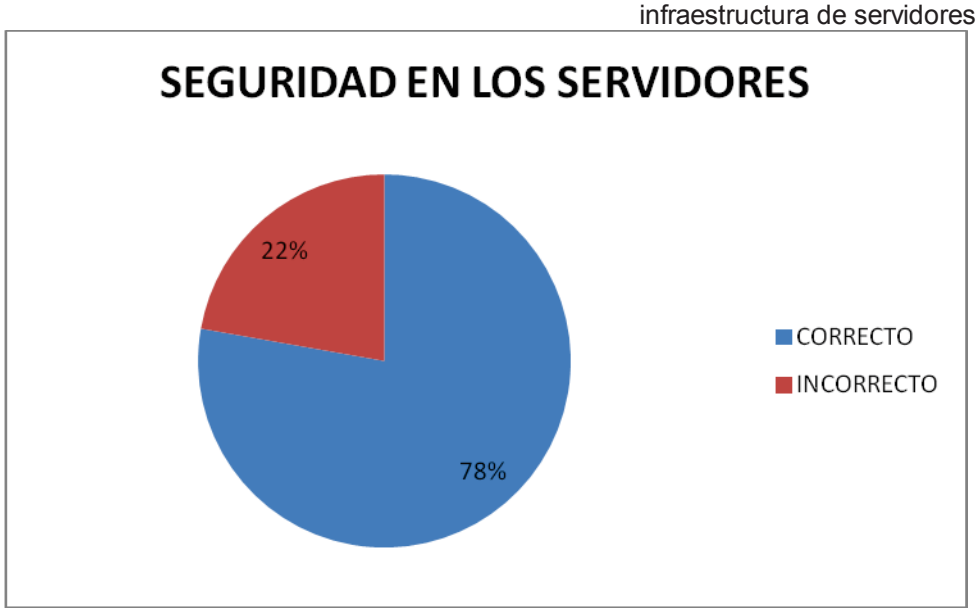
Para la tabulación de resultados se realizará la valoración basada en los resultados obtenidos de las pruebas realizadas (correcto o incorrecto). (Tabla 3.4)

Tabla 3.4 Verificación y análisis de seguridad de la infraestructura de servidores

SERVIDOR	VERIFICACION / PRUEBA	RESULTADO	
		CORRECTO	INCORRECTO
Servidor DNS	Resolución de nombres de dominio (Fig. 3.6)	✓	
Firewall	Escaneo de puertos (Fig. 3.7)	✓	
Servidor de correo	Verificación de listas negras (Fig. 3.8)	✓	
	Prueba de Open relay (Fig. 3.9)	✓	
	Verificación de sistema antispam (Fig. 3.10)	✓	
Servidor de DHCP	Estado del servicio (Fig. 3.11)	✓	
	Un único segmento de red para servidores y clientes		✓
Servidor de actualizaciones	Estado de las actualizaciones (Fig. 3.12)	✓	
Sistema de copias de seguridad	Estado de las tareas de copias de seguridad (Fig. 3.13)		✓

Fuente: Autor

Gráfico 3.4 Tabulación de resultados de verificación y análisis de seguridad de la infraestructura de servidores

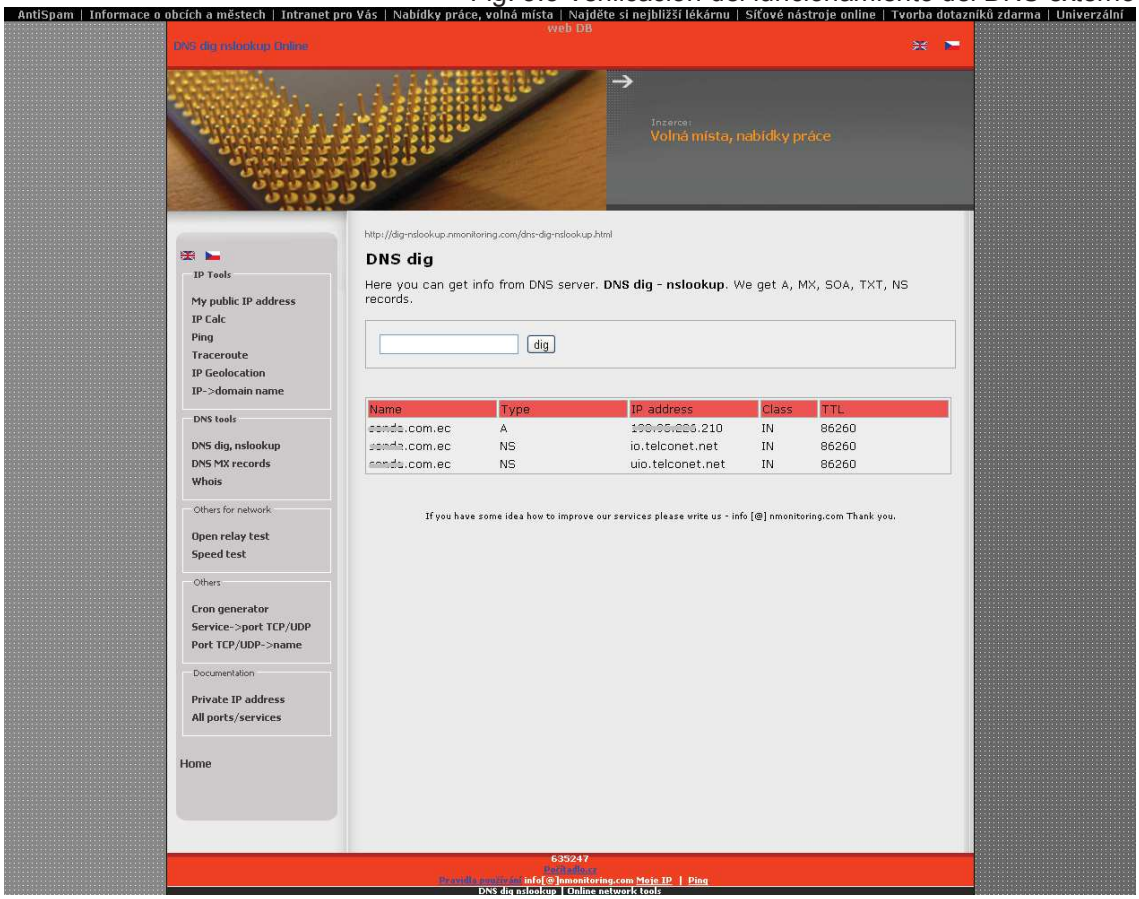


Fuente: Autor

Observaciones

- **Prueba de funcionamiento del servidor de DNS.-** Las pruebas demuestran que la dirección IP pública y el nombre de dominio se resuelven de forma correcta. (Fig. 3.3)

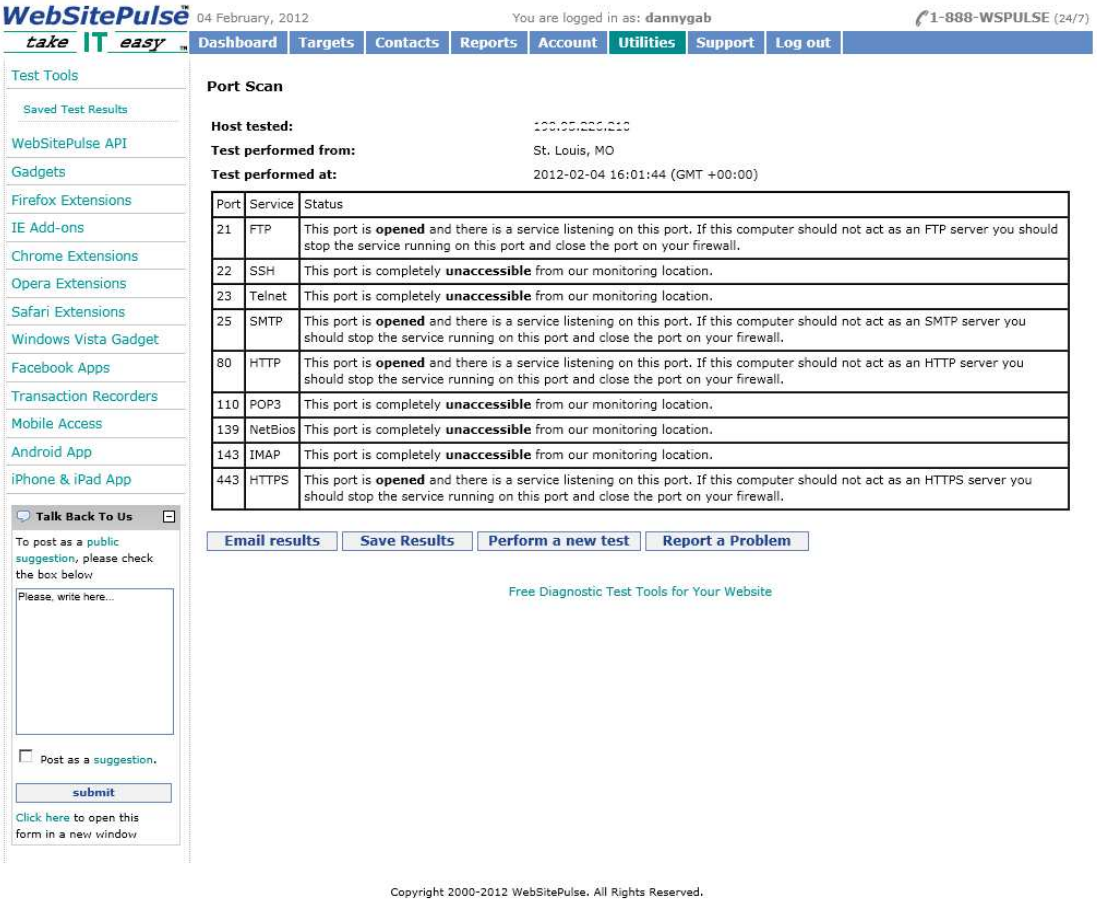
Fig. 3.3 Verificación del funcionamiento del DNS externo



Fuente: http://dig-nslookup.nmonitoring.com/dns-dig-nslookup.html

- **Prueba de funcionamiento del firewall.-** Se realiza un escaneo de puertos del firewall, como resultado de la prueba se observa que el equipo tiene puertos abiertos (21, 25, 80, 443), para proveer de servicios a los usuarios. (Fig. 3.4)

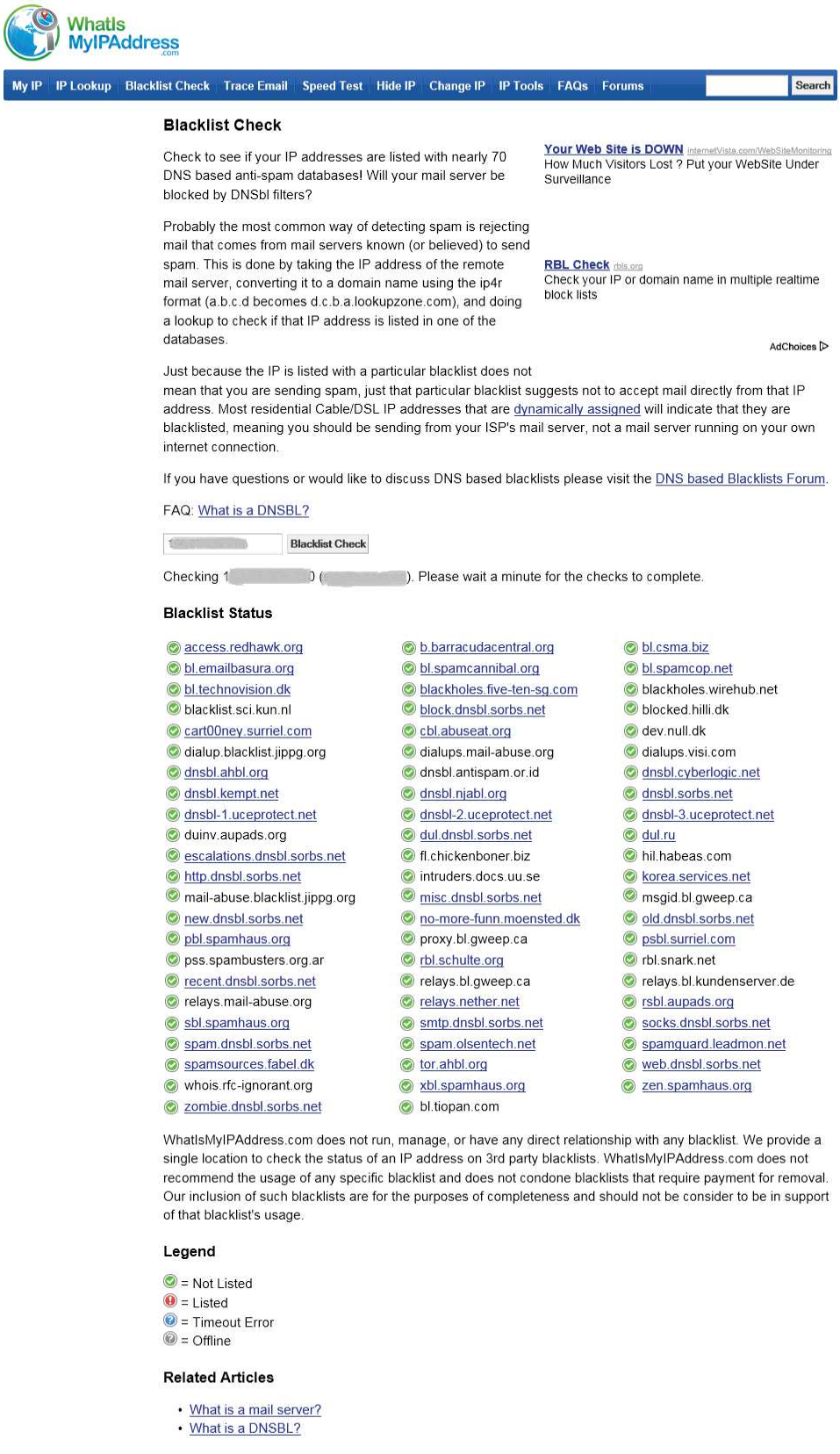
Fig. 3.4 Escaneo de puertos



Fuente: www.websitepulse.com

- **Prueba de funcionamiento del servidor de correo.-** Se verifica que la dirección IP pública no se encuentra en listas negras de envío de spam (Blacklist). (Fig. 3.5)

Fig. 3.5 Verificación de servidor de correo en listas negras



WhatIsMyIPAddress.com

My IP | IP Lookup | Blacklist Check | Trace Email | Speed Test | Hide IP | Change IP | IP Tools | FAQs | Forums | Search

Blacklist Check

Check to see if your IP addresses are listed with nearly 70 DNS based anti-spam databases! Will your mail server be blocked by DNSbl filters?

Probably the most common way of detecting spam is rejecting mail that comes from mail servers known (or believed) to send spam. This is done by taking the IP address of the remote mail server, converting it to a domain name using the ip4r format (a.b.c.d becomes d.c.b.a.lookupzone.com), and doing a lookup to check if that IP address is listed in one of the databases.

Just because the IP is listed with a particular blacklist does not mean that you are sending spam, just that particular blacklist suggests not to accept mail directly from that IP address. Most residential Cable/DSL IP addresses that are dynamically assigned will indicate that they are blacklisted, meaning you should be sending from your ISP's mail server, not a mail server running on your own internet connection.

If you have questions or would like to discuss DNS based blacklists please visit the DNS based Blacklists Forum.

FAQ: What is a DNSBL?

[redacted] Blacklist Check

Checking 1[redacted]0 ([redacted]). Please wait a minute for the checks to complete.

Blacklist Status

access.redhawk.org	b.barracudacentral.org	bl.csma.biz
bl.emailbasura.org	bl.spamcannibal.org	bl.spamcop.net
bl.technovision.dk	blackholes.five-ten-sg.com	blackholes.wirehub.net
blacklist.sci.kun.nl	block.dnsbl.sorbs.net	blocked.hilli.dk
cart00ney.surriel.com	cbl.abuseat.org	dev.null.dk
dialup.blacklist.jippg.org	dialups.mail-abuse.org	dialups.visi.com
dnsbl.ahbl.org	dnsbl.antispam.or.id	dnsbl.cyberlogic.net
dnsbl.kempt.net	dnsbl.njabl.org	dnsbl.sorbs.net
dnsbl-1.uceprotect.net	dnsbl-2.uceprotect.net	dnsbl-3.uceprotect.net
duinv.aupads.org	dul.dnsbl.sorbs.net	dul.ru
escalations.dnsbl.sorbs.net	fl.chickenboner.biz	hil.habeas.com
http.dnsbl.sorbs.net	intruders.docs.uu.se	korea.services.net
mail-abuse.blacklist.jippg.org	misc.dnsbl.sorbs.net	msgid.bl.gweep.ca
new.dnsbl.sorbs.net	no-more-funn.moensted.dk	old.dnsbl.sorbs.net
pbl.spamhaus.org	proxy.bl.gweep.ca	psbl.surriel.com
pss.spambusters.org.ar	rbl.schulte.org	rbl.snark.net
recent.dnsbl.sorbs.net	relays.bl.gweep.ca	relays.bl.kundenserver.de
relays.mail-abuse.org	relays.nether.net	rsbl.aupads.org
sbl.spamhaus.org	smtp.dnsbl.sorbs.net	socks.dnsbl.sorbs.net
spam.dnsbl.sorbs.net	spam.olsentech.net	spamguard.leadmon.net
spamsources.fabel.dk	tor.ahbl.org	web.dnsbl.sorbs.net
whois.rfc-ignorant.org	xbl.spamhaus.org	zen.spamhaus.org
zombie.dnsbl.sorbs.net	bl.tiopan.com	

WhatIsMyIPAddress.com does not run, manage, or have any direct relationship with any blacklist. We provide a single location to check the status of an IP address on 3rd party blacklists. WhatIsMyIPAddress.com does not recommend the usage of any specific blacklist and does not condone blacklists that require payment for removal. Our inclusion of such blacklists are for the purposes of completeness and should not be consider to be in support of that blacklist's usage.

Legend

= Not Listed
= Listed
= Timeout Error
= Offline

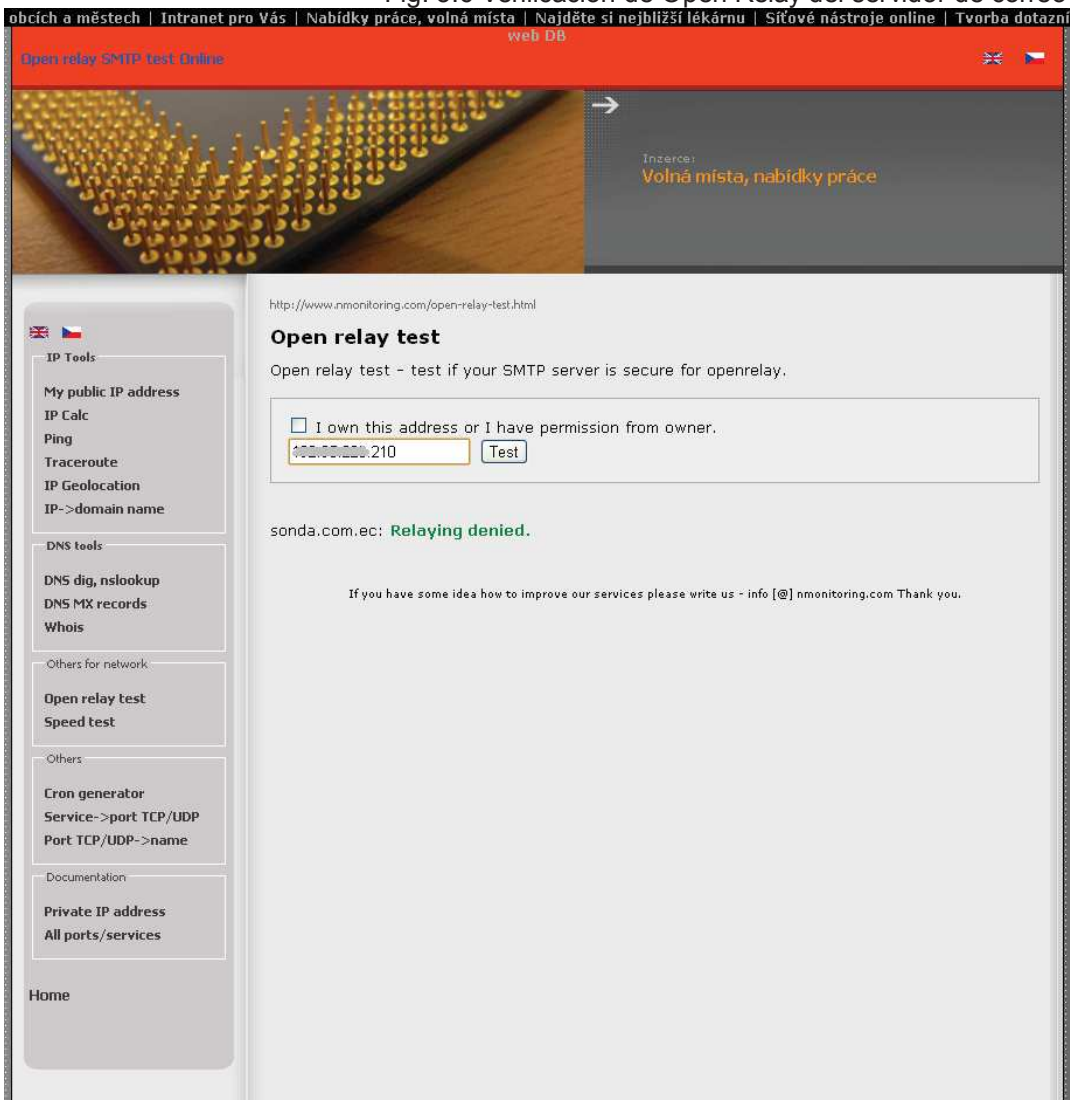
Related Articles

- What is a mail server?
- What is a DNSBL?

Fuente: http://whatismyipaddress.com/blacklist-check

- **Prueba de open relay.-** Se realiza una prueba de reenvío de correo electrónico no deseado. Los resultados demuestran que el servidor no reenvía correo basura. (Fig. 3.6)

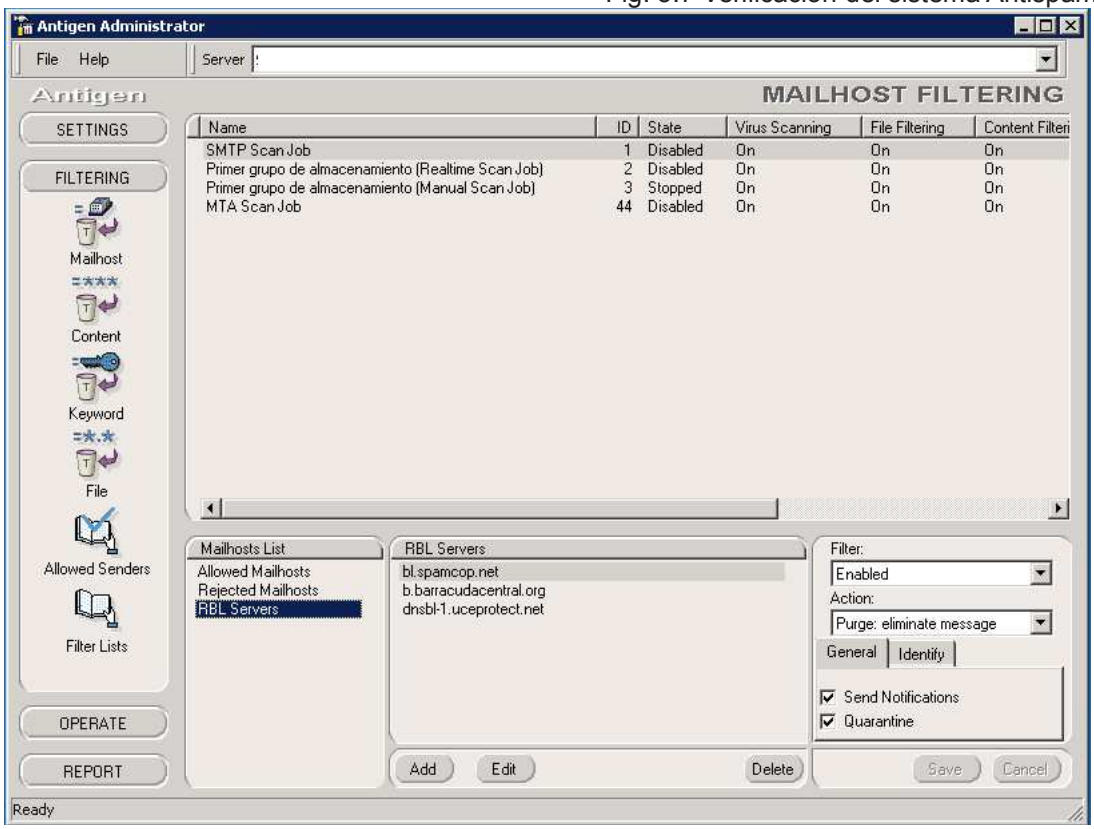
Fig. 3.6 Verificación de Open Relay del servidor de correo



Fuente: http://www.nmonitoring.com/open-relay-test.html

- **Prueba de AntiSpam.-** Se verifica la utilización de listas negras en el servidor AntiSpam Antigen de Microsoft. (Fig. 3.7)

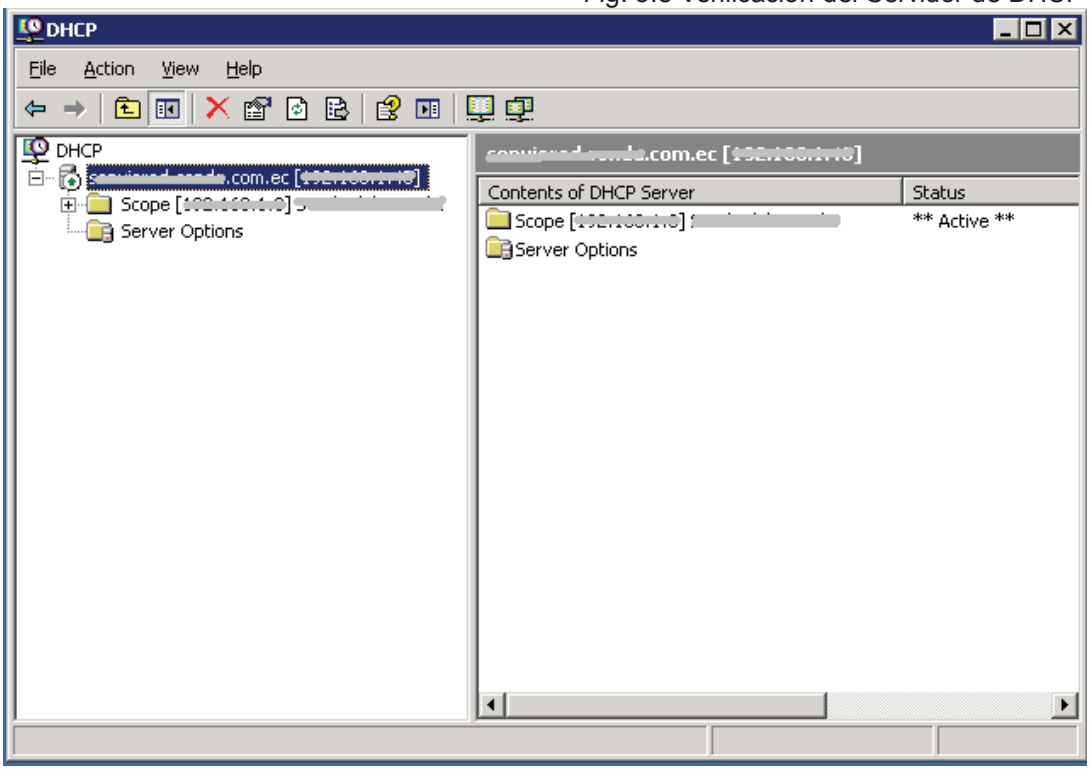
Fig. 3.7 Verificación del sistema Antispam



Fuente: Autor

- **Verificación del funcionamiento del servidor de DHCP.-** Se realiza la captura demuestra que el servicio se encuentra funcionando correctamente. (Fig. 3.8)

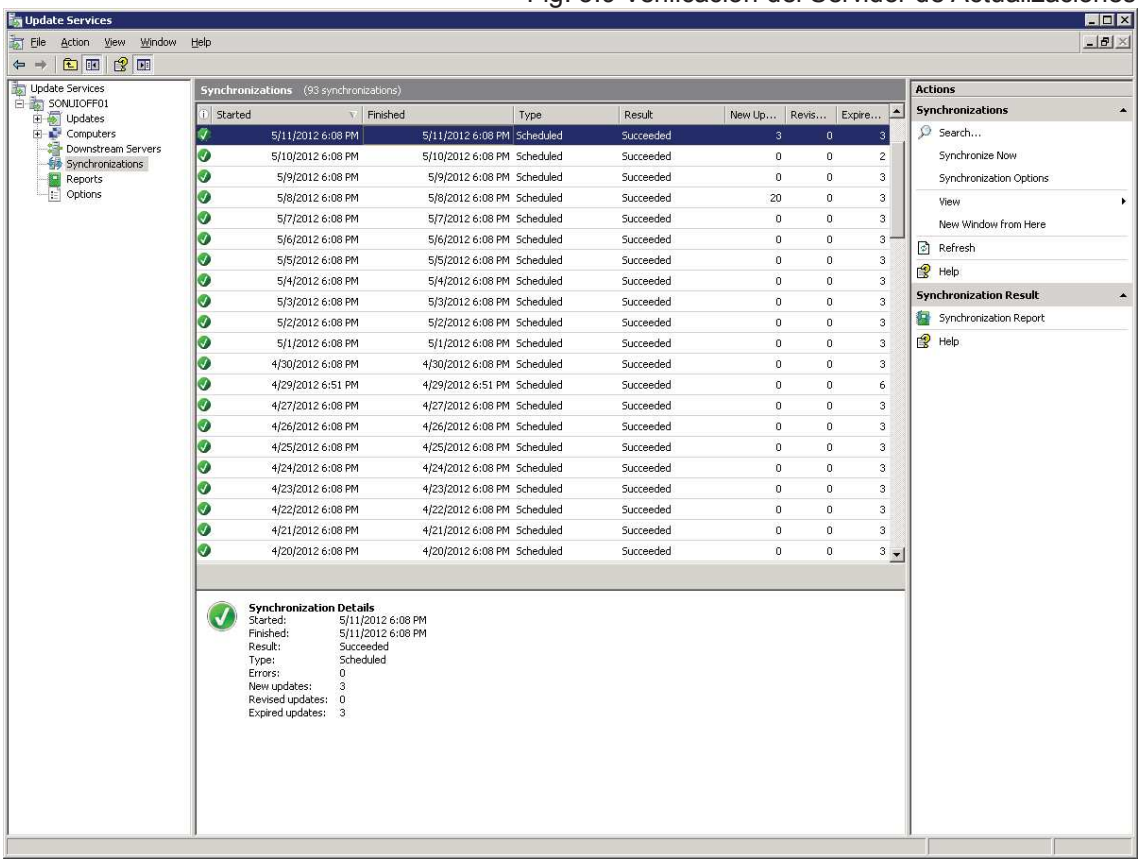
Fig. 3.8 Verificación del Servidor de DHCP



Fuente: Autor

- **Verificación del funcionamiento del servidor de actualizaciones.-** Se realiza la captura que demuestra la sincronización de actualizaciones diarias. (Fig. 3.9)

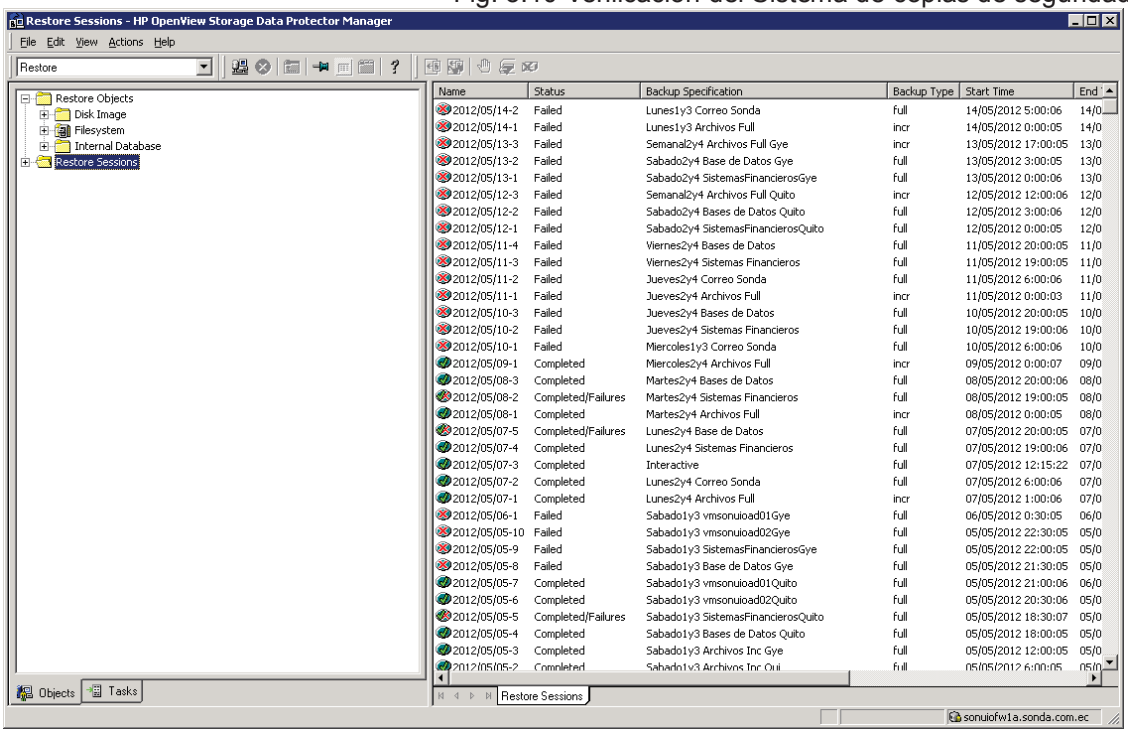
Fig. 3.9 Verificación del Servidor de Actualizaciones



Fuente: Autor

- **Verificación del funcionamiento del sistema de copias de seguridad.-** Se realiza la captura de pantalla de HP Data Protector, la misma muestra tareas fallidas o incompletas. (Fig. 3.10)

Fig. 3.10 Verificación del Sistema de copias de seguridad



Fuente: Autor

3.1.5. Verificación y análisis de seguridad de las estaciones de trabajo y políticas de acceso a recursos de red

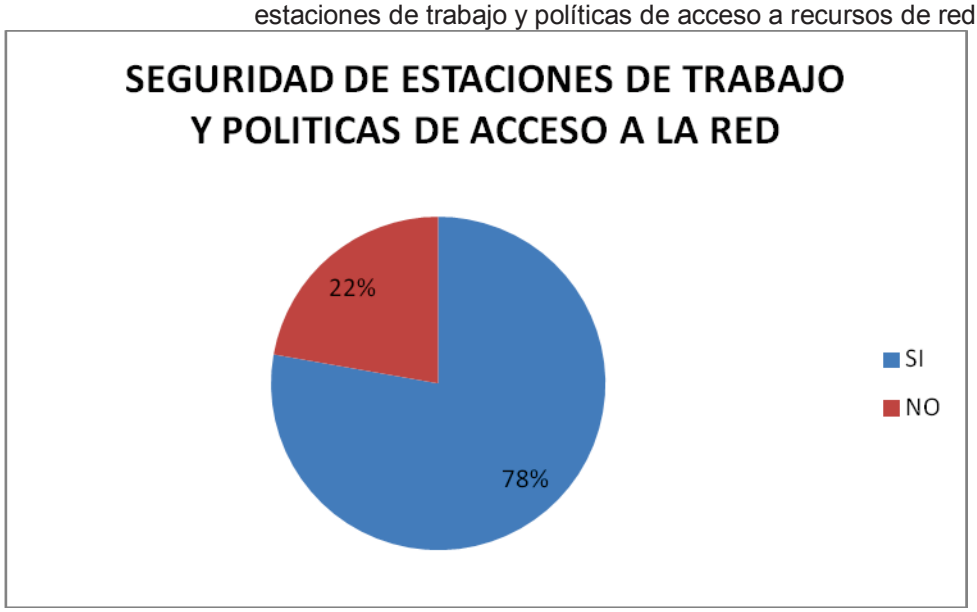
Para la tabulación de resultados se realizará una valoración de SI o NO dependiendo de la característica y la información recopilada durante el levantamiento de información. (Tabla 3.5)

Tabla 3.5 Verificación y análisis de seguridad de las estaciones de trabajo y políticas de acceso a recursos de red

VERIFICACION	**RESULTADO**	
	SI	**NO**
Software utilizado tiene licencia	✓	
Equipos y usuarios se administran por medio de directorio activo (Anexo 2)	✓	
Usuarios tienen derechos de administrador de equipos	✓	
Se realizan respaldos de datos de equipos de usuarios		✓
Existen políticas de renovación de contraseñas (Anexo 2)	✓	
Los clientes navegan a través de proxy (Fig. 3.14)	✓	
Antivirus se actualiza de forma automática (Fig. 3.15)	✓	
Funcionamiento efectivo del antivirus en correo electrónico (Fig. 3.16)		✓
Existen políticas de archivos compartidos (Fig. 3.17)	✓	

Fuente: Autor

Grafico 3.5 Tabulación de resultados de verificación y análisis de seguridad de las estaciones de trabajo y políticas de acceso a recursos de red

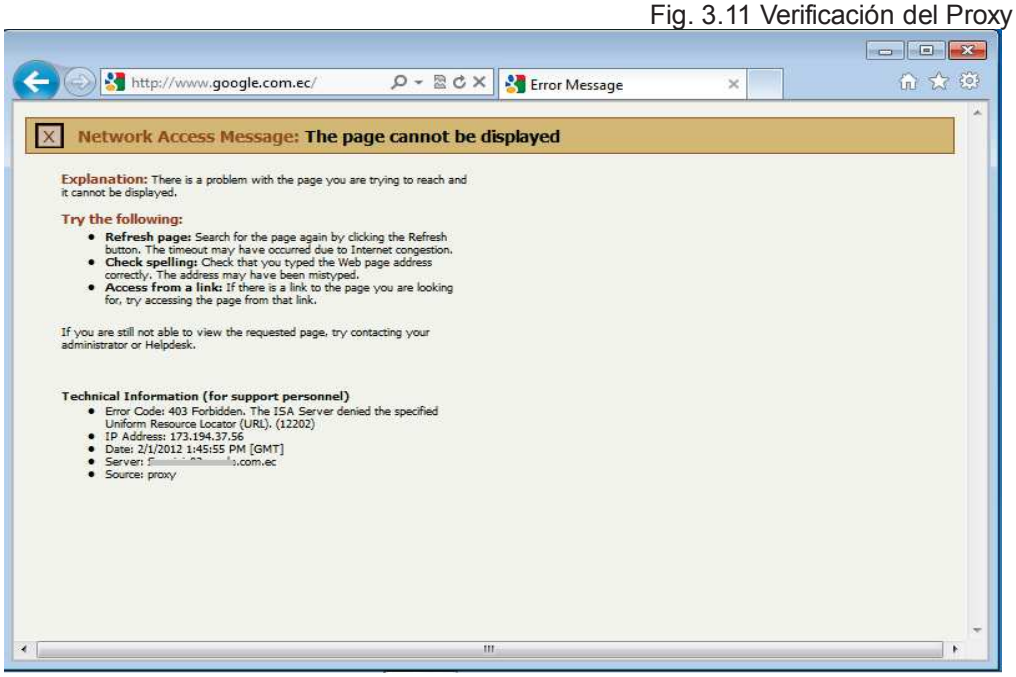


Fuente: Autor

Observaciones

- Las licencias de software de administran desde matriz hacia las filiales.
- **Verificación del funcionamiento del proxy.-** Se conecta un equipo que no pertenece a la red corporativa, y se intenta navegar en internet, la navegación se bloquea por medio del servidor proxy. (Fig. 3.11)

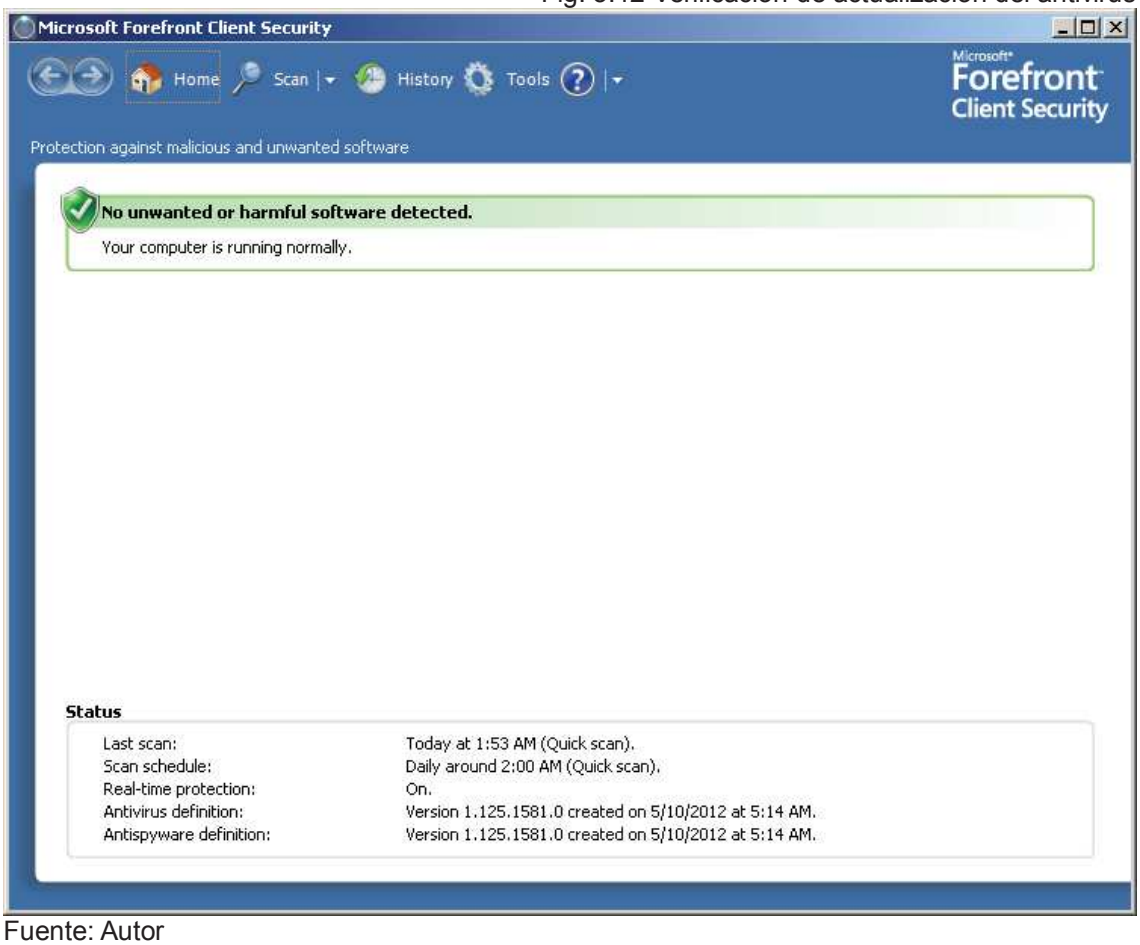
Fig. 3.11 Verificación del Proxy



Fuente: Autor

- **Verificación de actualización del antivirus.-** Se realiza una captura de pantalla que evidencia la actualización de la base de firmas de antivirus en uno de los equipos clientes. (Fig. 3.12)

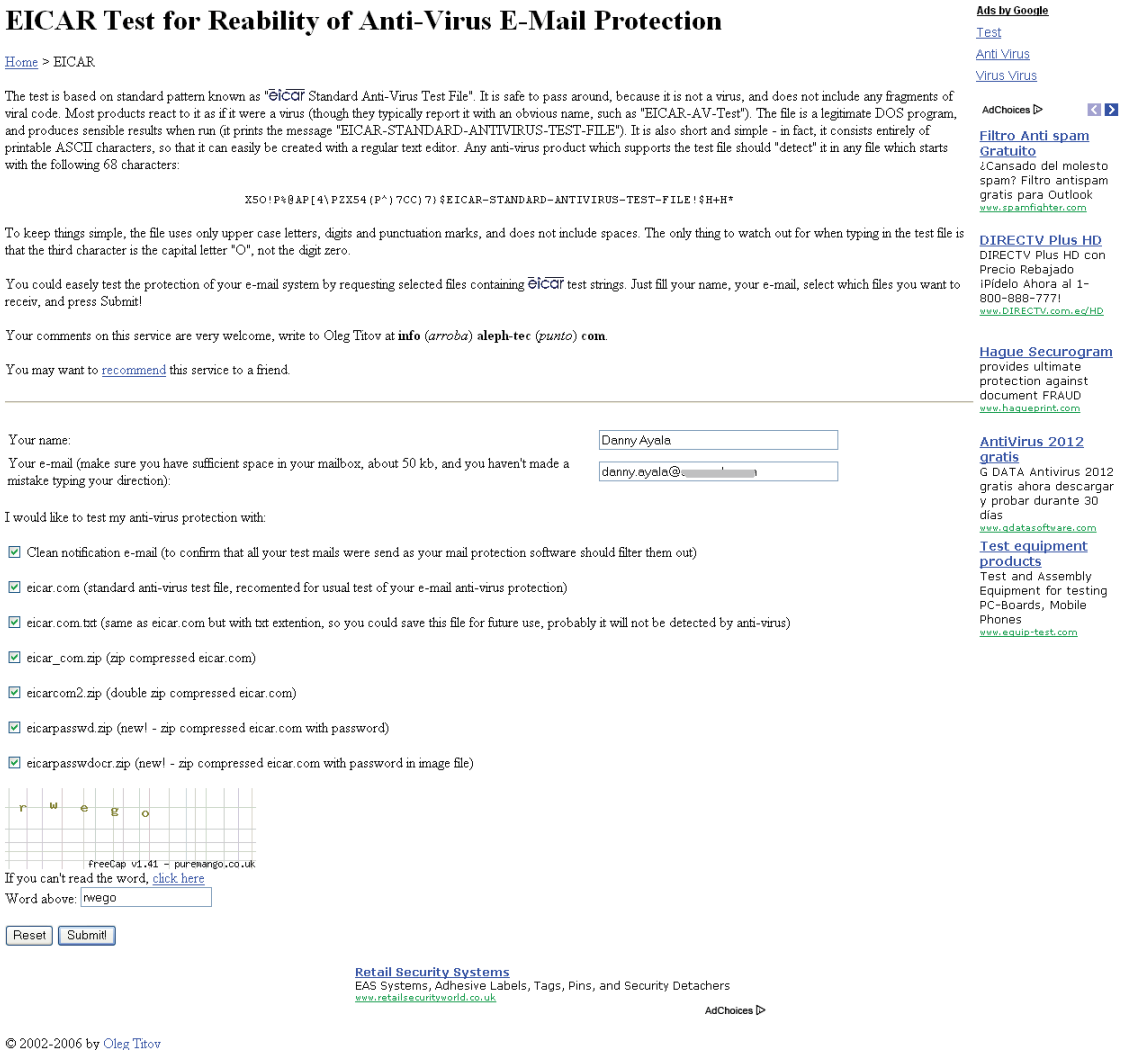
Fig. 3.12 Verificación de actualización del antivirus



Fuente: Autor

- **Verificación del funcionamiento del antivirus.-** Se realizan pruebas en una estación de trabajo, para lo cual se envía desde internet archivos de prueba al correo electrónico del usuario del equipo. (Fig. 3.13)

Fig. 3.13 a) Envío del test para antivirus



EICAR Test for Reability of Anti-Virus E-Mail Protection

Home > EICAR

The test is based on standard pattern known as "eicar Standard Anti-Virus Test File". It is safe to pass around, because it is not a virus, and does not include any fragments of viral code. Most products react to it as if it were a virus (though they typically report it with an obvious name, such as "EICAR-AV-Test"). The file is a legitimate DOS program, and produces sensible results when run (it prints the message "EICAR-STANDARD-ANTIVIRUS-TEST-FILE"). It is also short and simple - in fact, it consists entirely of printable ASCII characters, so that it can easily be created with a regular text editor. Any anti-virus product which supports the test file should "detect" it in any file which starts with the following 68 characters:

X5O!P%@AP[4\PZX54(P^)7CC)7)$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

To keep things simple, the file uses only upper case letters, digits and punctuation marks, and does not include spaces. The only thing to watch out for when typing in the test file is that the third character is the capital letter "O", not the digit zero.

You could easely test the protection of your e-mail system by requesting selected files containing eicar test strings. Just fill your name, your e-mail, select which files you want to receiv, and press Submit!

Your comments on this service are very welcome, write to Oleg Titov at **info** (*arroba*) **aleph-tec** (*punto*) **com**.

You may want to recommend this service to a friend.

Your name: Danny Ayala

Your e-mail (make sure you have sufficient space in your mailbox, about 50 kb, and you haven't made a mistake typing your direction): danny.ayala@

I would like to test my anti-virus protection with:

- Clean notification e-mail (to confirm that all your test mails were send as your mail protection software should filter them out)
- eicar.com (standard anti-virus test file, recomented for usual test of your e-mail anti-virus protection)
- eicar.com.txt (same as eicar.com but with txt extention, so you could save this file for future use, probably it will not be detected by anti-virus)
- eicar_com.zip (zip compressed eicar.com)
- eicarcom2.zip (double zip compressed eicar.com)
- eicarpasswd.zip (new! - zip compressed eicar.com with password)
- eicarpasswdocr.zip (new! - zip compressed eicar.com with password in image file)

rwego

FreeCap v1.41 - puremango.co.uk

If you can't read the word, click here

Word above: rwego

Reset Submit!

Retail Security Systems
EAS Systems, Adhesive Labels, Tags, Pins, and Security Detachers
www.retailsecurityworld.co.uk

AdChoices

© 2002-2006 by Oleg Titov

Ads by Google

Test

Anti Virus

Virus Virus

AdChoices

Filtro Anti spam Gratuito
¿Cansado del molesto spam? Filtro antispam gratis para Outlook
www.spamfighter.com

DIRECTV Plus HD
DIRECTV Plus HD con Precio Rebajado ¡Pídelo Ahora al 1-800-888-777!
www.DIRECTV.com.ec/HD

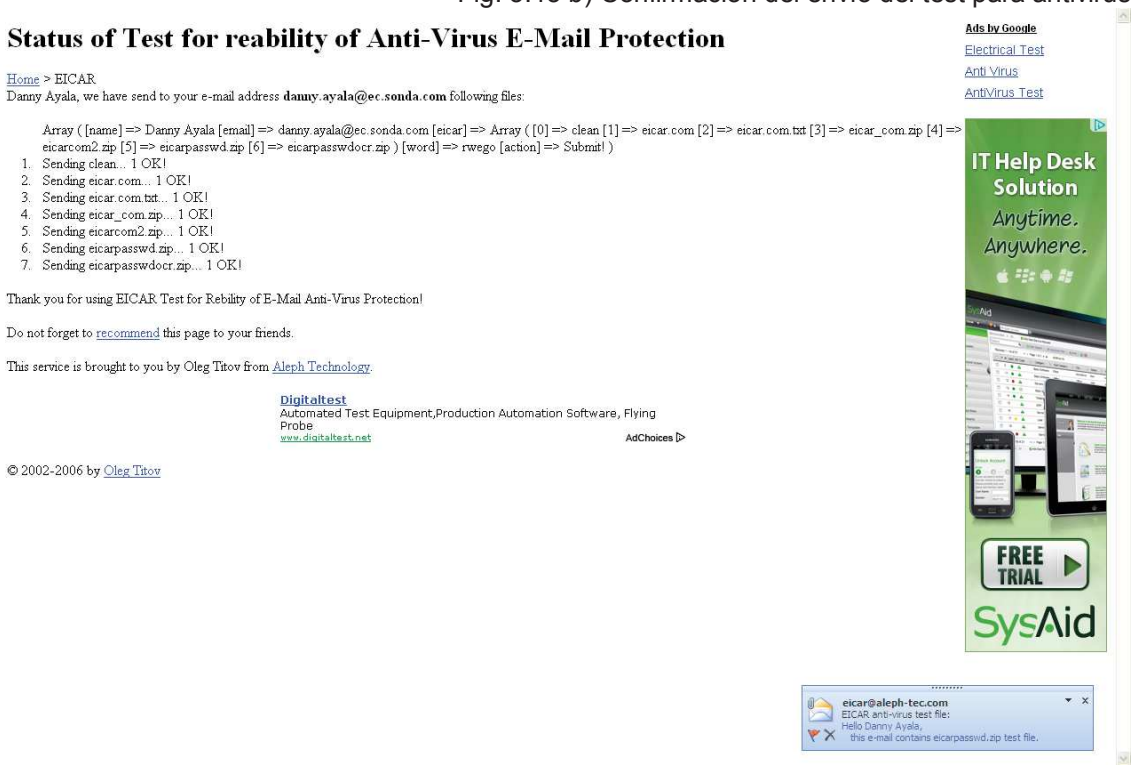
Hague Securogram
provides ultimate protection against document FRAUD
www.hagueprint.com

AntiVirus 2012 gratis
G DATA Antivirus 2012 gratis ahora descargar y probar durante 30 días
www.gdatasoftware.com

Test equipment products
Test and Assembly Equipment for testing PC-Boards, Mobile Phones
www.equip-test.com

Fuente: http://www.aleph-tec.com/eicar/index.php

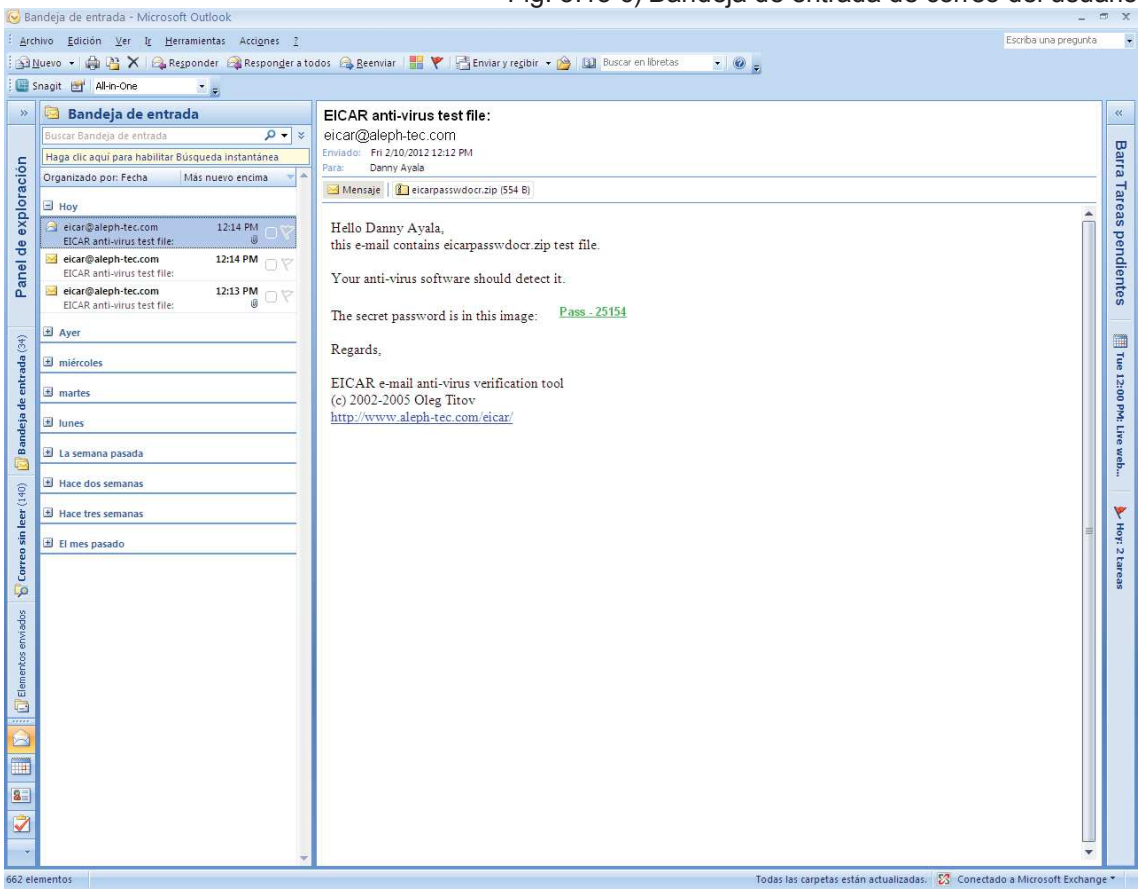
Fig. 3.13 b) Confirmación del envío del test para antivirus



Fuente: http://www.aleph-tec.com/eicar/index.php

- En la bandeja de entrada se reciben algunos archivos sospechosos.

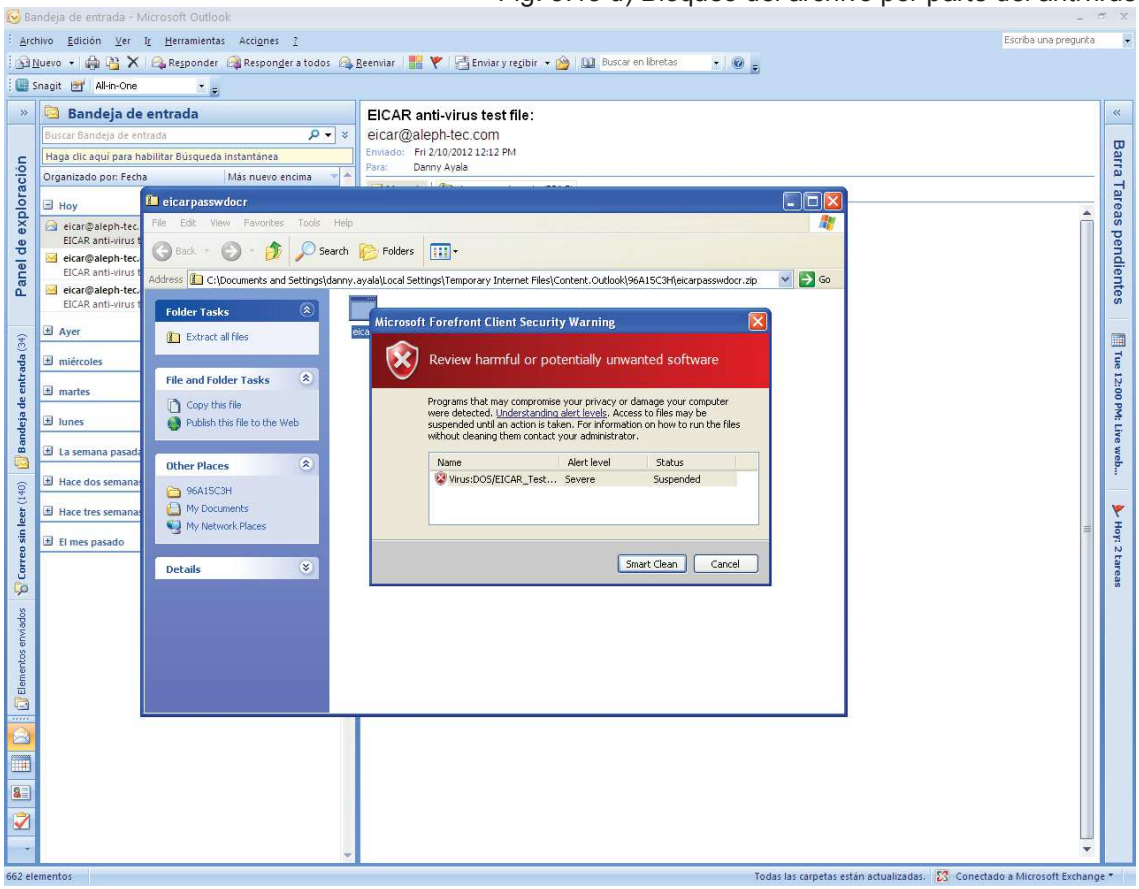
Fig. 3.13 c) Bandeja de entrada de correo del usuario



Fuente: Autor

- Se realiza una verificación para lo cual se intenta ejecutar los archivos de test recibidos, el antivirus los reconoce como archivos sospechosos y los bloquea.

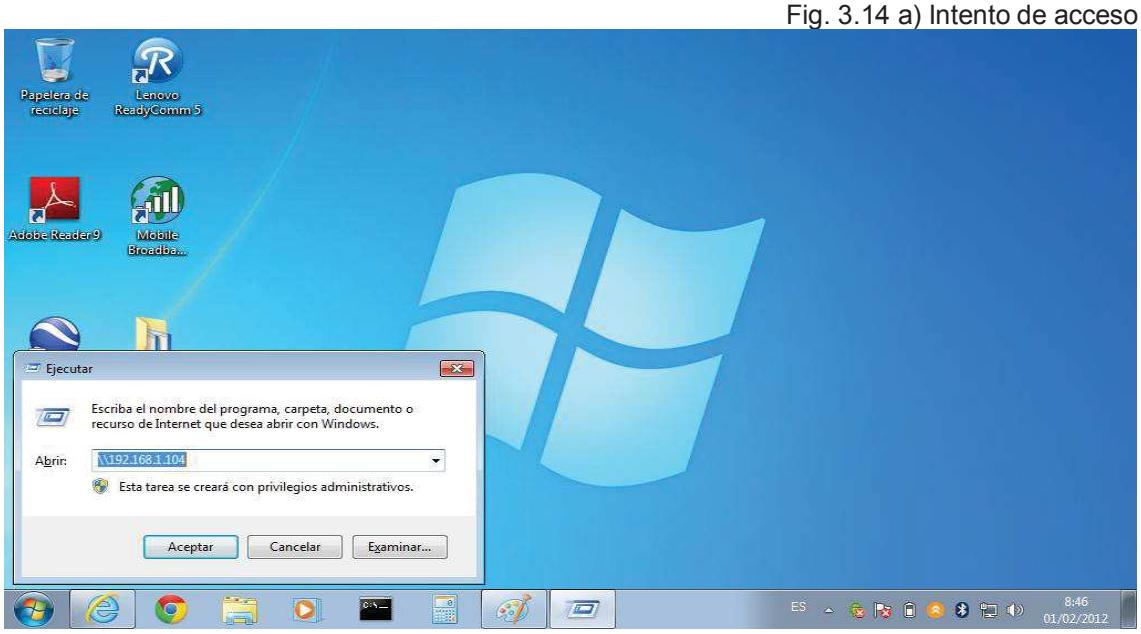
Fig. 3.13 d) Bloqueo del archivo por parte del antivirus



Fuente: Autor

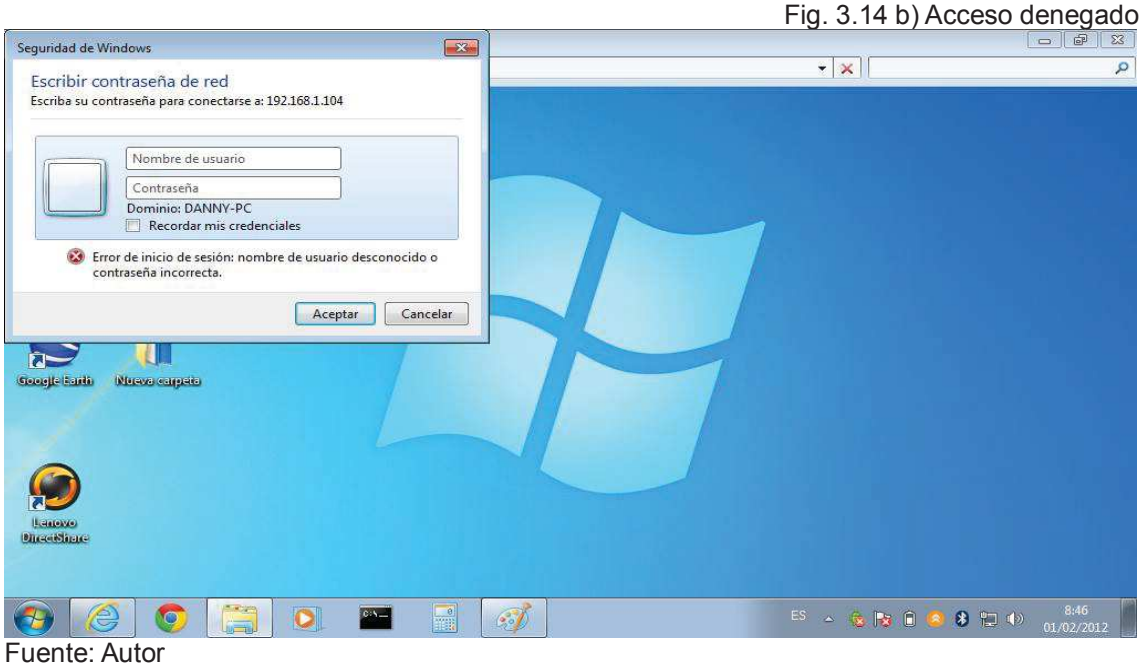
- **Verificación del funcionamiento de las políticas de compartición de archivos.-** Se realiza obtiene una captura de pantalla que evidencia el acceso a carpetas compartidas en un determinado cliente desde un computador que no pertenece a la red, el acceso no se concede. (Fig. 3.14)

Fig. 3.14 a) Intento de acceso



Fuente: Autor

Fig. 3.14 b) Acceso denegado



Fuente: Autor

3.2. Informe de auditoría

Una vez realizada la verificación y análisis de los sistemas de seguridad se elabora el respectivo informe para ser presentado a los administradores de la infraestructura de la organización.

INFORME DE AUDITORIA DE SEGURIDAD INFORMÁTICA INTERNA Y PERIMETRAL DE LA FILIAL EN ECUADOR DE UNA EMPRESA MULTINACIONAL

Como resultado de la verificación y análisis de los sistemas de seguridad informática de la filial en Ecuador de una empresa multinacional, se encontraron las siguientes oportunidades de mejora:

CENTRO DE DATOS Y CABLEADO ESTRUCTURADO

Listado de verificación:

	0% – 20% NO CUMPLE	21% - 40% MINIMO	41% - 60% REGULAR	61% - 80% BUENA	81% - 100% EXCELENTE
Centro de datos			✓		
Cableado estructurado y comunicaciones				✓	

Observaciones:

- El centro de datos no cuenta con controles ambientales adecuados para asegurar el continuo funcionamiento de los equipos.
- El centro de datos no tiene instalado piso antiestático para prevenir descargas electroestáticas.
- La organización de los cables de red en el rack de comunicaciones es

deficiente como consecuencia de que todos los puntos de red confluyen hacia él.

Riesgos:

- Interrupción de las operaciones.
- Daños en los equipos debido a descargas electroestáticas.
- Complejidad de identificación de fallas de comunicaciones para las estaciones de trabajo.

Recomendaciones:

- Implementar controles ambientales adecuados para centros de cómputo.
- Instalar piso flotante antiestático en el centro de datos.
- Descongestionar el rack de comunicaciones principal implementando gabinetes o racks en cada uno de los pisos de la entidad.

RED INALAMBRICA

Listado de verificación:

	0% – 20% NO CUMPLE	**21% - 40% MINIMO**	**41% - 60% REGULAR**	**61% - 80% BUENA**	**81% - 100% EXCELENTE**
Red inalámbrica				✓	

Observaciones:

- El sistema de cifrado WEP posee vulnerabilidades.

Riesgos:

- Conexiones no autorizadas a la red inalámbrica.

- Pérdida o robo de información.

Recomendaciones:

- Implementar un sistema de cifrado más robusto como WPA-2, o un servidor de autenticación.
- Implementar un sistema de prevención de intrusos.

INFRAESTRUCTURA DE SERVIDORES

Listado de verificación:

	0% – 20% NO CUMPLE	21% - 40% MINIMO	41% - 60% REGULAR	61% - 80% BUENA	81% - 100% EXCELENTE
Servidores				✓	

Observaciones:

- Se encontraron puertos abiertos en el firewall.
- Una sola VLAN para servidores y clientes
- Errores en la realización de las copias de seguridad.

Riesgos:

- Ataques hacia los servidores e interrupción de las operaciones.
- No existe escalabilidad de la red.
- Pérdida de información.

Recomendaciones:

- Reforzar la seguridad del firewall cerrando puertos que están abiertos de forma innecesaria.

- Implementar direccionamientos de red independientes para servidores y clientes de red.

- Llevar registros y seguimiento de las copias de seguridad.

ESTACIONES DE TRABAJO Y POLITICAS DE ACCESO A LA RED

Listado de verificación:

	0% – 20% NO CUMPLE	**21% - 40% MINIMO**	**41% - 60% REGULAR**	**61% - 80% BUENA**	**81% - 100% EXCELENTE**
Estaciones de trabajo y políticas de acceso a la red				✓	

Observaciones:

- El 74,4% de los usuarios posee permisos de administración local de su respectivo equipo.

- Llegada de correo con archivos adjuntos sospechosos a la bandeja de entrada de los usuarios.

Riesgos:

- Intrusiones de programas maliciosos instalados por los usuarios.

- Pérdida o robo de información personal o de la institución.

Recomendaciones:

- Reforzar o redefinir políticas de uso de los equipos y de derechos de administración de los mismos.

- Evaluar la posibilidad de reemplazar el antivirus en los clientes de la red.

CAPITULO IV
CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- La seguridad informática no debe ser abordada únicamente desde el punto de vista técnico o tecnológico, también el factor humano es determinante a la hora de establecer políticas o normas de tal forma que exista un compromiso real de colaboración entre todos los involucrados en la protección de la información y buen uso de los recursos informáticos.

- No existe una metodología única para realizar auditorías en el campo informático, sino que el éxito y veracidad de la misma se encuentra muy ligada a los conocimientos y experiencia del profesional que la realiza.

- La continua evolución de las redes de telecomunicaciones obliga a permanecer en constante actualización tanto de los sistemas como de los recursos humanos que intervienen en su operación.

- Existen varios sistemas de seguridad tanto de infraestructuras tecnológicas, como de información pero no se tiene establecida una norma general para obtener tal objetivo, por lo cual se debe tener claro que es lo que se debe proteger y cuál es la metodología más adecuada para lograrlo.

4.2. Recomendaciones

- Se recomienda realizar una evaluación periódica e integral de los sistemas de seguridad informática con el fin de determinar la efectividad de los mismos, y la vigencia de los procedimientos.

- Se recomienda la colocación de un switch en cada piso para

descongestionar el centro de datos y optimizar la administración y resolución de problemas de puntos de red.

- Es necesario actualizar el sistema de cifrado de la red inalámbrica ya que el utilizado actualmente puede ser vulnerado y se corre el riesgo de pérdida o robo de información.

- Se recomienda implementar un sistema de prevención de intrusos para reforzar las políticas que ya se encuentran establecidas.

REFERENCIAS

- Arias, J y Iliguicota, B. (2007), *POLITICAS DE AUDITORIA DE SEGURIDADES EN REDES LOCALES*, Recuperado el 30 de abril del 2012 de http://bibdigital.epn.edu.ec/bitstream/15000/140/1/CD-0548.pdf

- CISCO (2012), http://www.cisco.com

- D-link (2012), ftp://ftp.dlink.ru

- EICAR Test for Reability of Anti_Virus E-Mail Protection (2012), http://www.aleph-tec.com/eicar/index.php

- HP Business Support Center (2012), http://bizsupport2.austin.hp.com

- Online network tools (2012), http://www.nmonitoring.com

- Parreño, S. y Suntaxi, G. (2010), *AUDITORIA DE LA SEGURIDAD DE LA INFORMACION DE LA EMPRESA TRANSPORTES NOROCCIDENTAL* Recuperado el 30 de abril del 2012 de http://bibdigital.epn.edu.ec/bitstream/15000/2236/1/CD-3005.pdf

- Piattini, Mario y Emilio del Peso. (2001) Auditoría Informática. Un enfoque práctico, (2da ed.) Mexico D.F., Mexico: Editorial Alfaomega RA-MA.

- Universidad de Belgrano (2012), METODOLOGIA DE AUDITORIA INFORMATICA, Recuperado el 30 de abril del 2012 de http://www.ub.edu.ar/catedras/ingenieria/auditoria/tpmetodo/tpmetodo2.htm

- Website Monitoring & Web Server Monitoring Service by WebSitePulse (2012), http://www.websitepulse.com

- What is my IP address (2012), http://whatismyipaddress.com

- Wi-Fi Wireless LAN (2012), http://wi-fi.unas.cz
- Wikilibros(2012), *SEGURIDAD INFORMATICA*, Recuperado el 9 de abril del 2012 de http://es.wikibooks.org/wiki/Seguridad_informatica/Vulnerabilidad

ANEXOS

Anexo 1.

Extracto de documentación técnica de los equipos de comunicaciones

- **Router Cisco 1800 Series**

Tomado de: Guía rápida de los routers de la serie Cisco 1800 de servicios integrados (modulares) Pag.22

Configuración inicial mediante CLI de Cisco: configuración manual

En esta sección se muestra cómo ver un símbolo de sistema de la interfaz de línea de comandos (CLI) para configurar mediante CLI y cómo obtener documentación para configurar CLI. Puede usar CLI si los mensajes siguientes aparecen al final de la secuencia de inicio:

```
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Would you like to enter the initial configuration dialog? [yes/no]:
```

Si estos mensajes no aparecen, significa que en fábrica se instaló SDM en el router, así como un archivo de configuración predeterminado. Para usar SDM para configurar el router, consulte el documento "Configuración inicial mediante router Cisco y Security Device Manager" de la página 19.

Si necesita ayuda acerca de la numeración de interfaces y puertos, consulte la sección "Numeración de interfaces" de la página 18.

Paso 1 Para seguir adelante con la configuración manual mediante CLI, escriba **no** cuando dejen de aparecer los mensajes de encendido:

```
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Paso 2 Presione **Retorno** para terminar la instalación automática y seguir con la configuración manual:

```
Would you like to terminate autoinstall? [yes] (si) Retorno
```

Aparecerán varios mensajes que terminan con una línea similar a la siguiente:

```
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled <fecha> <hora> by <persona>
```

Paso 3 Presione **Retorno** para ver el símbolo de sistema `Router>`.

```
...
flashfs[4]: Initialization complete.
Router>
```

Fuente: CISCO (2012), Recuperado el 18 de abril del 2012 de http://www.cisco.com/en/US/docs/routers/access/1800/1841/hardware/quick/guide/spanish/qsg18esp.pdf

- **Switch 3Com 3824**

Tomado de: SuperStack® 3 Switch 3812, Switch 3824, and Switch 3848 Getting Started Guide Pag.44

Default Users and Passwords

If you intend to manage the Switch using the web interface or the command line interface, or to change the default passwords, you need to log in with a valid user name and password. The Switch has three default user names, and each user name has a different password and level of access. These default users are listed in Table 9.

CAUTION: *To protect your Switch from unauthorized access, you must change all three default passwords as soon as possible, even if you do not intend to actively manage your Switch*

Table 9 Default Users

User Name	Default Password	Access Level
monitor	monitor	monitor — the user can view all manageable parameters, except special/security features, but cannot change any manageable parameters.
manager	manager	manager — the user can access and change the operational parameters but not special/security features
admin	(no password)	security — the user can access and change all manageable parameters

Use the admin default user name (no password) to login and carry out initial Switch setup.

Fuente: HP Business Support Center (2012), Recuperado el 19 de abril del 2012 de http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c02583584/c02583584.pdf

- **Switch D-LINK 3226L**

Tomado de: DES-3226L Layer 2 Switch Command Line Interface Reference Manual Pag.6

With the serial port properly connected to a management computer, the following screen should be visible. If this screen does not appear, try pressing Ctrl+r to refresh the console screen.

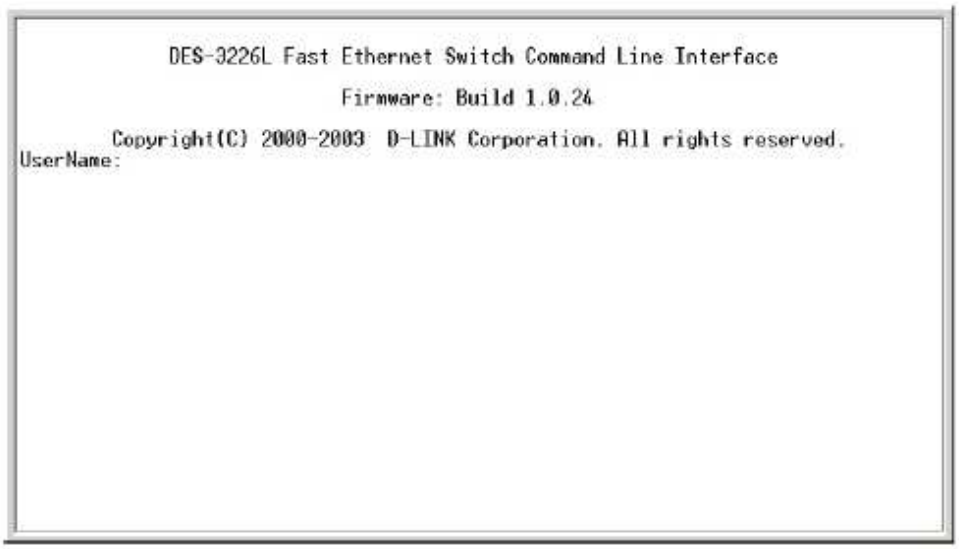


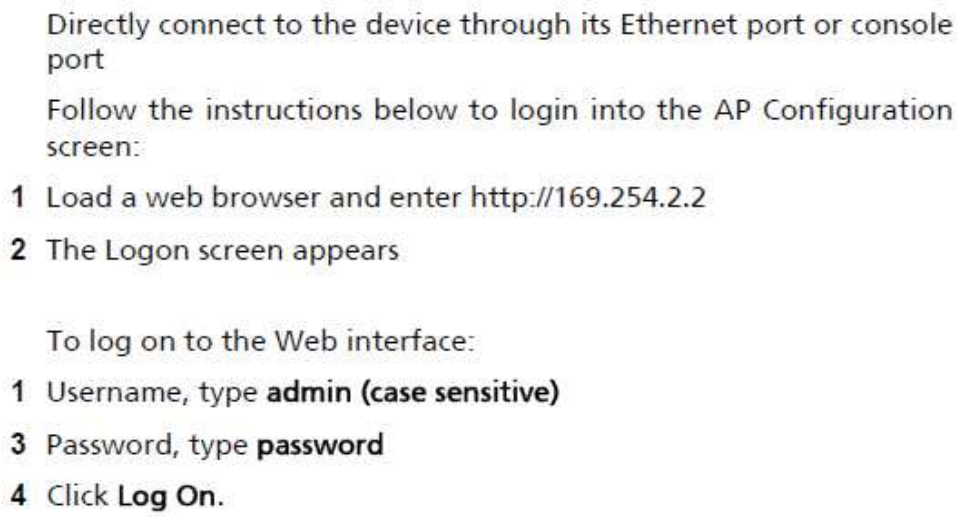
Figure 1-1. Initial Console screen.

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DES-3226L:4#**. This is the command line where all commands are input.

Fuente: D-link (2012), Recuperado el 19 de abril del 2012 de ftp://ftp.dlink.ru/pub/Switch/DES-3226L/Description/DES-3226L_+CLI_V100.pdf

- **Access Point 3Com 7760**

Tomado de: 3Com Wireless 7760 11 a/b/g PoE Access Point 3CRWE776075 / WL-561 Pag.15



Directly connect to the device through its Ethernet port or console port

Follow the instructions below to login into the AP Configuration screen:

1 Load a web browser and enter http://169.254.2.2

2 The Logon screen appears

To log on to the Web interface:

1 Username, type **admin (case sensitive)**

3 Password, type **password**

4 Click **Log On.**

Fuente: Wi-Fi Wireless LAN (2012), Recuperado el 19 de abril del 2012 de http://wi-fi.unas.cz/dokumentace/3CRWE776075/3Com_AP7760_User-Guide.pdf

Anexo 2.

Políticas de seguridad de Directorio Activo

Default Domain Policy

Data collected on: 5/14/2012 10:26:43 AM

General

Details

Domain	sonda.com.ec
Owner	ECUASONDA\Domain Admins
Created	12/28/2001 11:21:04 AM
Modified	2/8/2011 5:05:54 PM
User Revisions	37 (AD), 37 (sysvol)
Computer Revisions	123 (AD), 123 (sysvol)
Unique ID	{31B2F340-016D-11D2-945F-00C04FB984F9}
GPO Status	User settings disabled

Links

Location	Enforced	Link Status	Path
sonda	No	Enabled	sonda.com.ec

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
ECUASONDA\Domain Users

WMI Filtering

WMI Filter Name	None
Description	Not applicable

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
ECUASONDA\Domain Admins	Edit settings, delete, modify security	No
ECUASONDA\Domain Users	Read (from Security Filtering)	No
ECUASONDA\Enterprise Admins	Edit settings, delete, modify security	No
ECUASONDA\userforefront	Read	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Edit settings, delete, modify security	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No
S-1-5-21-1828855972-829503199-1256796775-6497	Edit settings, delete, modify security	No

S-1-5-21-1828855972-829503199-1256796775-7023	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	10 passwords remembered
Maximum password age	60 days
Minimum password age	0 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout threshold	3 invalid logon attempts

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit privilege use	Success, Failure

Local Policies/User Rights Assignment

Policy	Setting
Add workstations to domain	ECUASONDA\Domain Admins, ECUASONDA\adjordonez, a, S-1-5-21-1828855972-829503199-1256796775-9166, ECUASONDA\userforefront
Allow log on locally	BUILTIN\Administrators
Allow log on through Terminal Services	S-1-5-21-1828855972-829503199-1256796775-1776, S-1-5-21-1828855972-829503199-1256796775-1866, ECUASONDA\adjordonez, S-1-5-21-1828855972-829503199-1256796775-6497, S-1-5-21-1828855972-829503199-1256796775-9166,

Back up files and directories	ECUASONDA\userforefront, BUILTIN\Administrators ECUASONDA\userforefront, S-1-5-21-1828855972-829503199-1256796775-6497, S-1-5-21-1828855972-829503199-1256796775-9163, ECUASONDA\Domain Admins
Change the system time	S-1-5-21-1828855972-829503199-1256796775-9166, ECUASONDA\userforefront, administradores

Local Policies/Security Options
Network Security

Policy	Setting
Network security: Force logoff when logon hours expire	Disabled

Public Key Policies/Autoenrollment Settings

Policy	Setting
Enroll certificates automatically	Enabled
Renew expired certificates, update pending certificates, and remove revoked certificates	Disabled
Update certificates that use certificate templates	Disabled

Public Key Policies/Encrypting File System
Properties

Policy	Setting
Allow users to encrypt files using Encrypting File System (EFS)	Enabled

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	1/23/2005 9:05:18 AM	File Recovery

For additional information about individual settings, launch Group Policy Object Editor.

Public Key Policies/Trusted Root Certification Authorities
Properties

Policy	Setting
Allow users to select new root certification authorities (CAs) to trust	Enabled
Client computers can trust the following certificate stores	Third-Party Root Certification Authorities and Enterprise Root Certification Authorities
To perform certificate-based authentication of users and	Registered in Active Directory only

computers, CAs must meet the following criteria

User Configuration (Disabled)
Windows Settings
Remote Installation Services
Client Installation Wizard options

Policy	Setting
Custom Setup	Disabled
Restart Setup	Disabled
Tools	Disabled

Internet Explorer Maintenance
Browser User Interface/Customized Title Bar

Title Bar Text
por Dpto IT Sonda

Fuente: Departamento de IT, (2012)