ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DISEÑO DE UN ESQUEMA DE SEGURIDAD PARA LA RED DE DATOS DE UNA INSTITUCIÓN EDUCATIVA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO INFORMÁTICO MENCIÓN REDES DE INFORMACIÓN

ROSA VERÓNICA MARTÍNEZ ESPINEL
veromartinez55@hotmail.com

DIRECTOR: ING. WILLIAM ANDRADE
wandrade65@gmail.com

Quito, Octubre 2010

DECLARACIÓN

Yo, Rosa Verónica Martínez Espinel, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

Rosa Verónica Martínez Espinel

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Rosa Verónica Martínez Espinel, bajo mi supervisión.

_____

Ing. William Andrade

DIRECTOR DE PROYECTO

CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PRESENTACIÓN

La información es el recurso más valioso en cualquier tipo de organización, se dice que quien la posee tiene el poder; más aún, si a través del uso apropiado de esta, se provee de fuentes seguras para que los seres humanos tomen decisiones acertadas en todo campo, dirigiendo su potencial máximo en beneficio de la institución a la cual pertenece.

Existen muchos mecanismos que permiten administrar de una manera segura los datos y también, muchos recursos para transferir, procesar y almacenar información, más aún, con la tendencia creciente del uso de computadoras y redes, como medios de comunicación, es imperdonable e irresponsable en la actualidad dejar de lado los controles de seguridad; primeramente, por garantizar la integridad, disponibilidad y confidencialidad de la información y segundo, por la basta gama de recursos de software y hardware disponibles para este fin.

En el proyecto elaborado, se presenta una solución para mantener la seguridad de la red de datos adecuada al Colegio Militar Nro. 10 “Abdón Calderón”, específicamente en la seguridad física de las áreas críticas, la seguridad lógica de la red y el establecimiento de políticas y procedimientos de seguridad que responden a sus requerimientos, basadas en la metodología de test de intrusión, las normas ISO 27002 y el modelo de seguridad Safe de “Cisco”.

Este proyecto toma en cuenta la necesidad de un proceso urgente de capacitación en seguridad informática, el uso legal del software utilizado, la implementación del esquema de seguridad, la adopción de políticas y procedimientos de seguridad, y la realización permanente de controles que garanticen el funcionamiento, la evaluación y reingeniería del esquema de seguridad.

El beneficio de implementación del esquema de seguridad que se presenta, se refleja en: control de tráfico entrante y saliente de la institución, mejor administración de la red, menor tiempo dedicado al mantenimiento correctivo de

los equipos, mejor utilización del ancho de banda, detección a tiempo de intentos de ataque a la red, control de acceso a áreas sensibles, contar con servidores seguros, crear y mantener una cultura de seguridad informática, para lo cual se proyectan los costos referenciales de su implementación.

Este proyecto es un esquema de seguridad de red de datos que se ajusta a cualquier organización que cuente con características similares a la institución educativa para la cual fue desarrollado.

RESUMEN

El presente proyecto tiene como objetivo diseñar un esquema de seguridad para la red de datos de una institución educativa de Quito, con la finalidad de garantizar la integridad, disponibilidad y confidencialidad de la información frente a las amenazas internas y externas a las que está expuesta continuamente.

El proyecto inicia con una descripción general de la institución educativa, inmediatamente se analiza la situación actual de la red de datos en lo referente a la seguridad y se determina las vulnerabilidades y amenazas a las que está expuesta. En base de todo este análisis se establecen los requerimientos de seguridad, lo que permite diseñar un esquema adecuado a las necesidades de la institución educativa.

La determinación de vulnerabilidades y amenazas de la red de datos fue desarrollada en base a la “Penetration Testing Methodology” usado por el BSI, que provee el servicio de seguridad en tecnologías de información para el gobierno alemán. Esta metodología consta de 5 fases: Preparación, Reconocimiento, Análisis de Información y Riesgos, Intentos Activos de Intrusión y Análisis Final.

En la fase de “Preparación” se definen los objetivos y el alcance del test de penetración, tomando en cuenta los riesgos asociados con su ejecución.

En la fase de “Reconocimiento” se comienza a reunir información acerca del objetivo, tomando en cuenta el análisis de los datos publicados, la consulta sigilosa de información básica de la red, el escaneo sigiloso de puertos, la identificación de aplicaciones, la identificación de sistemas, la identificación sigilosa del router y firewall, investigación de vulnerabilidades e interfaces de aplicación. En la fase de “Análisis de Información de Riesgos” se analiza y evalúa la información obtenida en la fase anterior.

La fase “Intentos Activos de Intrusión” implica el mayor riesgo de seguridad por cuanto se invaden activamente los sistemas y módulos seleccionados en la fase anterior y no fue ejecutada debido a los riesgos asociados de realizarla en una estructura de red que no cuenta con la seguridad necesaria.

En la última fase “Análisis Final”, se muestran las conclusiones a las que se arribaron luego de realizar todo el proceso.

El diseño del esquema de seguridad para la red de datos se estableció en base a los requerimientos obtenidos del análisis de la situación actual de la empresa en cuanto a la seguridad de la información y del diagnóstico de las vulnerabilidades y amenazas, para su elaboración se utilizó como base el Modelo de Seguridad “SAFE” de Cisco para redes medianas, el cual divide al esquema seguro en 3 módulos: Módulo de Internet Corporativo, Módulo de Campo y Módulo WAN.

Para el diseño del esquema de seguridad físico se tomó en cuenta las normas ISO 27002. Ambos diseños se complementan con la elaboración de políticas y normas de seguridad.

En lo referente a la especificación de los componentes del esquema de seguridad y sus costos, se detallan las especificaciones técnicas mínimas requeridas para los equipos activos, seguridades físicas, así como las características necesarias para el software, con el objetivo de solicitar proformas a empresas especializadas, para así establecer un costo referencial para la implementación del esquema de seguridad planteado.

CAPITULO 1

ANÁLISIS DE RIESGOS

La Organización Internacional por la normalización define riesgo tecnológico como: “La probabilidad de que una amenaza se materialice, utilizando la vulnerabilidad existente de un activo o grupos de activos, generándole pérdidas o daños a la empresa”[1].

“Los objetivos del análisis de riesgos son:

- Identificar, evaluar y manejar los riesgos de seguridad.
- Estimar la exposición de un recurso a una amenaza determinada.
- Determinar cual combinación de medidas de seguridad proporcionará un nivel de seguridad razonable a un costo aceptable.
- Tomar mejores decisiones en seguridad informática.
- Enfocar recursos y esfuerzos en la protección de los activos.”[2]

En el presente capítulo se realiza el análisis de los riesgos de la red de datos, tomando en cuenta el estado actual de la misma y los resultados de los test de intrusión realizados, que revelan las vulnerabilidades y amenazas a las que está expuesta, así como la probabilidad de ocurrencia y el impacto de las mismas, para finalmente determinar los requerimientos de seguridad que permitan diseñar un esquema de seguridad que implemente los controles adecuados para disminuir o evitar la ocurrencia del riesgo.

1.1 DETERMINACIÓN DE LA INSTITUCIÓN EDUCATIVA

En esta sección se expone en términos generales la información que permite definir el tipo de institución educativa para la cual se está llevando a cabo el

[1] http://blogs.utpl.edu.ec/seguridadderedes/2008/11/17/administracion-de-riesgos/
[2] http://agoraproyectos.com/area_de_seguridad_informatica.php

presente proyecto, conociendo su actividad principal, historia, estructura organizacional, plan estratégico, ubicación y funciones del Centro de Informática.

1.1.1 INFORMACIÓN GENERAL

Nombre de la institución educativa:	Colegio Militar Nro. 10 “Abdón Calderón”
Tipo de institución educativa:	Unidad Educativa Técnica Experimental
Rector:	CRNL. CSM. Alberto P. Calvache F.
Dirección:	Av. Maldonado y Angel Polivio Chávez Av. Mariscal Sucre y Michelena
Teléfono:	(593-2) 2662-695, (593-2) 2583-732
Dirección Web:	http://www.comil10.edu.ec

Tabla 1.1 Información general de la institución educativa.

Fuente: COMIL 10 “Abdón Calderón”. http://www.comil10.edu.ec. Agosto 2009

1.1.2 DESCRIPCIÓN HISTÓRICA

La Institución nació en el año de 1.953 como Casa Maternal Militar Nro. 1, mediante decreto ejecutivo expedido por el Sr. Presidente de la República Dr. José María Velasco Ibarra.

En el año de 1.955 se inauguró el jardín de infantes con las secciones de pre-kinder y kinder. En 1.961 se crea el primer grado de instrucción primaria. En 1.972 se creó la escuela primaria completa con el nombre de "Abdón Calderón".

En 1.984 se crea el colegio mediante Acuerdo Ministerial Nº 1174, concluido el ciclo básico en Junio de 1.987 se crea el ciclo diversificado con tres especializaciones técnicas: Computación, Contabilidad y Secretariado en Español.

En 1985, por disposición de la Dirección de Educación de la Fuerza Terrestre el Colegio "Abdón Calderón", la Escuela y el Jardín de Infantes del mismo nombre, aparecen legalmente como Unidad Educativa "Abdón Calderón", conformada por los tres niveles antes citados.

En Febrero de 1.999 el Comando General de la Fuerza Terrestre, decide convertir a esta Unidad Educativa en Colegio Militar, nombrando a un oficial en el grado de Coronel como el primer Rector.

El Colegio Militar, se mantiene hasta la fecha con su noble misión, formar una juventud honesta, patriota y amante de la justicia, con virtudes que ennoblezcan su personalidad y competencias que les permitan continuar con su educación superior o ingresar al mundo laboral.

1.1.3 ACTIVIDAD PRINCIPAL

La institución educativa brinda a la comunidad en general servicios educativos en educación general básica y bachillerato con las especialidades técnicas de Comercio Exterior, Contabilidad y Aplicaciones Informáticas. El año lectivo 2010-2011 se ofrecerá también la especialidad de Ciencias de carácter general.

1.1.4 PLAN ESTRATÉGICO

1.1.4.1 Misión

“Formar Bachilleres Técnicos en Comercio y Administración, con especialización en Aplicaciones Informáticas, Contabilidad y Comercio Exterior; con proyección a Escuelas Militares, Politécnicas, Universidades e Institutos de Educación Superior, con una formación teórico profesional, integral y humanística de calidad, para alcanzar la excelencia educativa con la práctica de valores y lealtad a la Institución”[3].

[3] Agenda Educativa del Colegio Militar Nro. 10 “Abdón Calderón”

1.1.4.2 Visión

"Ser una institución educativa eminentemente humanística, integral, científico, técnico, mediante un sistema educativo moderno, eficiente y eficaz, con reconocimiento nacional e internacional, teniendo como fundamento la identidad nacional, el fortalecimiento de valores, la investigación científica, el fortalecimiento del idioma inglés, utilizando un currículo con enfoque de competencias para lograr bachilleres técnicos con especialización en función del desarrollo económico y social del país" [4] .

1.1.4.3 Objetivos Institucionales

- "Lograr que los alumnos que ingresen al primer año de EGB (Educación General Básica), egresen convertidos en eficientes bachilleres técnicos capaces de incorporarse exitosamente al sector productivo del país, o en bachilleres especializados para incursionar positivamente en la Educación Superior.

- Proporcionar a todos sus cadetes una formación integral que les permita su realización personal, dentro del medio en que se desenvuelven.

- Modernizar y optimizar todo el proceso educativo a fin de lograr la formación de bachilleres que respondan a las exigencias de la época actual"[5].

1.1.5 ORGÁNICO ESTRUCTURAL

La Figura 1.1 muestra el orgánico estructural bajo el cual funciona la Unidad Educativa en mención.

[4] http://www.comil10.edu.ec/html/quienes_somos.html
[5] Agenda Educativa del Colegio Militar Nro. 10 "Abdón Calderón"

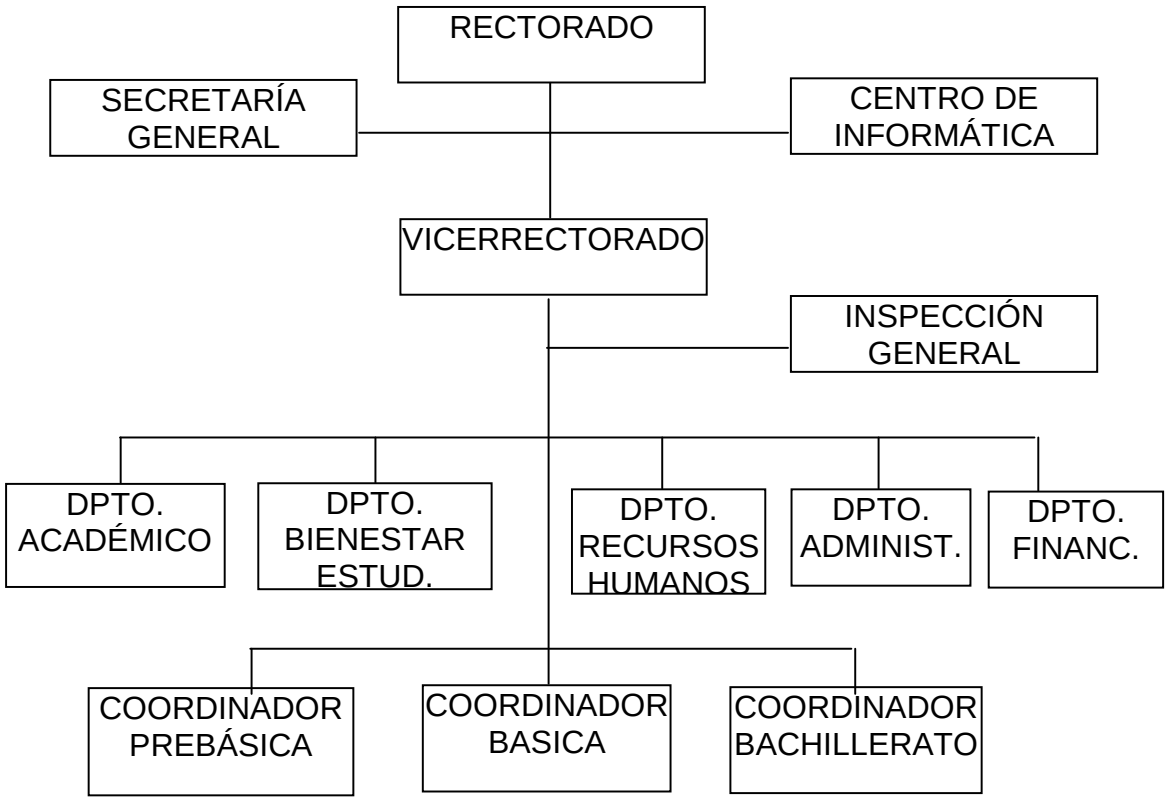


Figura 1.1 Orgánico Estructural de la Unidad Educativa.
Fuente: Normas de Gestión Administrativas de los Colegios Militares de la Fuerza Terrestre, 2008

1.1.6 UBICACIÓN

La Unidad Educativa funciona en dos locales geográficamente separados, en uno, ubicado en el centro de Quito, funciona de primero a séptimo año de educación general básica, que será referenciado en el presente proyecto como sección primaria y en otro, ubicado en el sur de Quito, funciona el área directiva, administrativa, financiera, la sección de bachillerato en la jornada matutina y de octavo a décimo año de educación general básica en la jornada vespertina, que será referenciado como sección secundaria.

1.1.7 ANÁLISIS DEL CENTRO DE INFORMÁTICA

Las funciones establecidas en el Reglamento Interno para el Centro de Informática son:

- "Programar y desarrollar los sistemas, las bases de datos: técnico – educativas y administrativas adquiridas por la Unidad Educativa.
- Realizar el estudio sobre nuevos programas y dar orientación al personal técnico sobre los mismos.
- Asistir técnicamente sobre instalaciones, actualizaciones, funcionamiento, mantenimiento de hardware y software.
- Llevar un registro de todos los programas implementados en el establecimiento educativo.
- Asesorar a los usuarios de la Institución sobre la correcta utilización de la información procesada.
- Velar por el funcionamiento de las redes de comunicación y equipos distribuidos en el establecimiento.
- Administrar el sistema físico y realizar el plan de mantenimiento de los equipos, coordinando con empresas especializadas.
- Mantener actualizados los sistemas de respaldo de la información
- Preparar y difundir normas y procedimientos que deben utilizarse en el manejo de los equipos.
- Determinar las normas de seguridad de los sistemas.
- Coordinar las actividades de capacitación profesional del personal del Centro de Informática.
- Establecer controles de entrada y salida de información"[6].

Las funciones establecidas en las Normas de Gestión Administrativas para el Jefe del Centro de Informática son:

- "Elaborar el proyecto de sistematización anual.

[6] Reglamento Interno de los Colegios Militares de la Fuerza Terrestre

- Planificar, organizar, ejecutar y controlar los procesos y archivos informáticos y las actividades del Centro de Informática, previo estudio y aprobación del Rectorado.
- Proporcionar apoyo técnico en el manejo de paquetes y utilitarios a los usuarios.
- Mantener en perfecto estado de funcionamiento los equipos informáticos y comunicaciones que tenga bajo su responsabilidad.
- Mantener en perfecto estado el material requerido para los equipos y custodiar las correspondientes licencias de uso.
- Informar al Rectorado de cualquier anomalía que detecte en el funcionamiento de la red.
- Preservar los equipos del colegio de la entrada de virus informáticos mediante el empleo y actualización de programas antivirus adecuados.
- Motivar a los estudiantes y profesores en el empleo de nuevas tecnologías, fomentando su espíritu de confianza académica dentro de la comunidad educativa.
- Recibir, clasificar, completar, procesar, archivar y custodiar la información del Centro de Informática.
- Organizar y evaluar el trabajo del personal bajo su responsabilidad.
- Organizar archivos de gestión automatizada, ficheros para el control de cintas, tonners, tintas, medios de almacenamiento y otros recursos informáticos de audio y video del Centro de Informática.
- Elaborar el informe técnico y cuadros comparativos para la adquisición de equipos.
- Desarrollar tareas de capacitación para el personal de la institución, de acuerdo al avance tecnológico"[7].

Las funciones de los asistentes del Centro de Informática no están claramente definidas, uno de los asistentes se ocupa del software y otro del hardware.

[7] Normas de Gestión Administrativa de los Colegios Militares de la Fuerza Terrestre

1.2 ESTADO ACTUAL DE LA RED DE DATOS

En esta sección se expone el estado actual de la red de datos, tomando en cuenta varios aspectos tales como: hardware, software, redes y comunicaciones, servicios, protocolos, aplicaciones, administración de la red y actividades inusuales detectadas.

La información presentada fue obtenida del Centro de Informática y/o recogida utilizando herramientas de software específicas para el análisis del tráfico e inventario de hardware y software de la red.

Para monitorear y analizar el tráfico de la red se utilizó Wireshark 1.2.1, un analizador de protocolos de red Open Source registrado bajo la licencia GNU GPL (General Public Licence), el cual permite capturar, filtrar, buscar, importar, exportar, crear estadísticas y examinar el contenido de paquetes desde una interfaz de red que trabaja en modo promiscuo.

Para obtener un inventario de hardware y software de varios equipos en la sección secundaria se utilizó OCSInventory 1.02.1, un programa libre que permite recopilar la información de hardware y software de los equipos conectados a la red, para lo cual hace uso de un servidor con interfaz web encargado de almacenar y gestionar la información y un agente instalado en cada equipo a ser inventariado que envía toda la información recolectada al servidor.

1.2.1 HARDWARE

1.2.1.1 Equipos de Computación

La Unidad Educativa cuenta con un total de 230 equipos de computación, 6 portátiles y 55 impresoras, distribuidos dentro de las áreas de los diversos departamentos, tanto de la sección primaria como secundaria, 134 equipos se encuentran conectados a la red, el resto trabaja en forma independiente. La Tabla 1.2 muestra la distribución de los equipos en cada departamento.

Sección	Departamento	Equipos	Portátiles	Impresoras
Secundaria	Rectorado	-----	1	-----
	Vicerrectorado	-----	1	-----
	Secretaría General	4		5
	Centro de Informática	6	1	4
	Inspección	5	-----	4
	Académico	118	-----	8
	Bienestar Estudiantil	10	-----	7
	Recursos Humanos	2	-----	2
	Administrativo	4	1	6
	Financiero	7	1	8
	Subtotales	**156**	**5**	**44**
Primaria	Administrativo	2		2
	Bienestar Estudiantil	6		4
	Académico	61		2
	Centro de Informática	3	1	1
	Inspección	2		2
	Total	**230**	**6**	**55**

Tabla 1.2 Distribución de los Equipos de Computación

Fuente: COMIL 10 “Abdón Calderón”. Centro de Informática, 2009

Los equipos de computación del Departamento Académico se encuentran distribuidos en los laboratorios, bibliotecas y aulas de la Unidad Educativa, en ambas secciones, así como en las jefaturas académicas.

Las características de hardware de varios de los equipos de la sección secundaria, levantadas con OCSInventory se encuentran detalladas en el Anexo 1 Resumen de características de hardware (A1-1).

1.2.1.2 Servidores

La Unidad Educativa cuenta con un total de 5 servidores distribuidos en ambas secciones, de los cuales 2 poseen arquitectura de servidor y 3 poseen arquitectura de estación de trabajo. Ver Tabla 1.3.

Sección	Modelo	Características	Función	S.O.
Secundaria	Clon	Hostname: COMIL10 Procesador: Intel (R) Pentium(R) 4 CPU 2.40 GHz Memoria: 256MB Disco: 70GB, 2 particiones	Servidor Proxy	Linux RedHat 8.0
	Clon	Hostname: SRVCOMIL10-RECO Procesador: Xeon (TM) CPU 3.06 GHz Memoria: 2.0GB Disco: 50GB, 4 particiones	Servidor de Base de Datos	Windows 2003 Server
	Clon	Hostname: SRVCOMIL10 Procesador: x86 Family 6 Model 8 Stepping 3 AT/AT compatible Memoria: 1GB Disco: 8GB, 2 particiones	Servidor de Base de Datos	Windows NT
Primaria	Clon	Hostname: COMIL10-RECOLETA Procesador: Intel (R) Pentium(R) 4 CPU 2.40 GHz Memoria: 512MB Disco: 70GB, 2 particiones	Servidor Proxy	Linux RedHat 8.0
	Clon	Hostname: SERVIDORREC Procesador: Xeon (TM) CPU 3.06 GHz Memoria: 2.0GB Disco: 50GB, 2 particiones	Servidor de Base de Datos	Windows XP

Tabla 1.3 Características de los servidores

Fuente: COMIL 10 “Abdón Calderón”. Centro de Informática, 2009

1.2.2 SOFTWARE

1.2.2.1 Sistema Operativo

La Tabla 1.4 muestra los Sistemas Operativos utilizados en los equipos de la Unidad Educativa junto con el número de máquinas por cada uno de ellos.

Sistema Operativo	Cantidad
Windows 98	20
Windows XP	206
Windows 2003 Server	1
Windows NT	1
Linux Red Hat 8.0	2

Tabla 1.4 Sistemas Operativos utilizados

Fuente: COMIL 10 “Abdón Calderón”. Centro de Informática, 2009

1.2.2.2 Software Institucional

El software utilizado para la gestión administrativa, financiera y académica de la institución, desarrollado por el Centro de Informática y/o adquirido a terceros es el siguiente:

- Sistema Integrado Educativo (SIE)
- Sistema Integrado de Gestión Financiera (ESIGEF)
- Sistema de la Fuerza Terrestre (SISFT)
- Sistema de Evaluación de Personal
- Sistema de Control de Personal
- Sistema de Activos Fijos
- Programa Control de Documentos
- Programa de Control de Inventarios
- Programa Roles de Pago

Únicamente el Sistema Integrado Educativo (SIE) corre en red, el resto lo hace de manera local.

1.2.2.3 Software Adicional

No existe un registro ni licencias del software adicional instalado en los equipos de la Unidad Educativa, por lo cual se levantó un inventario del software en varios equipos de la sección secundaria con OCSInventory, los resultados que aparecen en el Anexo 1 Listado de Software (A1-12), revelan la falta de control sobre las aplicaciones instaladas en los distintos computadores, especialmente en el área administrativa.

Dentro de estos programas aparecen: barras de navegación, screensavers, programas para buscar y descargar música, películas, archivos, imágenes; herramientas Google, juegos, pasatiempos, programas para mezclar y editar música, suites para celulares Motorola y Nokia, herramientas para edición y diseño gráfico, mensajería instantánea, clientes de correo electrónico, codecs para comprimir y descomprimir archivos de audio, herramientas ofimáticas, entre otros.

Una breve revisión en los equipos que actúan como servidores de bases de datos en la sección secundaria reveló la existencia de software instalado no necesario para cumplir con su función, tal como:

- Accesorios de Windows
- F-Prot
- Lexmark 5000 Serie Color Fine
- Micrograft for Kids
- Microsoft Visual Fox Pro
- PowerBuilder 6.0 y 8.0
- PowerDesigner 7.0
- WinZip

- Microsoft Office
- FullTime
- Acrobat Reader 5.0
- Outlook Express

1.2.3 REDES Y COMUNICACIONES

1.2.3.1 Cableado

El cableado en la sección secundaria se concentra en el edificio administrativo y en la biblioteca, donde se ha utilizado cable UTP categoría 5. La topología de red es en estrella.

Algunos tramos de cableado tienen canaletas en buen estado y en otros casos el cable va de un piso a otro por tubería o se encuentra a la vista, algunos cajetines se encuentran rotos y los conectores RJ45 sin protección. En ciertas áreas del edificio existen cables en mal estado e incluso sueltos, es decir sin cajetín o conectores. Ver Anexo 2 Fotográfico de las instalaciones de red de la Unidad Educativa (A2-1).

El cableado en la sección primaria se concentra en el segundo y tercer piso del edificio y en un par de áreas separadas y un poco distantes dentro de la misma institución, por lo que se ha utilizado cable UTP y STP categoría 5. Algunos cables se encuentran a la vista y demasiado cerca de cables eléctricos, en algunos lugares el cable va directo a las estaciones de trabajo, no existen cajetines ni patch cords. Ver Anexo 2 Fotográfico de las instalaciones de red de la Unidad Educativa (A2-16).

Lo antes mencionado y la inexistencia de certificación del cableado, denotan una falencia en el cableado, el cual no se encuentra en condiciones óptimas para la transmisión de datos y no respeta las normas de cableado estructurado.

La Unidad Educativa cuenta con 134 puntos de red.

1.2.3.2 Equipos Activos de la Red

Los equipos de interconexión en la red de datos se muestran en la Tabla 1.5.

Cantidad	Equipos Activos	Fabricante	Modelo
5	Router	Cisco	SB101
2	Switch	3Com	5500G
5	Switch	3Com	4200
3	Switch	3Com	2024
1	Switch	DLink	S/M

Tabla 1.5 Equipos de interconexión de la red de datos

Fuente: COMIL 10 “Abdón Calderón”. Centro de Informática, 2009

1.2.3.3 Diseño lógico de la red

La Figura 1.2 muestra el diseño lógico actual de la red de datos.

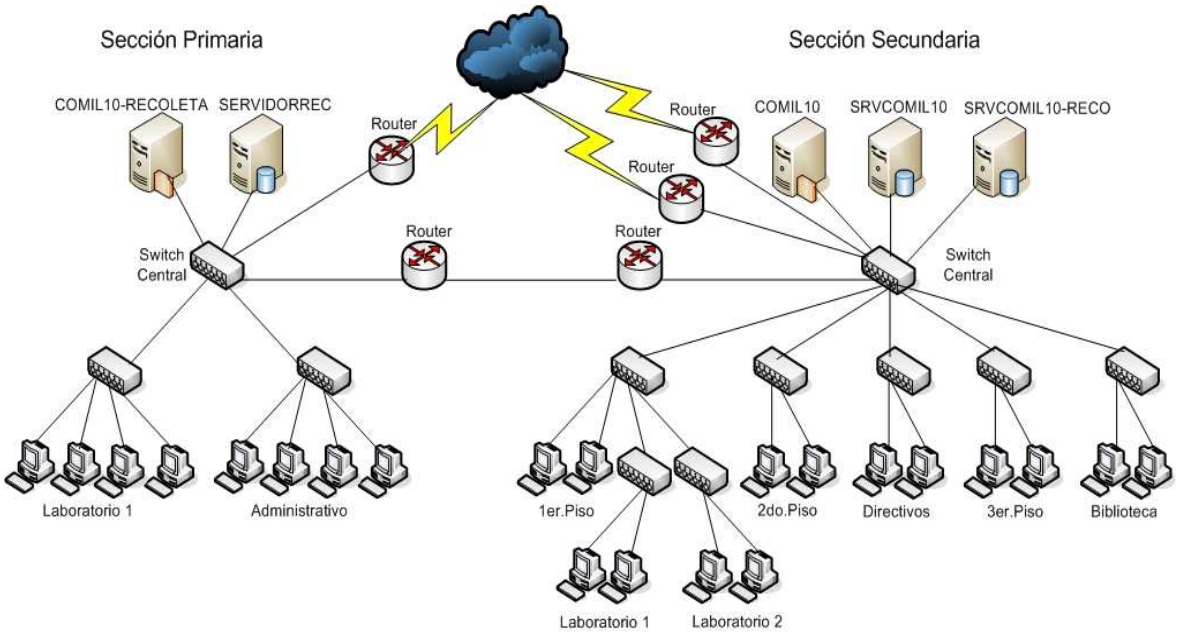


Figura 1.2 Diseño Lógico de la Red

Fuente: COMIL 10 “Abdón Calderón”. Centro de Informática, 2009

1.2.3.4 Direccionamiento IP

Utilizando el software Wireshark, se detecta que la Unidad Educativa trabaja con 4 redes internas, 3 de las cuales están definidas en la sección secundaria y una en la sección primaria, su utilización se detalla en la Tabla 1.6.

Los equipos dentro de las redes son asignados, con números IP en forma manual y no planificada, por lo que en ocasiones se han suscitado duplicidades.

SECCIÓN	DIRECCIÓN IP	DESCRIPCIÓN
Secundaria	192.168.101.0	Red Administrativa y Académica
	192.168.102.0	Red Laboratorios de Informática
	192.168.103.0	Red Biblioteca
Primaria	192.168.110.0	Red Administrativa y Laboratorio

Tabla 1.6 Detalle del direccionamiento IP

Fuente: Monitoreo de la red con Wireshark, 2009

1.2.4 SERVICIOS

Los servicios configurados en la institución son: acceso al Internet, Proxy y base de datos, se encuentran distribuidos según muestra la Tabla 1.7.

Servidor	Aplicaciones	Servicios
COMIL10	Squid 2.5 bajo Linux	Proxy
COMIL10-RECOLETA	Squid 2.5 bajo Linux	Proxy
SRVCOMIL10-RECO	Sybase SQL Anywhere 5.0	Base de Datos
SRVCOMIL10	Sybase SQL Anywhere 5.0	Base de Datos
SERVIDORREC	Sybase SQL Anywhere 5.0	Base de Datos

Tabla 1.7 Servicios de la Red

Fuente: COMIL 10 “Abdón Calderón”. Centro de Informática, 2009

1.2.4.1 Acceso al Internet

Todos los equipos conectados a la red disponen de este servicio. El ISP que proporciona acceso al Internet, servicio de hosting y un enlace WAN de datos punto a punto desde la sección primaria hasta la sección secundaria es Telconet. Cabe mencionar que este enlace de datos no se ha usado nunca por fallas en la configuración de la red.

El acceso del Internet se lo hace desde cada sección por separado, es así que en la sección primaria se dispone de 256 Kbps, en la sección secundaria se dispone de dos enlaces uno de 512 Kpbs para el uso de estudiantes, personal docente y administrativo y otro de 256 Kbps para uso exclusivo de los directivos. Además el enlace de datos WAN punto a punto de fibra óptica entre la sección primaria y secundaria es de 256 Kbps.

1.2.4.2 Servidor Proxy

Se tienen instalados dos servidores Proxy, uno en cada sección de la Unidad Educativa, los cuales permiten el acceso al Internet de cada una de las secciones por separado. La Figura 1.3 muestra las ACLs (Listas de Control de Accesos) configuradas en el servidor Proxy de la sección secundaria.

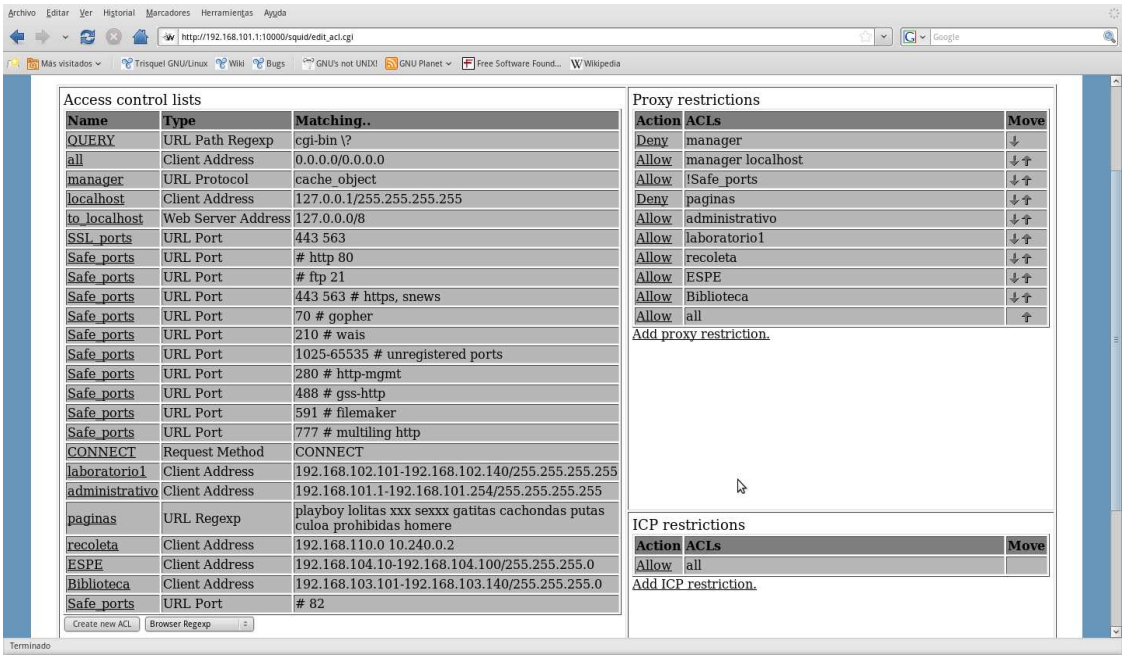


Figura 1.3 ACLs configuradas en el Servidor Proxy Secundaria

Fuente: COMIL 10 “Abdón Calderón”. Configuración Squid, 2009

1.2.4.3 Bases de Datos

La Unidad Educativa utiliza Sybase SQL Anywhere 5.0 como motor de base de datos el cual se utiliza en las aplicaciones del Sistema Integrado Educativo (SIE).

1.2.4.4 Correo Electrónico

No se encuentra configurado el servicio de correo electrónico interno ni externo.

1.2.4.5 Antivirus

La institución educativa utiliza software antivirus libre como el AVG Free y gratuito como las versiones de prueba de NOD32 en forma local, el que se actualiza siempre y cuando el equipo esté conectado al Internet y configurado para tal propósito, no existe ningún equipo que actúe de servidor principal, que permita descargar las actualizaciones para de forma automática actualizarlo en los equipos con versiones antivirus de cliente.

1.2.4.6 DNS

No existe servidor de nombres, los nombres en la red interna se resuelven utilizando NetBios y para salir al Internet se utiliza el servicio de DNS del ISP.

1.2.4.7 Directorio Activo

No se encuentra configurado el servicio de directorio activo en ninguno de los servidores de la red de datos, por lo tanto no existe un medio que permita organizar, controlar y administrar centralizadamente el acceso a los recursos de la red, todos los recursos como: impresoras, archivos, carpetas que necesitan ser accesados desde otros equipos de la red están configurados como recursos compartidos.

1.2.4.8 Servidor Web

No se cuenta con un servidor Web institucional, se utiliza el hosting provisto por el ISP donde reside la página Web de la Institución.

1.2.4.9. Servidor de Archivos

No existe servidor de archivos configurado.

1.2.4.10 Servidor de Aplicaciones

No existe servidor de aplicaciones, las aplicaciones que corren en red se encuentran grabadas en forma local en todos los equipos que las necesitan.

1.2.4.11 Servidor de Respaldos

No existe un servidor de respaldos configurado, sin embargo uno de los servidores de bases de datos de la sección secundaria mantiene una copia permanente de las bases de datos del SIE.

1.2.5 PROTOCOLOS

Se ha detectado la utilización de múltiples protocolos circulando a través de las redes internas. Los protocolos más utilizados en la red de datos de la Unidad Educativa de acuerdo al escaneo realizado con Wireshark se muestran en la Figura 1.4.

- Capa de Enlace
  - ✓ ARP (Address Resolution Protocol).- Utilizado para convertir las direcciones IP en direcciones de red física dentro de la red interna.

- Capa de Red:
  - ✓ IP (Internet Protocol).- Utilizado para la comunicación entre equipos (origen y destino) a través de la red interna y externa.

  - ✓ ICMP (Internet Control Message Protocol).- Usado principalmente por los routers para envío de mensajes de error hacia otros routers.

  - ✓ IGMP (Internet Group Management Protocol).- Se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión.

  - ✓ CDP (Cisco Discovery Protocol).- Protocolo de red propietario utilizado por los routers Cisco de ambas secciones para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP.

- Capa de Transporte:
  - ✓ TCP (Transmission Control Protocol).- Permite a los usuarios internos transferir ficheros entre equipos de la red, además descargar y subir archivos del Internet.

- ✓ UDP (User Datagram Protocol).- Utilizado principalmente por las aplicaciones del SIE que corren en red para actualizar la información en el servidor de bases de datos.

- Capa de Presentación:
  - ✓ NBNS (Name Bios Name Server).- Protocolo utilizado para la resolución de nombres de equipos de la red interna.

- Capa de Aplicación:
  - ✓ HTTP (Hypertext Transfer Protocol): Utilizado para la transferencia de hipertexto entre dos dispositivos de la red.

  - ✓ DHCP (Dynamic Host Configuration Protocol).- Protocolo utilizado para solicitar la asignación dinámica de una dirección IP.

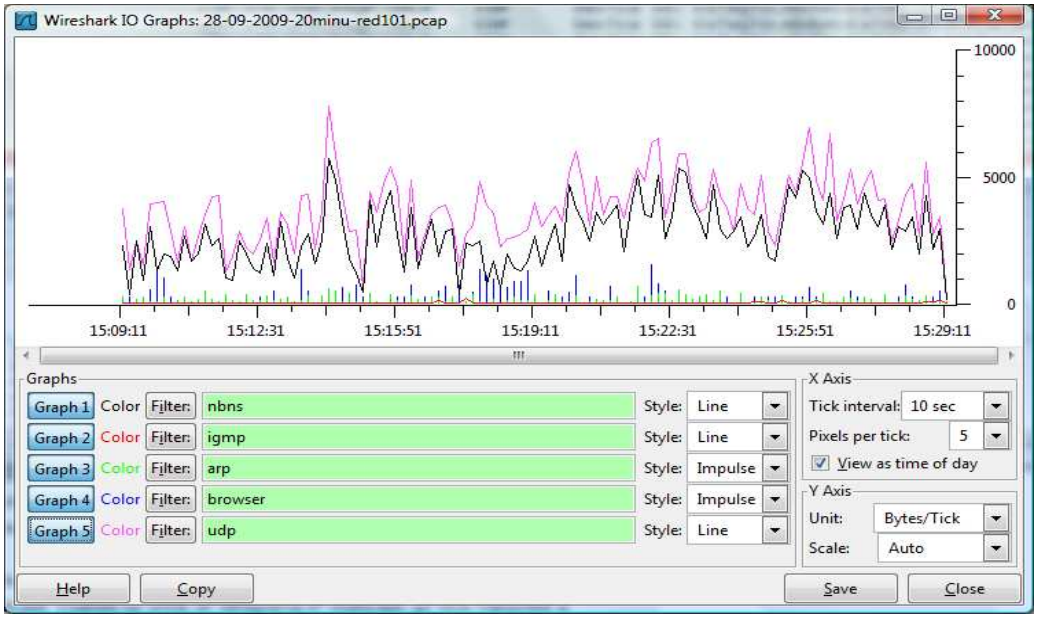


Figura 1.4 Protocolos más utilizados en la red

Fuente: Monitoreo de la red con Wireshark, Septiembre 2009

El tráfico UDP dentro de la red aumenta en fechas especiales como: registro de notas en el sistema académico e inscripciones y matrículas en los sistemas de secretaría y colecturía. En la Figura 1.5 se puede observar que un gran porcentaje

del tráfico UDP capturado proviene o tiene destino al equipo que actúa como servidor de bases de datos, al puerto 1498, designado para sybase-sqlany.

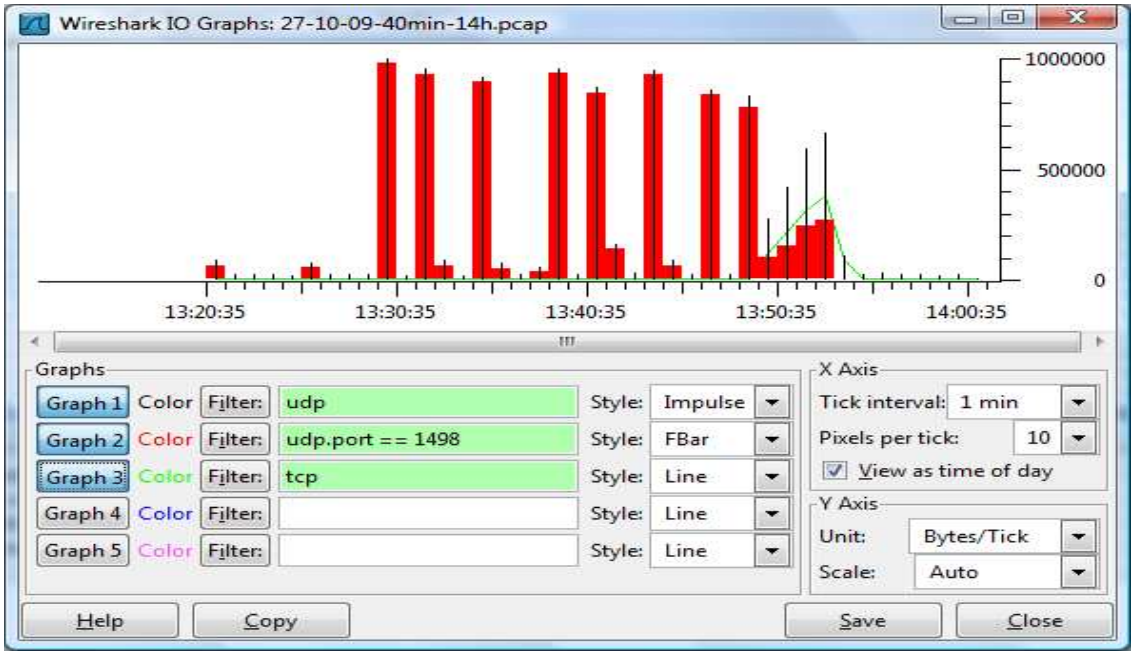


Figura 1.5 Uso de protocolo UDP y TCP

Fuente: Monitoreo de la red con Wireshark, Octubre 2009

1.2.6 APLICACIONES

A continuación se describen las aplicaciones institucionales más representativas:

1.2.6.1 Sistema Integrado Educativo (SIE)

Este sistema está desarrollado en PowerBuilder y utiliza la base de datos Sybase SQL Anyware. Está conformado por los módulos: Colecturía, Académico y Secretaría. No existen programas fuentes de estos módulos, el código ejecutable fue adquirido a un programador particular, por lo cual para cualquier modificación, la Unidad Educativa debe recurrir a la persona que lo desarrolló y pagar por cualquier cambio a realizarse. Las Figuras 1.6 y 1.7 muestran la interfaz principal de cada módulo.

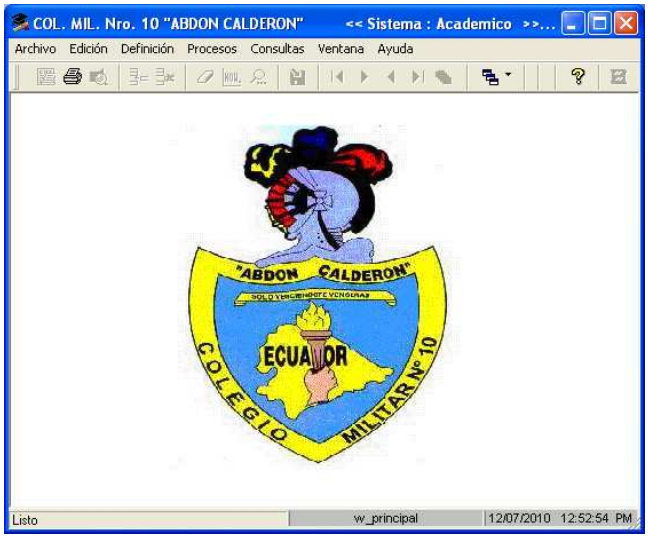


Figura 1.6 Interfaz Principal - Módulo Académico

Fuente: COMIL 10 “Abdón Calderón”. Área Académica, 2009

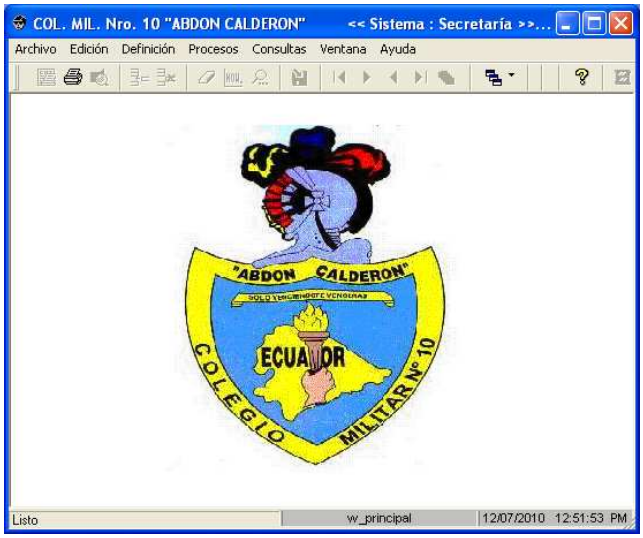


Figura 1.7 Interfaz Principal - Módulo Secretaría

Fuente: COMIL 10 “Abdón Calderón”. Secretaría General, 2009

La aplicación Académico, que sirve para el ingreso de notas se encuentra copiada en todos los equipos de las áreas académicas, coordinación académica, secretaría general y en algunos equipos del laboratorio. La Figura 1.8 permite determinar que los equipos se conectan con el servidor de bases de datos utilizando el software Sybase SQL Anywhere Network Requestor, el cuál se encarga de encontrar el servidor de bases de datos, establecer una conexión y toda la comunicación posterior entre cliente y servidor.

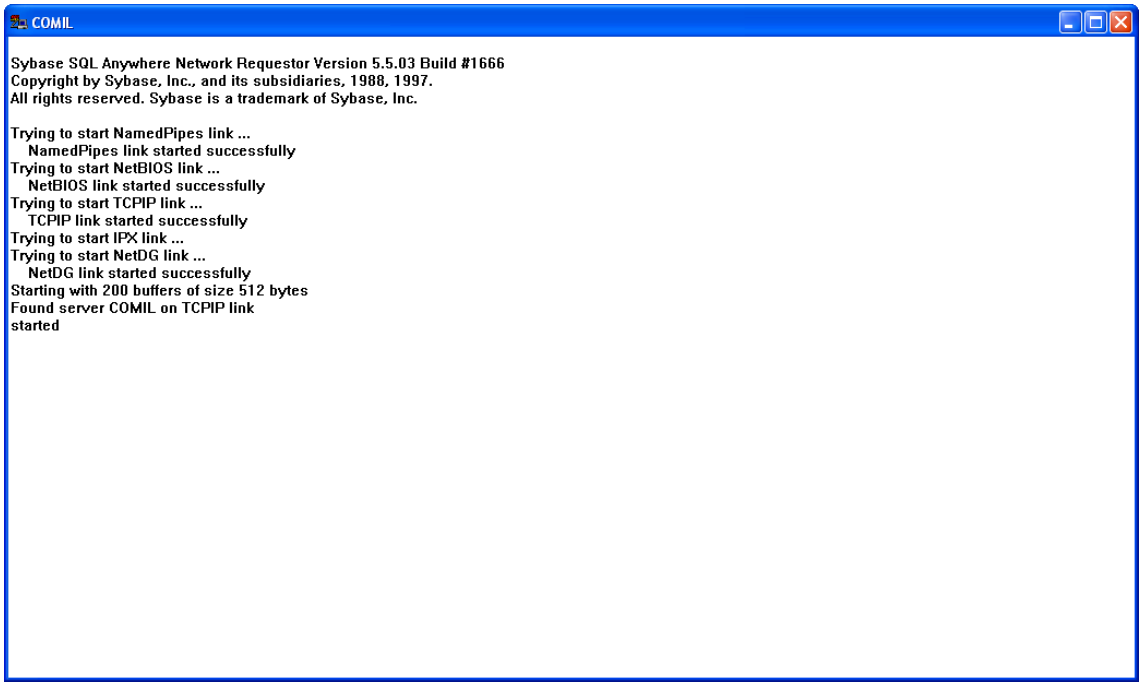


Figura 1.8 Conexión a la base de datos desde aplicación Académico
Fuente: COMIL 10 “Abdón Calderón”. Área Académica, 2009

La aplicación Colecturía es utilizada por el colector de la Unidad Educativa para la generación de papeletas y cobro de inscripciones, matrículas y pensiones.

La aplicación Secretaría es utilizada por Secretaría General para los procesos de inscripción y matriculación de estudiantes.

1.2.6.2 Sistema Financiero (ESIGEF)

Software creado por el Ministerio de Finanzas para el manejo de las finanzas públicas centralizadas, elaborado en .NET y compatible solo con Microsoft Internet Explorer 6.0 o superior.

El personal del Departamento Financiero utiliza este software para la gestión presupuestaria y contable de la institución, para lo cual ingresan a la dirección web: https://esigef.mef.gov.ec/esigef/login/frmlogin.aspx, la Figura 1.9 muestra la interfaz de acceso al mencionado sistema.

Figura 1.9 Interfaz de acceso – ESIGEF

Fuente: COMIL 10 “Abdón Calderón”. Departamento Financiero, 2009

1.2.6.3 Sistema Financiero (SISFT)

Este sistema fue desarrollado por el Departamento de Sistemas de la Dirección de Finanzas de la Fuerza Terrestre y fue utilizado hasta el año anterior por el personal financiero, se encuentra conformado por los módulos: Presupuesto y Contabilidad, lo utilizan actualmente solo para realizar consultas. La Figura 1.10 muestra la interfaz de acceso al recurso compartido residente en el servidor NT.

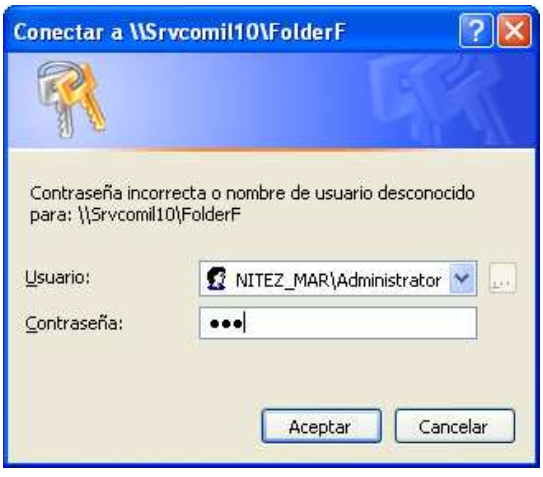


Figura 1.10 Interfaz de acceso – Recurso compartido - servidor NT

Fuente: COMIL 10 “Abdón Calderón”. Departamento Financiero, 2009

1.2.6.4 Sistema de Control de Personal

Este sistema permite el control de ingreso y salida del personal, vino incluido en el dispositivo biométrico de lectura de huella digital.

1.2.6.5 Programa Roles de Pago

Este sistema permite la generación de los confidenciales de todo el personal que labora en la Unidad Educativa y fue elaborado por el Departamento de Sistemas de la Dirección de Finanzas de la Fuerza Terrestre.

1.2.7 ADMINISTRACIÓN DE LA RED

1.2.7.1 Gestión de Hardware

Todos los equipos de computación de los laboratorios se someten a un mantenimiento preventivo al inicio de cada año lectivo y al finalizar cada trimestre, con la finalidad de ofrecer un rendimiento apropiado, el resto de equipos lo hace por lo menos una vez al año.

El mantenimiento correctivo de los equipos se lo realiza en el momento en que se presente la falla, inicialmente lo realiza el personal técnico del Centro de Informática, sin embargo si el daño no puede ser reparado se envía el equipo a reparación en una tercera empresa.

1.2.7.2 Gestión de Software

No existe ningún procedimiento para la gestión del software.

1.2.7.3 Gestión de Usuarios

La mayoría de equipos dentro de las áreas administrativas son manejados con usuarios locales tipo Administrador, los equipos pertenecientes al área docente tienen configurado en forma local dos usuarios, un usuario local limitado sin contraseña y un usuario local tipo Administrador con contraseña, conocida solo por el personal de mantenimiento del Centro de Informática.

Los equipos de los laboratorios en la sección secundaria, tienen cinco usuarios locales creados, un usuario tipo Administrador para el manejo del laboratorista, otros cuatro tipo Limitado para el manejo de los estudiantes, aunque en ocasiones por el tipo de software a utilizar se permite el uso del usuario Administrador por los estudiantes de la especialización de Aplicaciones Informáticas.

Los equipos de la biblioteca tienen tres usuarios locales creados, un usuario tipo Administrador con contraseña para el manejo del personal de mantenimiento, y dos usuarios tipo Limitado para el uso de estudiantes y docentes.

En la sección primaria tanto del laboratorio como de las áreas administrativas, existen usuarios locales tipo Administrador sin contraseña, para el uso de estudiantes de 7 a 11 años, personal administrativo y docente.

No existe gestión de usuarios a nivel de red, los recursos compartidos pueden ser accesados por todos los usuarios de la red.

1.2.7.4 Plan de respaldos

No existe ningún plan de respaldos.

1.2.7.5 Políticas de seguridad

La Unidad Educativa no posee ningún documento que especifique las políticas de seguridad propias, sin embargo cuenta con un instructivo referente a las políticas

de seguridad informática para el empleo en la Fuerza Terrestre, que no se aplica en la Unidad Educativa, por cuanto está diseñado para otra realidad y su contenido solo es de conocimiento de los miembros del Centro de Informática.

1.2.8 ACTIVIDAD INUSUAL EN LA RED

Examinando los resultados obtenidos con varios escaneos realizados en un período de tiempo considerable y utilizando Wireshark, se pudo detectar varias actividades inusuales en la red, las cuales se detallan a continuación.

1.2.8.1 Sección Secundaria

1.2.8.1.1 Escaneo del 28-09-2009 y 29-09-2009

Como lo muestra el Figura 1.11, las direcciones IP 192.168.101.183 y 192.168.101.233 envían mensajes a la dirección broadcast, utilizando el protocolo NBNS y averiguando por las direcciones IP de SHV4.NO-IP.BIZ y BOOSTER.ESTR.ES, que son catalogadas como nombres de dominio DNS relacionados con servidores de control y comandos de botnets, que permiten entre otras cosas el envío de spams a servidores de correo, ataques de DoS (Denegación de Servicio) y fraudes, además de causar lentitud anormal en el sistema y aumento en el consumo de ancho de banda.

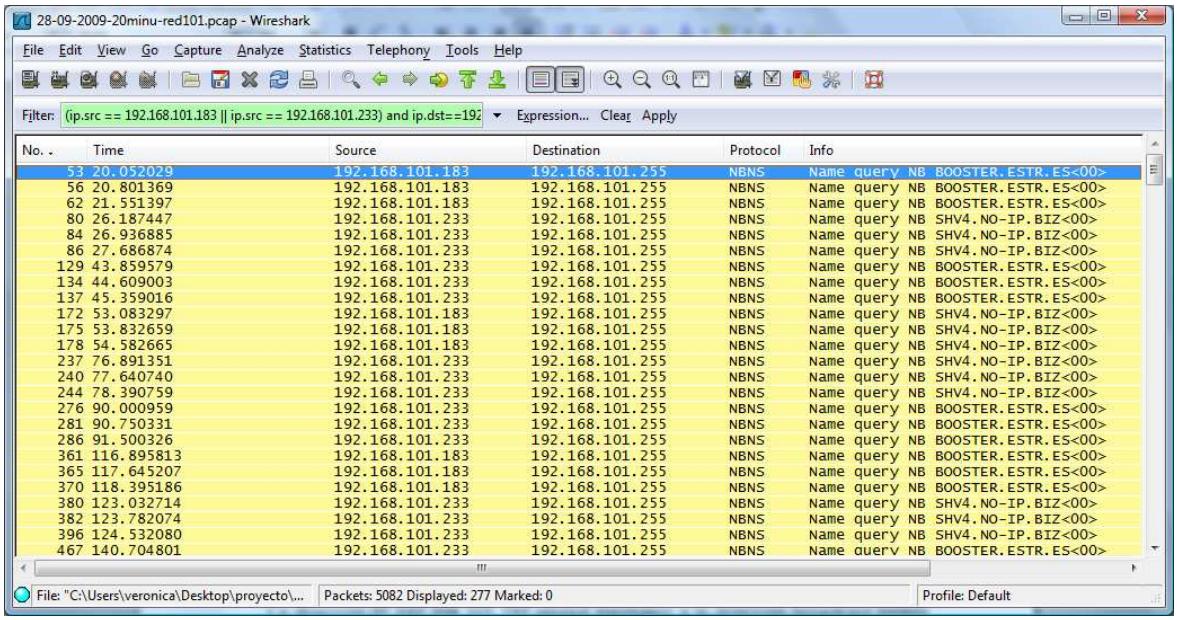


Figura 1.11 Name query SHV4.NO-IP.BIZ y BOOSTER.ESTR.ES 28-09-2009

Fuente: Monitoreo de la red con Wireshark, Septiembre 2009

Existen paquetes DCHP desde la dirección MAC 00:1a:73:bc:de:f9 hacia la dirección broadcast, es decir, existe equipo que solicita IP de forma dinámica.

1.2.8.1.2 Escaneo del 01-10-2009

Como se muestra en el Figura 1.12, las direcciones IP 192.168.101.183 y 192.168.101.197 envían mensajes a la dirección broadcast utilizando el protocolo NBNS y averiguando por SHV4.NO-IP.BIZ, BOOSTER.ESTR.ES.

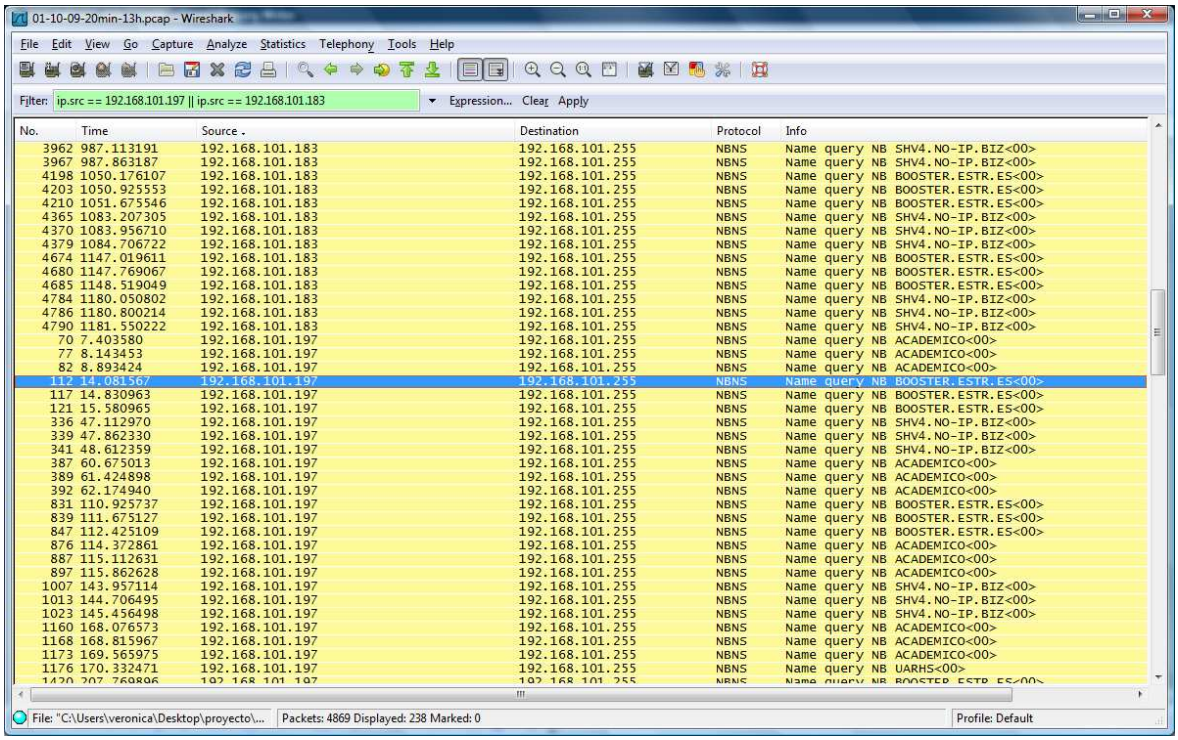


Figura 1.12 Name query SHV4.NO-IP.BIZ y BOOSTER.ESTR.ES 01-10-2009

Fuente: Monitoreo de la red con Wireshark, Octubre 2009

El Figura 1.13, muestra a la dirección IP 192.168.101.107 enviando mensajes broadcast ARP averiguando por cada una de las direcciones MAC de la red.

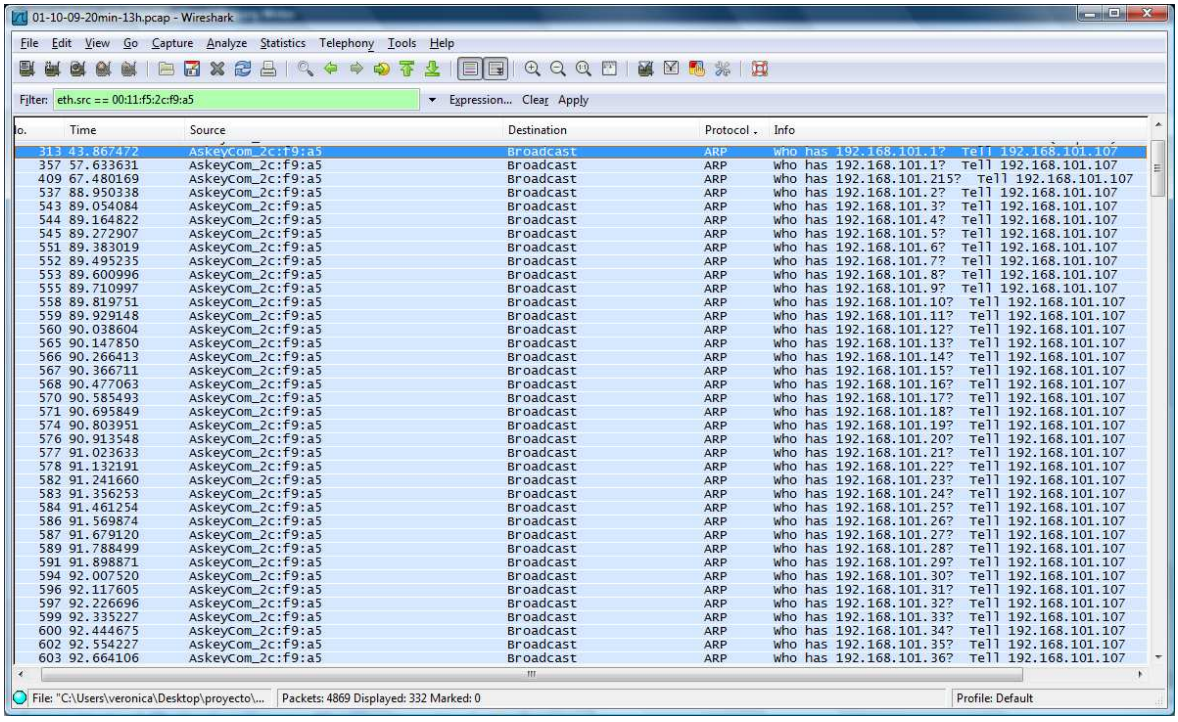


Figura 1.13 Broadcast ARP 192.168.101.107

Fuente: Monitoreo de la red con Wireshark, Octubre 2009

Como lo muestran los Figuras 1.14 y 1.15, existe tráfico desde la dirección MAC: 00:21:00:50:e5:45 con direcciones IPv4: 192.168.101.222 e IPv6: fe80::206e:6fdb:5b7d:8f46 utilizando varios protocolos tales como: NBNS, ICMPv6, DHCPv6, LLMNR y SSDP hacia la dirección broadcast y/o varias direcciones multicast, lo que hace pensar que existe un equipo con Windows Vista o Windows Server cuya tarjeta de red tiene configurado ambas versiones de protocolo IP.

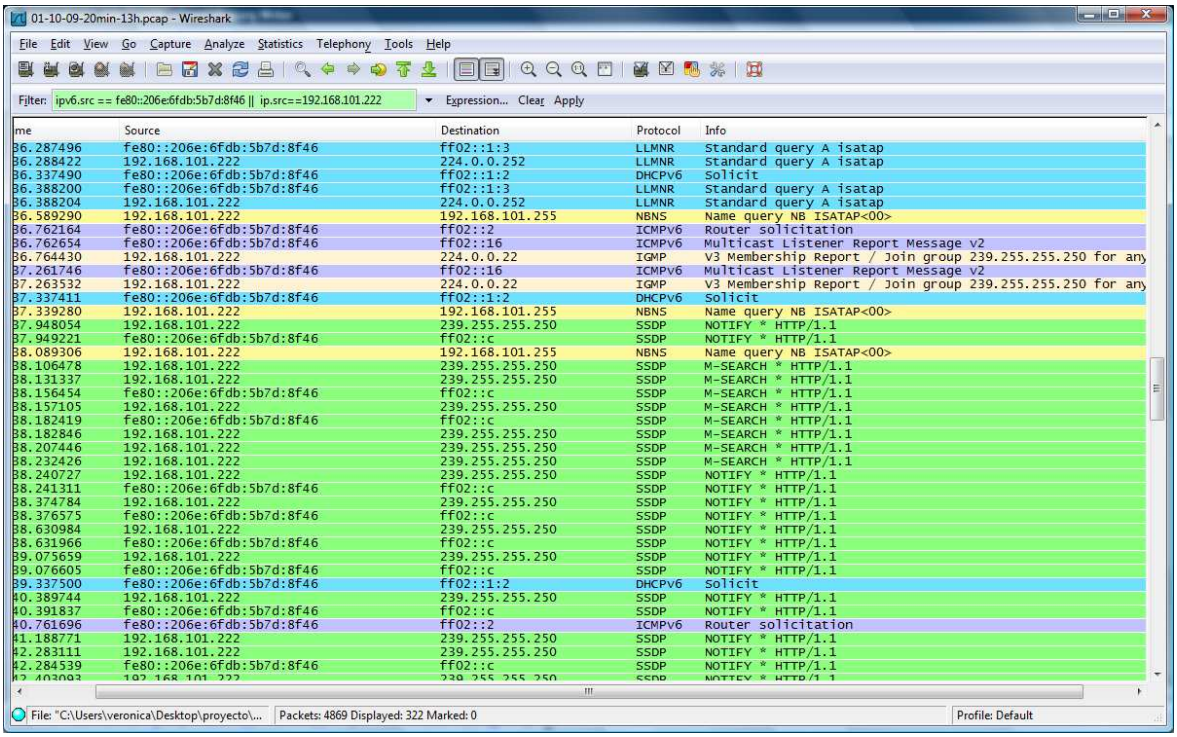


Figura 1.14 Protocolos LLMNR, IGMP, SSDP, DHCPv6, ICMPV6

Fuente: Monitoreo de la red con Wireshark, Octubre 2009

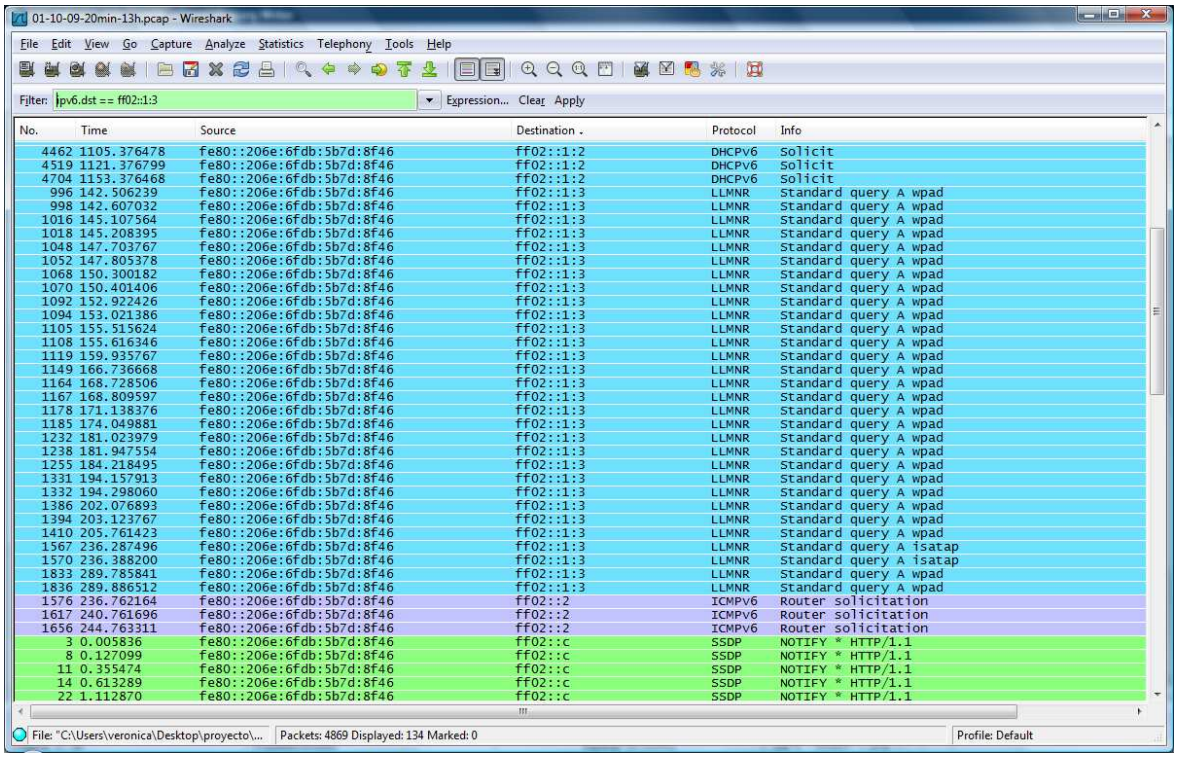


Figura 1.15 Protocolos LLMNR, SSDP, DHCPv6, ICMPV6

Fuente: Monitoreo de la red con Wireshark, Octubre 2009

1.2.8.1.3 Escaneo 15-10-2009

La dirección IP 192.168.101.197 mantiene su envío de paquetes a la dirección broadcast NBNS averiguando por SHV4.NO-IP.BIZ, BOOSTER.ESTR.ES.

1.2.8.1.4 Escaneo 27-10-2009

Existen paquetes broadcast ARP sobre la pregunta de la IP 192.168.101.195 sobre quienes son todas las direcciones IP de la subred.

1.2.8.1.5 Escaneo 01-12-2009

En el Figura 1.16 se puede observar que la dirección IP 192.168.101.93 envía paquetes broadcast con protocolo NBNS preguntando por la dirección IP de: QAIEQD.WS, ICHRNJRF.INFO, OXOCVWH.CN, VWDNIXGS.INFO, EPEDFCRG.WS, KRQFTZYIQR.BIZ, KQZTOZ.ORG, GEYWMWYQ,NET,

TDOQCEW.COM, QBGAI.CC, ACRSKJCROF.INFO, SDHJQQO.NET, NJCLTJ.CC, QDQMXFZS.COM, OWFPYIDP.BIZ, HKDLFVTMM.INFO, IMUREEWS.ORG, XIOLRJR.WS, EPIRBF.ORG, entre otros. Estos dominios son usados por el gusano conficker.

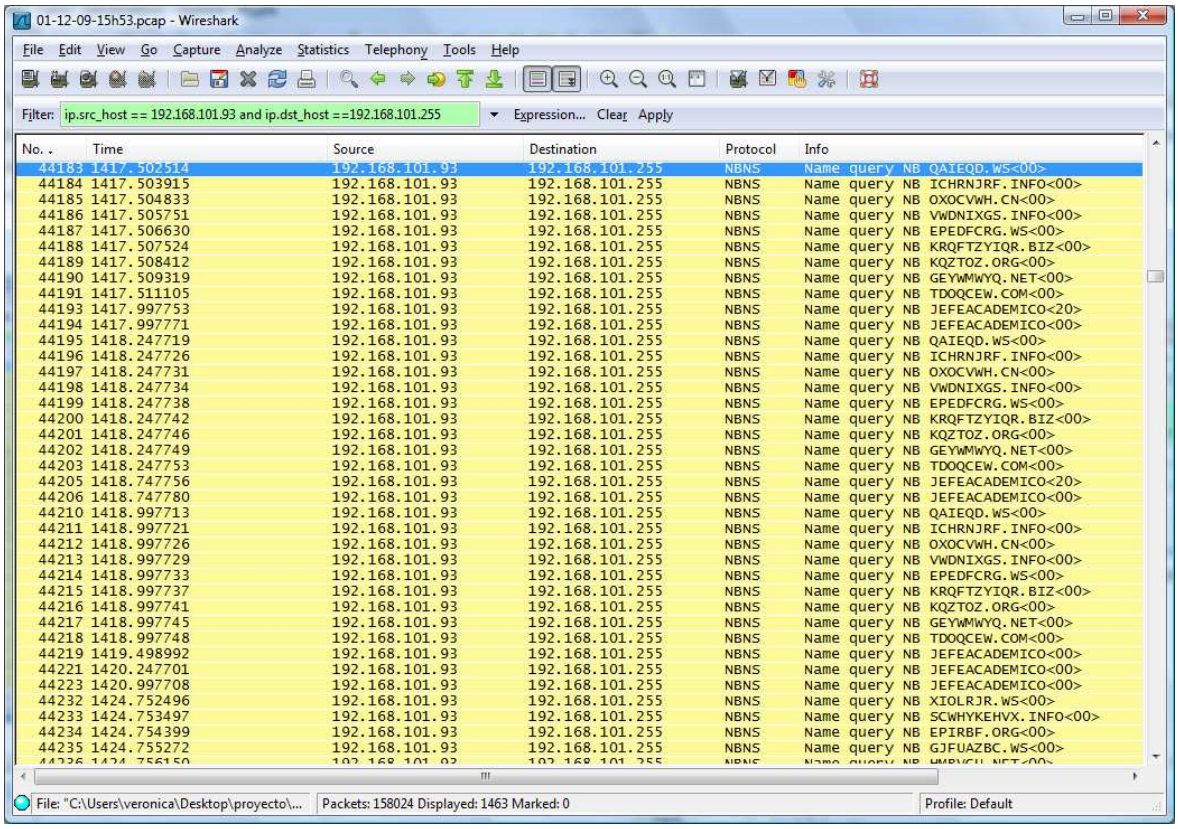


Figura 1.16 Name query a varios dominios identificados con el gusano Conficker
Fuente: Monitoreo de la red con Wireshark, Diciembre 2009

1.2.8.2 Sección Primaria

En el escaneo del 26-01-2010, se pudo detectar actividad inusual del equipo que hace la función de servidor de bases de datos (192.168.110.250), a través del puerto 137, existen envíos de solicitudes broadcast, preguntando por las direcciones IP de ZKARMY.DIP.JP, TONKOR.OR.TP, DIESAM.MOE.HM y LEMOX.MYHOME.CX, identificados como sitios comprometidos por el gusano Harakit, como se puede observar en el Figura 1.17.

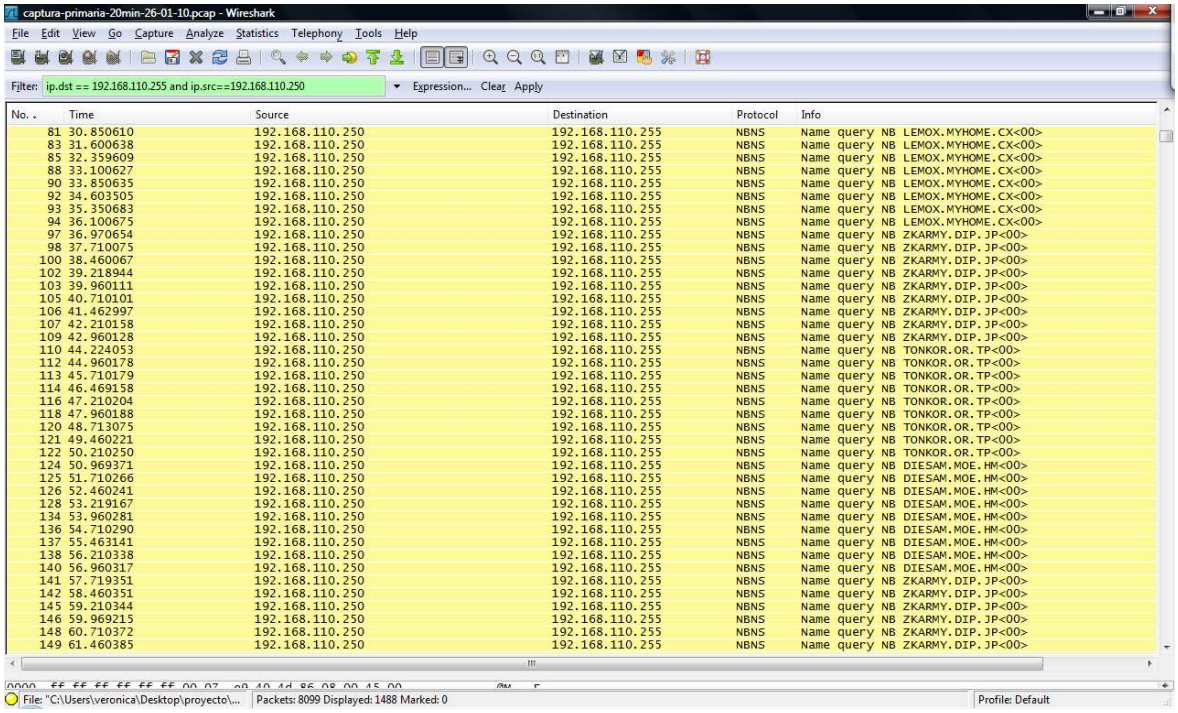


Figura 1.17 Name query a varios dominios identificado con el gusano Harakit

Fuente: Monitoreo de la red con Wireshark, Enero 2010

En las Figuras 1.18, 1.19 y 1.20 se muestra el tráfico broadcast originado desde el computador que actúa como servidor de bases de datos en la sección primaria, como puede observarse en la mayoría de tramos es casi igual al tráfico broadcast total generado por lo que puede concluirse que estos paquetes están inundando la red y esta podría ser una de las causas de la lentitud en el servicio de Internet.

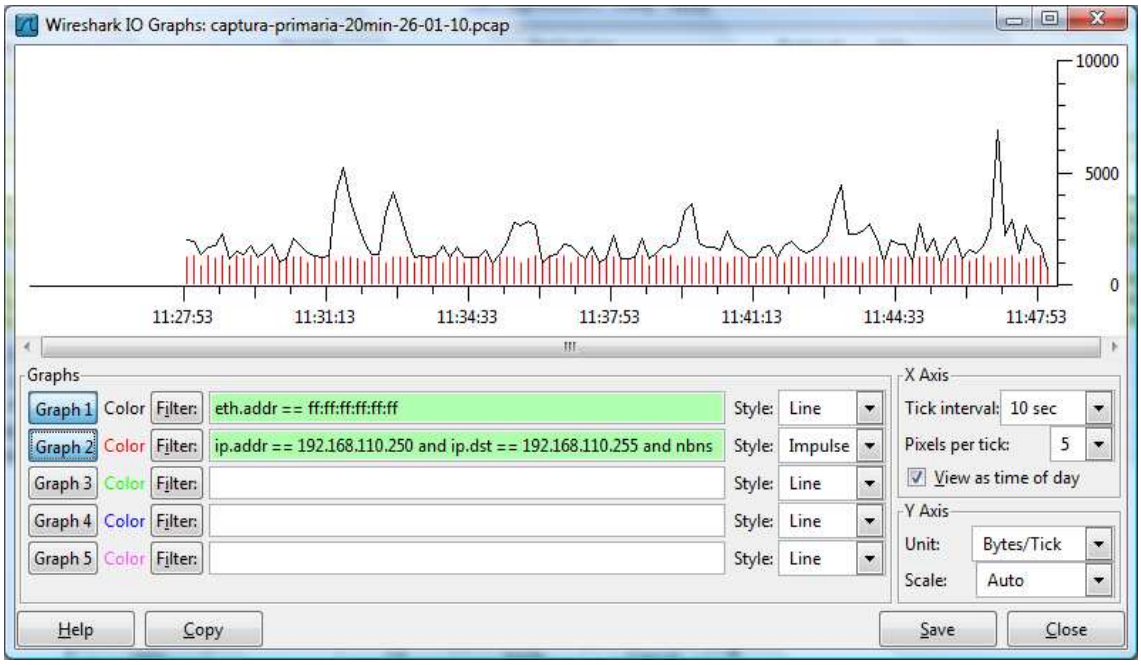


Figura1.18 Tráfico broadcast por bytes en red primaria

Fuente: Monitoreo de la red con Wireshark, 26-01-2010

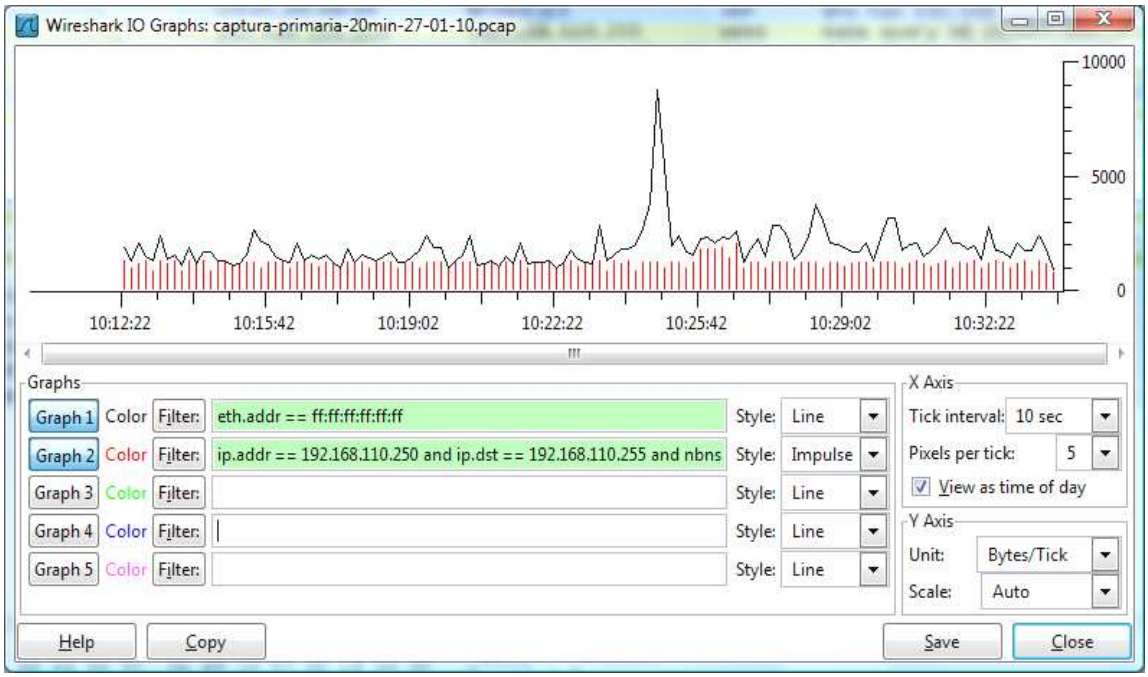


Figura 1.19 Tráfico broadcast por bytes en red primaria

Fuente: Monitoreo de la red con Wireshark, 27-01-2010

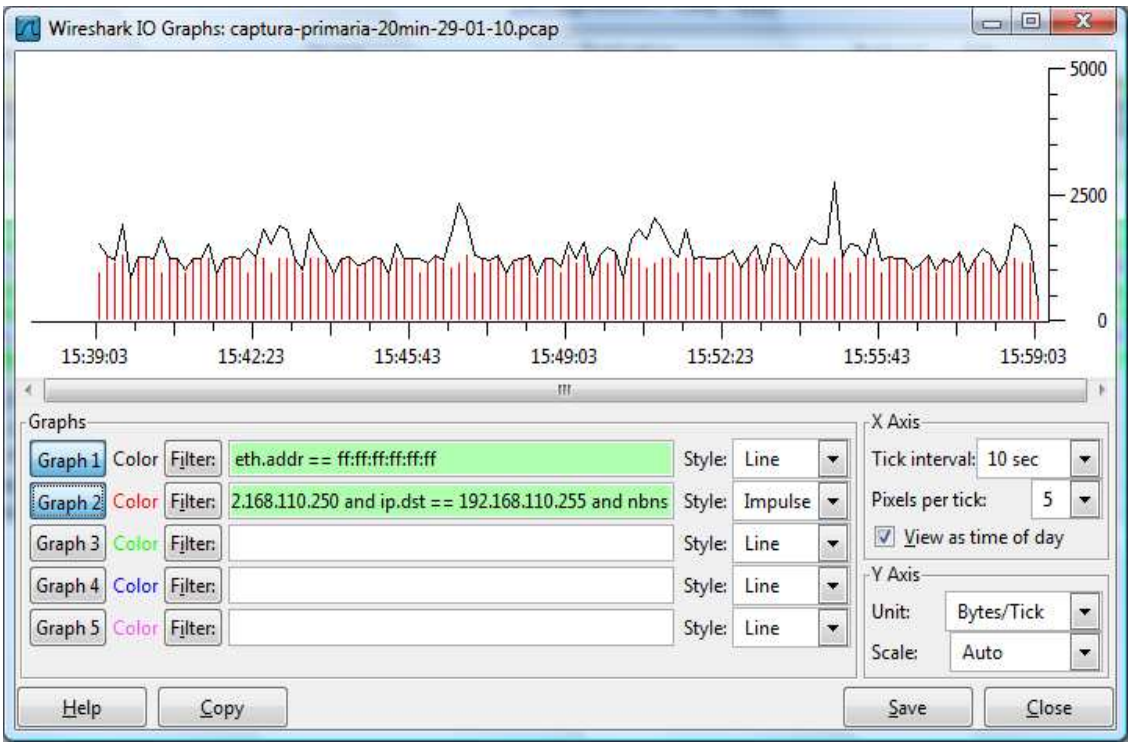


Figura 1.20 Tráfico broadcast por bytes en red primaria

Fuente: Monitoreo de la red con Wireshark, 29-01-2010

1.3 DETERMINACIÓN DE VULNERABILIDADES Y AMENAZAS DE LA RED DE DATOS

Este literal expone la metodología escogida para la determinación de vulnerabilidades y amenazas de la red y presenta los resultados de la misma.

1.3.1 METODOLOGÍA PARA UN TEST DE PENETRACIÓN

Para determinar las vulnerabilidades y amenazas de la red de datos de la Unidad Educativa, se tomó como base la metodología “Penetration Testing Methodology”, emitida por BSI (Federal Office for Information Security), la agencia del gobierno alemán a cargo de la gestión de la seguridad informática y la comunicación, cuyas áreas de especialización y responsabilidad incluyen la seguridad de las aplicaciones informáticas, protección de infraestructuras críticas, seguridad en Internet, criptografía, contra espionaje, la certificación de productos de seguridad

y acreditación de laboratorios de prueba. Esta metodología establece un procedimiento estructurado para realizar un test de intrusión específico.

1.3.1.1 Objetivos

Para que un test de penetración cumpla las expectativas del cliente, la definición clara de los objetivos es absolutamente esencial. Los objetivos que pueden ser alcanzados mediante un test de intrusión son:

- "Mejorar la seguridad de los sistemas técnicos.
- Identificar las vulnerabilidades.
- Tener la seguridad de TI (Tecnologías de Información), confirmada por un tercero externo.
- Mejorar la seguridad de la infraestructura de organización y del personal."[8]

1.3.1.2 Clasificación

La Figura 1.21 muestra una clasificación de los posibles tests de penetración. A la izquierda constan los seis criterios para la definición de los test de penetración, a la derecha aparecen los distintos valores de los criterios resumidos en un diagrama de árbol compacto.

[8]Penetration Test Methodology.

https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/27983/penetration_pdf.pdf, 2005

Criterio:

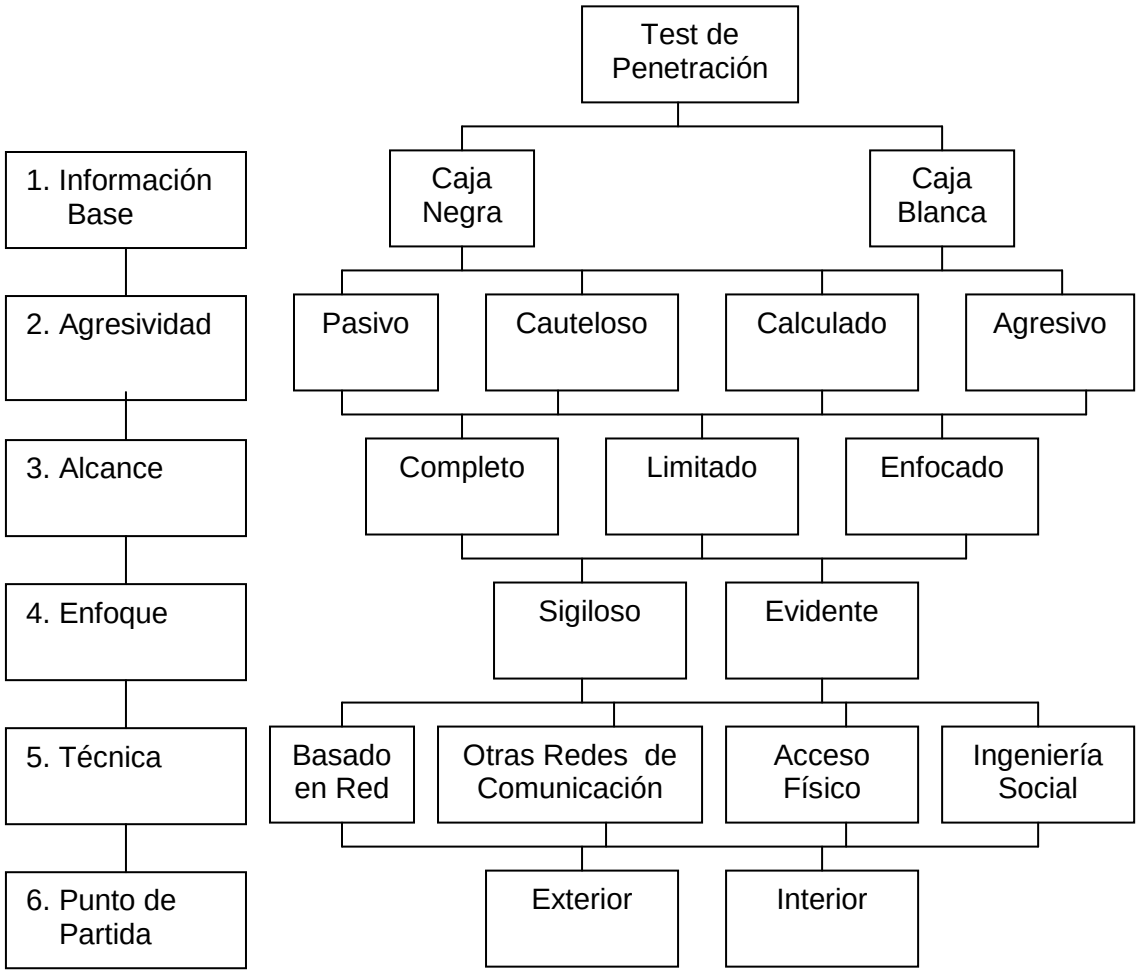


Figura 1.21 Clasificación General de un Test de Penetración

Fuente: Penetration Test Methodology.

https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/27983/penetration_pdf.pdf, 2005

Cabe señalar que no todas las combinaciones posibles son pruebas útiles, en el caso de aplicar un test agresivo, este podría ser identificado rápidamente, y esto no es ideal en combinación con técnicas de ocultación. Del mismo modo, un test de penetración público podría no ser adecuado en el caso de querer obtener información confidencial de los empleados mediante técnicas de ingeniería social que han sido advertidos con antelación.

1.3.1.3 Fases

1.3.1.3.1 Fase 1: Preparación

Los objetivos y alcance del test de penetración deben aclararse y definirse con la Unidad Educativa. El tester debe asegurarse que los procedimientos del test no van a infringir las disposiciones legales y que los riesgos asociados a las técnicas utilizadas hayan sido discutidos y documentados.

1.3.1.3.2 Fase 2: Reconocimiento

El tester comienza a reunir información acerca del objetivo, es el test de penetración pasivo, el objetivo es obtener una visión completa y detallada de los sistemas instalados mediante: análisis de datos publicados, escaneo de puertos, identificación de sistemas y aplicaciones, identificación de equipos activos de la red e investigación de vulnerabilidades, incluyendo áreas abiertas a un ataque o deficiencias de seguridad conocidas. El tiempo necesario para ejecutar cada paso del test debe ser planificado con cuidado, tomando en cuenta el tamaño de la red que se examine.

1.3.1.3.3 Fase 3: Análisis de Información de Riesgos

El análisis y evaluación de la información obtenida en la fase debe incluir los objetivos definidos del test de penetración, los riesgos potenciales para el sistema y el tiempo previsto requerido para la evaluación de las fallas de seguridad potenciales para los intentos de penetración activa posterior. Los objetivos de la fase 4 son seleccionados en base a este análisis. De la lista de sistemas identificados el tester elige aquellos de los cuales está bien informado.

1.3.1.3.4 Fase 4: Intentos Activos de Penetración

Los sistemas seleccionados son atacados activamente. Esta fase implica el riesgo más alto en un test de penetración y debe realizarse con el debido cuidado.

Para sistemas con muy alta disponibilidad o requerimientos de integridad, los efectos potenciales deben ser cuidadosamente considerados antes de realizar procedimientos críticos de prueba, por lo cual existe la posibilidad de excluir esta fase del test seleccionado.

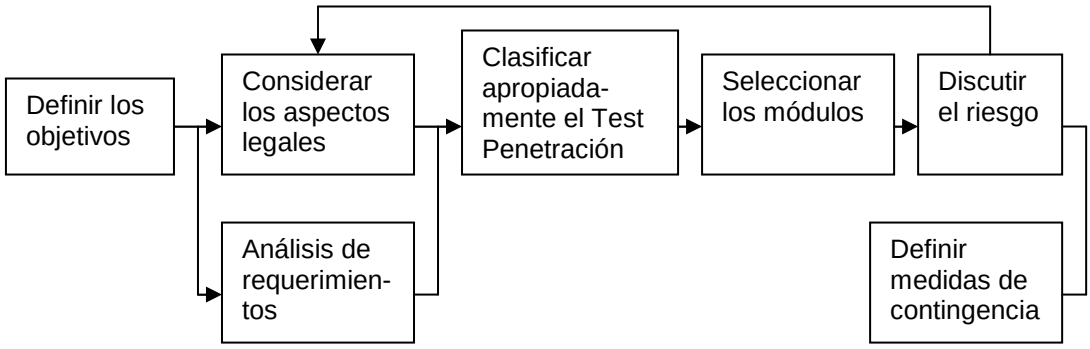
1.3.1.3.5 Fase 5: Análisis Final

El informe final debe contener una evaluación de las vulnerabilidades detectadas, los de riesgos potenciales y las recomendaciones para eliminarlos.

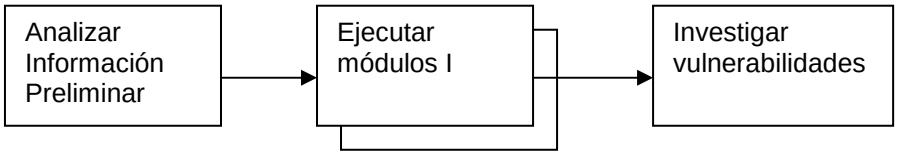
1.3.1.4 Enfoque

El enfoque descrito en la Figura 1.22 logra que la documentación del test de penetración sea recogida durante todas las fases, esto asegura que los pasos del test y los resultados de todas las fases sean documentados y hace el test de penetración transparente y trazable.

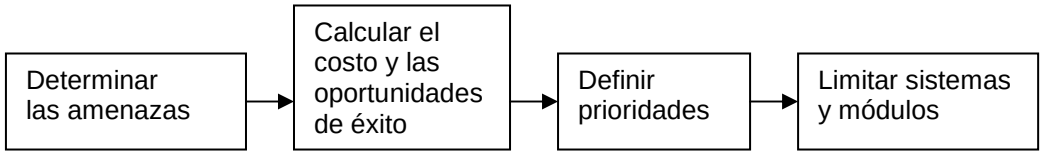
Fase 1: Preparación



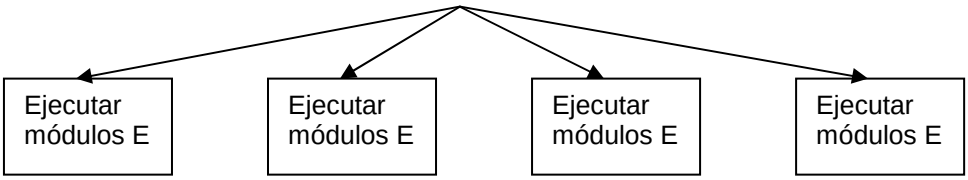
Fase 2: Reconocimiento



Fase 3: Análisis de Información y Riesgos



Fase 4: Intentos de Intrusión Activos



Fase 5: Análisis Final

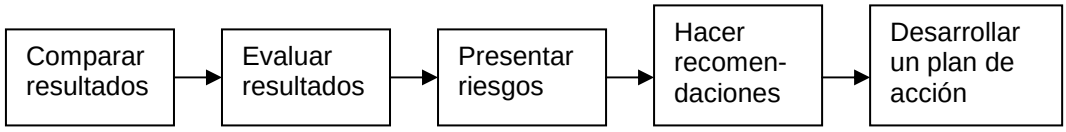


Figura 1.22 Fases del Test de Penetración

Fuente: Penetration Test Methodology.

https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/27983/penetration_pdf.pdf, 2005

1.3.1.5 Módulos

El enfoque descrito no contiene procedimientos explícitos de testeo, menciona únicamente la realización de los módulos I y E. Tomando como base la metodología OSSTMM (Open Source Security Testing Methodology Manual) han sido agrupados juntos en módulos para el Reconocimiento e Intentos Activos de Intrusión.

1.3.1.5.1 Módulos de Reconocimiento

La Tabla 1.8 muestra la lista de los módulos para el reconocimiento.

Nro.	Módulos
I1	Análisis de Datos Publicados
I2	Consulta Sigilosa de Información Básica de la Red
I3	Consulta Evidente de Información Básica de la Red
I4	Escaneo Sigiloso de Puertos
I5	Escaneo Evidente de Puertos
I6	Identificación de Aplicaciones
I7	Identificación de Sistemas
I8	Identificación Sigilosa del Router
I9	Identificación Evidente del Router
I10	Identificación Sigilosa del Firewall
I11	Identificación Evidente del Firewall
I12	Investigación de Vulnerabilidades
I13	Identificación de Vulnerabilidades en las Interfaces de Aplicación
I14	Recolección de Información para la Ingeniería Social
I15	Recolección de Información basada en Informática para Ingeniería Social
I16	Recolección de Información personal para Ingeniería Social
I17	Pruebas de Comunicación Inalámbrica
I18	Pruebas del Sistema Telefónico
I19	Pruebas del Sistema de Correo de Voz
I20	Pruebas del Sistema de Fax
I21	Análisis del Entorno Físico
I22	Identificación del Control de Acceso

Tabla 1.8 Módulos de Reconocimiento

Fuente: Penetration Test Methodology.

https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/27983/penetration_pdf.pdf, 2005

1.3.1.5.2 Módulos de Intentos Activos de Intrusión

La Tabla 1.9 contiene la lista de los módulos para intentos activos de intrusión

Nro.	Módulos
E1	Verificación Sigilosa de Vulnerabilidades Actuales
E2	Verificación Evidente de Vulnerabilidades Actuales
E3	Verificación de las Vulnerabilidades Actuales en las Interfaces de Aplicación
E4	Prueba Sigilosa del Router
E5	Prueba Evidente del Router
E6	Prueba de Sistemas Confiados
E7	Prueba Sigilosa de Firewall desde el Exterior
E8	Prueba Evidente de Firewall desde el Exterior
E9	Prueba del Firewall desde ambos lados
E10	Prueba del Sistema de Detección de Intrusos
E11	Intercepción de Contraseñas
E12	Descrifrado de Contraseñas
E13	Pruebas de sensibilidad para ataques DoS
E14	Ingeniería Social basado en Informática
E15	Ingeniería Social directa al Personal con Acceso Físico
E16	Ingeniería Social indirecta al Personal sin Acceso Físico
E17	Pruebas de Comunicación Inalámbrica
E18	Pruebas de Acceso Administrativo al Sistema Telefónico
E19	Pruebas del Sistema de Correo de Voz
E20	Pruebas de Puntos de Acceso Administrativo al Sistema de Fax
E21	Pruebas del MODEM
E22	Pruebas del Control de Acceso
E23	Procedimientos para Pruebas de Contención

Tabla 1.9 Módulos para Intentos Activos de Intrusión

Fuente: Penetration Test Methodology.

https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/27983/penetration_pdf.pdf, 2005

1.3.1.5.3 Principio de Exclusión

Tomando en cuenta la clasificación seleccionada, los módulos que no se pueden realizar debido al enfoque escogido serán excluidos del test. Si un módulo no se excluye, los pasos del test que figuran en él deben llevarse a cabo, lo que contribuye a garantizar un test de penetración exhaustivo. Si un módulo ha de ser excluido por otras razones, estas razones deben estar establecidas y documentadas.

La clasificación elegida entonces determina a través del principio de exclusión cuáles módulos de reconocimiento y de penetración activa no se puede realizar.

La Figura 1.23 muestra encerrado en paréntesis los módulos que serán excluidos para cada uno de los criterios.

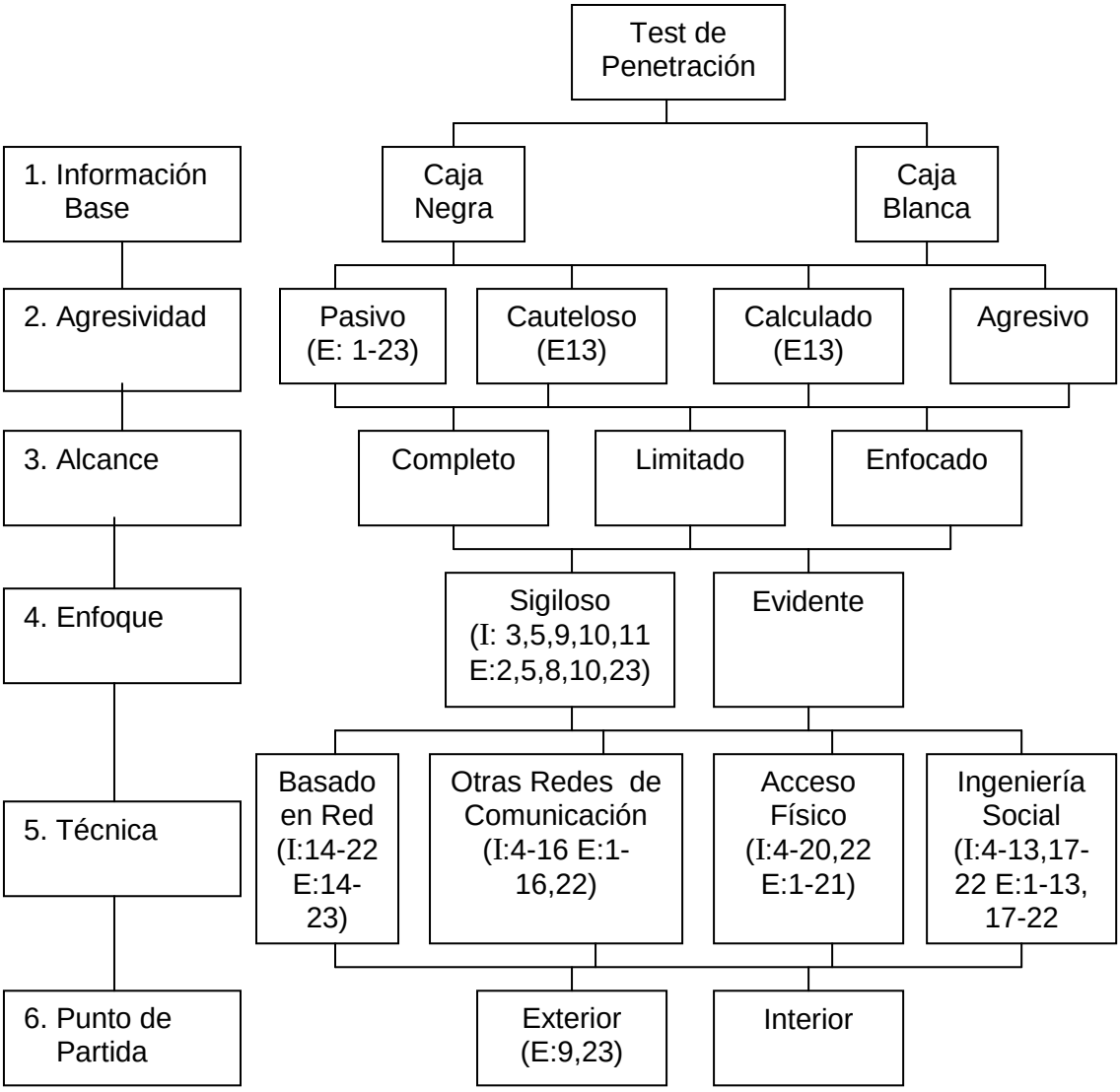


Figura 1.23 Principio de Exclusión

Fuente: Penetration Test Methodology.

https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/27983/penetration_pdf.pdf, 2005

1.3.2 EJECUCIÓN DEL TEST DE PENETRACIÓN

En esta sección se ejecuta el test de penetración, iniciando con la selección de las herramientas de escaneo a utilizar, tomando en cuenta los siguientes criterios:

- Instalación y configuración
- Tipo de distribución y plataforma
- Facilidad para generar reporte

- Flexibilidad de la herramienta
- Documentación adecuada

Luego de un análisis de las herramientas más conocidas para realizar tareas tales como: escaneo de puertos, identificación de servicios, banners, escaneo de vulnerabilidades y amenazas, se han seleccionado las siguientes:

- Nmap 5.21
- ScanLine 1.01
- Nessus 4.0
- GFILANguard
- ParosProxy 3.2.13

1.3.2.1 Fase 1: Preparación

Los objetivos para ejecutar el test de penetración son:

- Mejorar la seguridad de los equipos en la red.
- Identificar las vulnerabilidades y amenazas de los equipos activos de la red.
- Alcanzar una seguridad confirmada por terceros.

Tomando en cuenta el detalle de las Figuras 1.21 y 1.23 donde aparece la clasificación y el principio de exclusión, además en base a las expectativas y requerimientos del Jefe del Centro de Informática, se ha seleccionado la propuesta que consta en la Tabla 1.10, la cual cubre con la totalidad de los objetivos presentados.

		Principio de Exclusión	
Criterio	**Valor**	**Módulos I**	**Módulos E**
1. Información Base	Caja Negra	-	-
2. Agresividad	Pasivo	-	1 – 23
3. Alcance	Limitado	-	-
4. Enfoque	Sigiloso	3, 5, 9, 10, 11	2, 5, 8, 10, 23
5. Técnica	Basado en Red	14 – 22	14 – 23
6. Punto de Partida	Exterior	-	9, 23
Módulos Excluidos		3, 5, 9, 11, 14 - 22	1 - 23

Tabla 1.10 Test de Penetración Seleccionado

La posibilidad de que el rendimiento de la red se vea afectado, obligó a considerar la ejecución de un test pasivo.

Las medidas que se tomaron para la fase de reconocimiento son:

- El análisis de vulnerabilidades comenzó una vez el Rector de la Unidad Educativa aprobó esta actividad y designó a un miembro del Centro de Informática como responsable del monitoreo y control de las pruebas que se realicen dentro de la institución.

- Las herramientas utilizadas fueron ejecutadas inicialmente en un equipo de prueba, para conocer su funcionamiento y posibles resultados.

- Las vulnerabilidades detectadas y catalogadas como críticas se informaron inmediatamente al responsable del monitoreo y control de las pruebas.

Los servicios, equipos activos y servidores seleccionados para la aplicación del test de intrusión son:

- Los servidores de bases de datos
- Los servidores Proxy

- Los routers externos

1.3.2.2 Fase 2: Reconocimiento

Una vez definidos los objetivos, el alcance y discutidos los riesgos asociados con el test, se ejecutan los módulos I.

1.3.2.2.1 I1: Análisis de Datos Publicados

Mediante este análisis, el tester trata de obtener información sobre la empresa, sus empleados, la tecnología utilizada.

Resultados esperados:	Perfil de la empresa Perfil de los empleados Reconocimiento de asociados

Pasos de Prueba:

- Buscar información en la página inicial de la empresa

La dirección Web de la página inicial de la institución es http://www.comil10.edu.ec, la información proporcionada está relacionada con los servicios que presta la Unidad Educativa, las especialidades que oferta, el detalle del proceso de inscripción y matrícula, su ubicación, servicio teleacadémico, información referente a LOTAIP (Ley Orgánica de Transparencia y Acceso a la Información Pública), donde consta el presupuesto de la institución y la lista del personal docente de la institución, con sus títulos académicos y el nombre de la universidad donde los obtuvieron.

- Buscar información relevante en los grupos de noticias

Los grupos de noticias revisados son:

- ✓ http://www.hoy.com.ec
- ✓ http://www.elcomercio.ec

- ✓ http://www.metrohoy.com.ec
- ✓ http://www.eluniverso.com.ec

La información encontrada fue del año 2003, referente a triunfos en concursos de bandas de guerra y eventos deportivos, donde se revelan nombres de algunos cadetes participantes y entrenadores.

- Investigar información en bases de datos públicas

Las bases de datos públicas revisadas son:

- ✓ http://www.google.com.ec
- ✓ http://www.yahoo.com

La información encontrada está relacionada con la gratuidad de los colegios militares a partir de enero del 2011 y las opiniones de diversos sectores.

1.3.2.2.2 I2: Consulta Sigilosa de Información Básica de la Red

Resultados esperados:	Nombres de dominio Rangos de direcciones IP Nombres de hosts Direcciones IP Descripción de los servidores y funciones Información del ISP Contacto administrativo

Requerimientos

- Direcciones IP/Rango IP o Dominio/Nombres del servidores

La investigación se inicia a partir del dominio de Internet “comil10.edu.ec”.

Pasos de Prueba:

- Consultar la base de datos Whois. Ver Tabla 1.11.

Registrante: Colegio Militar 10 Crnl. E.M. Franco Ordóñez G. comil10@yahoo.es Telf:5932-2658374 Fax:5932-2662695 Av. Mariscal Sucre S/N y Michelena Quito, Pichincha, Ecuador
Nombre de Dominio: comil10.edu.ec
Contacto Administrativo: Telconet S.A. Igo Krochin ikrochin@uio.telconet.net Telf: 5932-3963100 Fax:5932-2435856 Pedro Gosseal 148 y Moriano Echeverría Quito, Pichincha, Ecuador
Contacto Técnico y de Facturación Telconet S.A. Departamento Dominios dominios@telconet.net Telf: 5932-3963100 Fax: 5932-2435856 Pedro Gosseal 148 y Moriano Echeverría Quito, Pichincha, Ecuador
Fecha de expiración del dominio: 27-Enero-2011 **Fecha de creación del dominio:** 27-Enero-2006 **Fecha de última modificación del registro**: 27-Enero-2010
Nombres de Servidores DNS listados en orden: uio.telconet.net uio.telconet.net

Tabla 1.11 Whois del dominio “comil10.edu.ec”

Fuente: http://www.nic.ec/reg/whois.asp?dominio=comil10.edu.ec, Diciembre 2009

- Consultar servidores de nombres.

Si la consulta se envía de alguno de los equipos de la red, no se obtiene respuesta por cuanto no existe servidor DNS, sin embargo al hacerlo desde el servidor Proxy se obtuvo la siguiente respuesta:

Server: 200.93.216.2
Address: 200.93.216.2#53

Name: comil10.edu.ec
Address: 200.93.192.99

- Examinar las cabeceras de los correos electrónicos.

Se examinó una cabecera de un email enviado desde un equipo en la Unidad Educativa a una cuenta de Hotmail. La cabecera resultante es la siguiente:

```
X-Message-Delivery: Vj0xLjE7dXM9MDtsPTE7YT0xO0Q9MDtTQ0w9MA==
X-Message-Status: n:0
X-SID-PRA: =?iso-8859-1?B?VmVy8m5pY2EgTWFydOxuZXogRXNwaW5lbA==?=
<veromartinez55@hotmail.com>
X-SID-Result: Pass
X-AUTH-Result: PASS
X-Message-Info:
JGTYoYF78jGuWFBuhofpQrqW+74VrIIJ3IDsjLg618DLgINpp54uggUOOjRT6VEFGqG+69igT
nUKY/ZjUACU27vyMPzPUo3l
Received: from bay0-omc1-s12.bay0.hotmail.com ([65.54.190.23]) by bay0-
hmmc2-f21.Bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);
         Thu, 20 May 2010 06:10:58 -0700
Received: from BAY139-W21 ([65.54.190.61]) by bay0-omc1-
s12.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.4675);
         Thu, 20 May 2010 06:10:55 -0700
Message-ID: <BAY139-W218BE667D9A3A218B3BEE2D3E30@phx.gbl>
Return-Path: veromartinez55@hotmail.com
Content-Type: multipart/mixed;
        boundary="_ff775c63-c891-40bb-bc29-45c5a44cda79_"
X-Originating-IP: [190.95.172.98]
From: =?iso-8859-1?B?VmVy8m5pY2EgTWFydOxuZXogRXNwaW5lbA==?=
       <veromartinez55@hotmail.com>
To: <veromartinez55@hotmail.com>, <veromartinez55@gmail.com>
Subject: biblioteca
Date: Thu, 20 May 2010 13:10:55 +0000
Importance: Normal
MIME-Version: 1.0
X-OriginalArrivalTime: 20 May 2010 13:10:55.0994 (UTC)
FILETIME=[E1D345A0:01CAF81D]
```

```
--_ff775c63-c891-40bb-bc29-45c5a44cda79_
Content-Type: multipart/alternative;
        boundary="_d1cac4c4-9637-4924-8b11-0b5d83fbf2b9_"

--_d1cac4c4-9637-4924-8b11-0b5d83fbf2b9_
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
```

Como puede observarse, la dirección X-Originating-IP es 190.95.172.98, la cual corresponde a una de las direcciones configuradas en el servidor Proxy de la sección secundaria.

- Examinar la información HTML contenida en el sitio Web en busca de enlaces externos o comentarios.

Al examinar la información del código HTML del sitio Web se encontró una referencia a un enlace externo, como se puede observar en la Tabla 1.12.

```
src="file:///C|/./assets/images/autogen/clearpixel.gif" alt="" border="0"
height="1" width="12"></td>
              <td> <p> </p>
                <p><font size="1"><strong><em><font color="#00ccff"
size="2">PARA
                  OBTENER MAYOR INFORMACION SOBRE LOS CADETES DEL COMIL
No. 10</font></em></strong></font></p>
                <p><font color="#00ccff" size="2"><em><strong>OPRIMA
AQUI:</strong></em></font></p>
                <p><a href="http://www.c-3.com.ec/abdon.asp"><img
src="./Imagenes/logo_teleacademico.JPG" border="0"
```

Tabla 1.12 Fragmento de código HTML del sitio Web de la institución

Fuente: http://www.comil10.edu.ec/index.html, Enero 2010

Este fragmento de script pertenece a la codificación del servicio teleacadémico y direcciona el acceso hacia la dirección web: http://www.c-3.com.ec/abdon.asp.

Examinando el dominio “c-3.com.ec” en http://www.nic.ec, se encontró que el dominio está registrado a nombre de Jacqueline Guerrón, quien no pertenece a Telconet ni a la Unidad Educativa, por lo tanto se concluyó que es un tercero quien ofrece este servicio.

- Buscar ofertas de puestos de trabajo en tecnologías de información de la empresa para analizar referencias de hardware y software.

No existen ofertas de trabajo en tecnologías de la información relacionadas con la Unidad Educativa. Se realizó la búsqueda en las páginas Web:

http://www.computrabajo.com.ec
http://www.porfinempleo.com
http://www.multitrabajos.com

1.3.2.2.3 I4: Escaneo Sigiloso de Puertos

Se ejecuta un escaneo sigiloso de los puertos en todos los equipos que actúan como servidores para conocer los servicios que ofrecen y bajo que sistema operativo.

Resultados esperados:	Información de los servicios ofrecidos por los dispositivos

Requerimientos:

- Conocimiento de información básica de la red

Pasos de Prueba:

- Ejecutar un escaneo de puertos que sea difícil de detectar.

La herramienta empleada para realizar el escaneo de puertos fue NMAP 5.21, un software libre con licencia Open Source muy útil para auditoría de seguridad y exploración de la red.

NMAP utiliza paquetes IP para determinar entre otras características: los hosts que están disponibles en la red, los servicios ofrecen, los sistemas operativos que

están corriendo, los filtros que están en uso, incluye además de la interfaz de comandos una interfaz gráfica de usuario y un visor de resultados.

Los escaneos fueron realizados tanto desde la red interna como fuera de ella, se utilizó escaneos tipo SYN y FIN con la finalidad de ejecutarlos de forma sigilosa, el detalle de los mismos aparece en el Anexo 3.

Las Tablas 1.13, 1.14, 1.15, 1.16, 1.17, 1.18, 1.19 y 1.20 muestran un resumen de los resultados del escaneo de puertos en los equipos objetivo.

Puerto	Servicio	ESCANEO		
		TCP SYN	TCP FIN	UDP
23	telnet	Abierto	Abierto	-----
25	smtp	Abierto	Abierto	-----
80	http	Abierto	Abierto	-----
110	pop3	Abierto	Abierto	-----
3128	squid-http	Abierto	Abierto	-----
10000	webmin-httpd	Abierto	Abierto	-----
1023	unknown	-----	-----	Abierto/Filtrado
3130	squid-ipc	-----	-----	Abierto/Filtrado
3457	vat_control	-----	-----	Abierto/Filtrado
9199	unknown	-----	-----	Abierto/Filtrado
9876	sd	-----	-----	Abierto/Filtrado
10000	unknown	-----	-----	Abierto/Filtrado
16680	unknown	-----	-----	Abierto/Filtrado
16938	unknown	-----	-----	Abierto/Filtrado
17219	unknown	-----	-----	Abierto/Filtrado
18883	unknown	-----	-----	Abierto/Filtrado
18958	unknown	-----	-----	Abierto/Filtrado
19096	unknown	-----	-----	Abierto/Filtrado
19933	unknown	-----	-----	Abierto/Filtrado
19995	unknown	-----	-----	Abierto/Filtrado
20117	unknown	-----	-----	Abierto/Filtrado
21524	unknown	-----	-----	Abierto/Filtrado
32771	sometimes-rpc6	-----	-----	Abierto/Filtrado
34861	unknown	-----	-----	Abierto/Filtrado
40805	unknown	-----	-----	Abierto/Filtrado
44946	unknown	-----	-----	Abierto/Filtrado
49196	unknown	-----	-----	Abierto/Filtrado
57409	unknown	-----	-----	Abierto/Filtrado
58797	unknown	-----	-----	Abierto/Filtrado

Tabla 1.13 Escaneo Sigiloso de puertos en Proxy Secundaria.
Ver Anexo 3 Escaneo con NMAP (A3-1, A3-4)

Puerto	Servicio	ESCANEO		
		TCP SYN	TCP FIN	UDP
22	Ssh	Abierto	Abierto	-----
23	telnet	-----	Abierto/Filtrado	-----
110	Pop3	-----	Abierto	-----
111	rpcbind	-----	Abierto/Filtrado	-----
3128	squid-http	Abierto	Abierto	-----
6000	X11	-----	Abierto/Filtrado	
10000	Webmin-httpd	Abierto	Abierto	-----
32768	rpcbind	Abierto	Abierto	-----
1048	unknown	-----	-----	Abierto/Filtrado
1485	lansource	-----	-----	Abierto/Filtrado
3130	squid-ipc	-----	-----	Abierto/Filtrado
4666	edonkey	-----	-----	Abierto/Filtrado
5555	rplay	-----	-----	Abierto/Filtrado
10000	webmin	-----	-----	Abierto
16862	unknown	-----	-----	Abierto/Filtrado
17823	unknown	-----	-----	Abierto/Filtrado
19140	unknown	-----	-----	Abierto/Filtrado
20409	unknown	-----	-----	Abierto/Filtrado
20717	unknown	-----	-----	Abierto/Filtrado
27444	Trinoo_Bcast	-----	-----	Abierto/Filtrado
32768	status	-----	-----	Abierto
32769	unknown	-----	-----	Abierto/Filtrado
33249	unknown	-----	-----	Abierto/Filtrado
33459	unknown	-----	-----	Abierto/Filtrado
34422	unknown	-----	-----	Abierto/Filtrado
36108	unknown	-----	-----	Abierto/Filtrado
42172	unknown	-----	-----	Abierto/Filtrado
43195	unknown	-----	-----	Abierto/Filtrado
44179	unknown	-----	-----	Abierto/Filtrado
49167	unknown	-----	-----	Abierto/Filtrado
49200	unknown	-----	-----	Abierto/Filtrado
49214	unknown	-----	-----	Abierto/Filtrado
49262	unknown	-----	-----	Abierto/Filtrado

Tabla 1.14 Escaneo Sigiloso de puertos en Proxy Primaria
Ver Anexo 3 Escaneo con NMAP (A3-18, A3-21)

Examinando los resultados arrojados por el escaneo de los servidores Proxy, se puede notar que existen varios puertos TCP abiertos que no responden a la función de los equipos, los cuales se convierten en posibles vulnerabilidades.

El escaneo UDP no es determinante pues reporta la posibilidad que varios puertos podrían estar abiertos o que existe un filtro de paquetes bloqueando la comunicación, tampoco fue posible determinar el servicio que corre en la mayoría de los puertos, sin embargo en los que si fue posible, se puede identificar servicios relacionados con troyanos, tal como: Trinoo_Bcast en el puerto 27444 y servicios que no están de acuerdo con la función de los equipos tal como: edonkey en el puerto 4666, el cual sirve para el intercambio de archivos P2P.

Puerto	**Servicio**	**ESCANEO**		
		TCP SYN	**TCP FIN**	**UDP**
135	msrpc	Abierto	Cerrado	-----
139	netbios-ssn	Abierto	Cerrado	-----
445	microsoft-ds	Abierto	Cerrado	-----
1025	NFS-or-IIS	Abierto	Cerrado	-----
1026	LSA-or-nterm	Abierto	Cerrado	-----
2041	interbase	Abierto	Cerrado	-----
123	ntp	-----	-----	Abierto/Filtrado
137	netbios-ns	-----	-----	Abierto
138	netbios-dgm	-----	-----	Abierto/Filtrado
445	microsoft-ds	-----	-----	Abierto/Filtrado
500	isakmp	-----	-----	Abierto/Filtrado
1027	unknown	-----	-----	Abierto/Filtrado
4500	Nat-t-ike	-----	-----	Abierto/Filtrado

Tabla 1.15 Escaneo Sigiloso de puertos en Servidor Bases de Datos 1 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-9, A3-12)

Puerto	Servicio	ESCANEO		
		TCP SYN	TCP FIN	UDP
135	msrpc	Abierto	Cerrado	-----
139	netbios-ssn	Abierto	Cerrado	-----
1027	IIS	Abierto	Cerrado	-----
135	msrpc	-----	-----	Abierto
137	netbios-ns	-----	-----	Abierto
138	netbios-dgm	-----	-----	Abierto/Filtrado

Tabla 1.16 Escaneo Sigiloso de puertos en Servidor Bases de Datos 2 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-14, A3-16)

Puerto	Servicio	ESCANEO		
		TCP SYN	TCP FIN	UDP
135	Msrpc	Abierto	Cerrado	-----
139	netbios-ssn	Abierto	Cerrado	-----
445	microsoft-ds	Abierto	Cerrado	-----
123	Ntp	-----	-----	Abierto
137	netbios-ns	-----	-----	Abierto
138	netbios-dgm	-----	-----	Abierto/Filtrado
445	microsoft-ds	-----	-----	Abierto/Filtrado
500	Isakmp	-----	-----	Abierto/Filtrado
1900	Upnp	-----	-----	Abierto/Filtrado
4500	Nat-t-ike	-----	-----	Abierto/Filtrado

Tabla 1.17 Escaneo Sigiloso de puertos en Servidor Bases de Datos Primaria
Ver Anexo 3 Escaneo con NMAP (A3-25, A3-27)

Examinando los resultados arrojados por el escaneo de los servidores de bases de datos, se puede notar que existen varios puertos TCP abiertos que no responden a la función de los equipos, tal como el IIS y LSA o que brindan servicios redundantes como el que corre en los puertos 139 y 445 y que además

se convierte en un riesgo de seguridad por cuanto ambos permiten la propagación de virus en la red.

Tener abierto el puerto 135 puede convertirse también en una vulnerabilidad sin embargo es necesario cuando se comparten recursos en la red.

El escaneo UDP no es determinante pues reporta la posibilidad que varios puertos podrían estar abiertos o que existe un filtro de paquetes bloqueando la comunicación, sin embargo fue posible determinar los servicios que corren en dichos puertos.

Puerto	**Servicio**	**ESCANEO**		
		TCP SYN	**TCP FIN**	**UDP**
110	pop3-proxy	-----	Abierto	-----
67	dhcps	-----	-----	Abierto/Filtrado
135	msrpc	-----	-----	Abierto/Filtrado
137	netbios-ns	-----	-----	Abierto/Filtrado
138	netbios-dgm	-----	-----	Abierto/Filtrado
161	snmp	-----	-----	Abierto
162	snmptrap	-----	-----	Abierto/Filtrado
445	microsoft-ds	-----	-----	Abierto/Filtrado
1434	Ms-sql-m	-----	-----	Abierto/Filtrado

Tabla 1.18 Escaneo Sigiloso de puertos en Router 1 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-50, A3-52)

Puerto	Servicio	ESCANEO		
		TCP SYN	TCP FIN	UDP
80	http	Abierto	Abierto	-----
110	pop3-proxy	-----	Abierto	-----
113	auth	-----	Cerrado	-----
67	dhcps	-----	-----	Abierto/Filtrado
135	msrpc	-----	-----	Abierto/Filtrado
137	netbios-ns	-----	-----	Abierto/Filtrado
138	netbios-dgm	-----	-----	Abierto/Filtrado
161	snmp	-----	-----	Abierto
162	snmptrap	-----	-----	Abierto/Filtrado
445	microsoft-ds	-----	-----	Abierto/Filtrado
1434	Ms-sql-m	-----	-----	Abierto/Filtrado

Tabla 1.19 Escaneo Sigiloso de puertos en Router 2 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-30, A3-33)

Puerto	Servicio	ESCANEO		
		TCP SYN	TCP FIN	UDP
80	http	-----	Cerrado	-----
110	pop3-proxy	-----	Abierto	-----
113	auth	-----	Cerrado	-----
67	dhcps	-----	-----	Abierto/Filtrado
135	msrpc	-----	-----	Abierto/Filtrado
137	netbios-ns	-----	-----	Abierto/Filtrado
138	netbios-dgm	-----	-----	Abierto/Filtrado
161	snmp	-----	-----	Abierto
162	snmptrap	-----	-----	Abierto/Filtrado
445	microsoft-ds	-----	-----	Abierto/Filtrado
1434	Ms-sql-m	-----	-----	Abierto/Filtrado

Tabla 1.20 Escaneo Sigiloso de puertos en Router Primaria
Ver Anexo 3 Escaneo con NMAP (A3-37, A3-39)

Examinando la información obtenida del escaneo a los routers, podemos observar que se encuentra abierto el puerto 135, lo cual permite la entrada de virus y por lo tanto podría considerarse como una posible vulnerabilidad.

El escaneo UDP no es determinante pues reporta la posibilidad que varios puertos podrían estar abiertos o que existe un filtro de paquetes bloqueando la comunicación, sin embargo es posible determinar que los tres routers tienen configurado soporte snmp.

1.3.2.2.4 I6: Identificación de Aplicaciones

El tester identifica las aplicaciones y servicios que pueden ser accedidos desde el Internet.

Resultados esperados:	Identificación de servicios ofrecidos Identificación de las aplicaciones ofrecidas

Requerimientos:

- Resultado del escaneo previo de puertos

Pasos de Prueba:

- Identificación de servicios disponibles por el servidor

Determinados los puertos abiertos, filtrados y cerrados en los distintos servidores y equipos activos, se identifican los servicios y aplicaciones que están escuchando en los puertos abiertos.

En las Tablas 1.21, 1.22, 1.23, 1.24, 1.25, 1.26, 1.27 y 1.28 aparece la información destacada de cada uno de los objetivos.

Protocolo	Puerto	Servicio	Aplicación
TCP	23	telnet	tcpwrapped
	25	Smtp	Sendmail 8.12.8/8.12.8
	80	http	Squid webproxy 2.5.STABLE1
	110	pop3	ipopd 2002.78rh
	3128	squid-http	Squid webproxy 2.5.STABLE1
	10000	webmin-httpd	Webmin httpd
UDP	1023	Unknown	-----
	3130	squid-ipc	-----
	3457	vat_control	-----
	9199	Unknown	-----
	9876	Sd	-----
	10000	Unknown	-----
	16680	Unknown	-----
	16938	Unknown	-----
	17219	Unknown	-----
	18883	Unknown	-----
	18958	Unknown	-----
	19096	Unknown	-----
	19933	Unknown	-----
	19995	Unknown	-----
	20117	Unknown	-----
	21524	Unknown	-----
	32771	sometimes-rpc6	-----
	34861	Unknown	-----
	40805	Unknown	-----
	44946	Unknown	-----
	49196	Unknown	-----
	57409	Unknown	-----
	58797	unknown	-----

Tabla 1.21 Identificación de Aplicaciones en Proxy Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-1, A3-4)

Protocolo	Puerto	Servicio	Aplicación
TCP	22	ssh	Open SSH 3.51 (protocol 1.99)
	23	telnet	-----
	110	pop3	-----
	111	rpcbind	-----
	3128	http	Squid webproxy 2.5.STABLE1
	6000	X11	-----
	10000	httpd	Webmin
	32768	rpcbind	-----
UDP	1048	unknown	-----
	1485	lansource	-----
	3130	squid-ipc	-----
	4666	edonkey	-----
	5555	rplay	-----
	10000	http	Webmin
	16862	unknown	-----
	17823	unknown	-----
	19140	unknown	-----
	20409	unknown	-----
	20717	unknown	-----
	27444	Trinoo_Bcast	-----
	32768	status	rpc #1000024
	32769	unknown	-----
	33249	unknown	-----
	33459	unknown	-----
	34422	unknown	-----
	36108	unknown	-----
	42172	unknown	-----
	43195	unknown	-----
	44179	unknown	-----
	49167	unknown	-----
	49200	unknown	-----
	49214	unknown	-----
	49262	unknown	-----

Tabla 1.22 Identificación de Aplicaciones en Proxy Primaria
Ver Anexo 3 Escaneo con NMAP (A3-18, A3-21)

Examinando los resultados obtenidos se puede determinar que en los servidores Proxy se encuentran instaladas aplicaciones TCP que no responden a la función de los mismos, tales como: tcpwrapped, sendmail 8.12 y Open SSH 3.51. No fue posible determinar las aplicaciones que corren en los puertos UDP.

Protocolo	Puerto	Servicio	Aplicación
TCP	135	msrpc	-----
	139	netbios-ssn	-----
	445	microsoft-ds	Microsoft Windows 2003
	1025	NFS-or-IIS	-----
	1026	LSA-or-nterm	Microsoft Windows RPC
	2041	interbase	-----
UDP	123	ntp	-----
	137	netbios-ns	-----
	138	netbios-dgm	-----
	445	microsoft-ds	-----
	500	isakmp	-----
	1027	unknown	-----
	4500	nat-t-ike	-----

Tabla 1.23 Identificación de Aplicaciones en
Servidor Bases de Datos 1 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-9, A3-12)

Protocolo	Puerto	Servicio	Aplicación
TCP	135	msrpc	Microsoft Windows RPC
	139	netbios-ssn	-----
	1027	IIS	-----
UDP	135	msrpc	-----
	137	netbios-ns	-----
	138	netbios-dgm	-----

Tabla 1.24 Identificación de Aplicaciones en Servidor Bases de Datos 2 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-14, A3-16)

Protocolo	Puerto	Servicio	Aplicación
TCP	135	Msrpc	Microsoft Windows RPC
	139	netbios-ssn	-----
	445	microsoft-ds	Microsoft Windows XP microsoft-ds
UDP	123	ntp	Microsoft NTP
	137	netbios-ns	Microsoft Windows NT netbios-ssn (workgroup: DOMAIN)
	138	netbios-dgm	-----
	445	microsoft-ds	-----
	500	isakmp	-----
	1900	upnp	-----
	4500	nat-t-ike	-----

Tabla 1.25 Identificación de Aplicaciones en Servidor Bases de Datos Primaria
Ver Anexo 3 Escaneo con NMAP (A3-25, A3-27)

Examinando los resultados obtenidos en los servidores de bases de datos, se puede determinar que todas las aplicaciones TCP y UDP encontradas pertenecen a servicios Windows, algunos de los cuales no responden a la función de estos

equipos. Además el escaneo reveló la probabilidad de que dos servidores de bases de datos estén infectados con Conficker.C o inferior.

Protocolo	Puerto	Servicio	Aplicación
TCP	110	pop3-proxy	AVG pop3 proxy (broken)
UDP	67	Dhcps	-----
	135	Msrpc	-----
	137	netbios-ns	-----
	138	netbios-dgm	-----
	161	Snmp	Cisco SNMP service
	162	Snmptrap	-----
	445	microsoft-ds	-----
	1434	ms-sql-m	-----

Tabla 1.26 Identificación de Aplicaciones en Router 1 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-50, A3-52)

Protocolo	Puerto	Servicio	Aplicación
TCP	80	http	Cisco IOS administrative httpd
	110	pop3-proxy	AVG pop3 proxy (broken)
UDP	67	Dhcps	-----
	135	Msrpc	-----
	137	netbios-ns	-----
	138	netbios-dgm	-----
	161	Snmp	Cisco SNMP service
	162	Snmptrap	-----
	445	microsoft-ds	-----
	1434	ms-sql-m	-----

Tabla 1.27 Identificación de Aplicaciones en Router 2 Secundaria
Ver Anexo 3 Escaneo con NMAP (A3-30, A3-33)

Protocolo	Puerto	Servicio	Aplicación
TCP	110	pop3-proxy	AVG pop3 proxy (broken)
UDP	67	Dhcps	-----
	135	Msrpc	-----
	137	netbios-ns	-----
	138	netbios-dgm	-----
	161	Snmp	Cisco SNMP service
	162	Snmptrap	-----
	445	microsoft-ds	-----
	1434	ms-sql-m	-----

Tabla 1.28 Identificación de Aplicaciones en Router Primaria
Ver Anexo 3 Escaneo con NMAP (A3-37, A3-39)

Como se puede observar en las tablas existen varios puertos en los cuales no ha sido posible determinar el servicio ni la aplicación que corre detrás de estos, sin embargo las aplicaciones que fueron detectadas responden a los servicios propios de un dispositivo router, tal como: Cisco SNMP Service, AVG pop3 proxy y Cisco IOS Administrative.

- Identificar las aplicaciones de Internet disponibles al público

En la Figura 1.24 se puede observar la interfaz de ingreso al servicio de teleacadémico, como se mencionó en el literal 1.3.2.2.2 en lo referente a la revisión del contenido del sitio Web, esta aplicación es proporcionada por un tercero, para ingresar a este servicio es necesario digitar el número de matrícula del estudiante y la cédula del representante, sin embargo el link de Calificaciones de este servicio no está funcionando en forma adecuada como lo muestra la Figura 1.25.

Figura 1.24 Interfaz de ingreso, Servicio Teleacadémico

Fuente: http://www.comil10.edu.ec, Enero 2010

Figura 1.25 Acceso a link Calificaciones, Servicio Teleacadémico

Fuente: http://www.comil10.edu.ec, Enero 2010

1.3.2.2.5 I7: Identificación de Sistemas

El tester intenta obtener información sobre el sistema operativo, el estado de nivel de parchado y el sistema de hardware.

Resultados esperados:	Información sobre el sistema operativo Información sobre el estado del nivel de parchado Información sobre el hardware

Requerimientos:

Conocimientos de información básica de la red.

Pasos de Prueba:

- Ejecutar un escaneo con detección del sistema y análisis de paquete IP

La técnica conocida como “OS Fingerprinting” es la que la mayoría de los analizadores de puertos avanzados utilizan para determinar el sistema operativo del equipo remoto.

A continuación en la Tabla 1.29 aparece los resultados de la aplicación del software Nmap, cuyos resultados completos aparecen en el Anexo 3.

Equipo	Sistema Operativo
Servidor Proxy Secundaria	Linux 2.6.18
Servidor Proxy Primaria	Linux 2.6.18
Servidor Base de Datos Secundaria 1	Windows Server 2003 SP0 - SP2
Servidor Base de Datos Secundaria 2	Windows NT 4.0 SP5 - SP6a
Servidor Base de Datos Primaria	Windows XP SP2 or SP3
Router 1 Secundaria	Cisco IOS 12.X
Router 2 Secundaria	IOS
Router Primaria	Cisco IOS 12.X

Tabla 1.29 Identificación de Sistemas

Fuente: Escaneo con NMAP, 2009

- Analizar la información del banner

La herramienta utilizada para resolver banners fue ScanLine 1.01, un escaner de puertos de línea de comandos, ofrecido como herramienta libre por Foundstone, una división de McAfee, esta herramienta corre en todas las plataformas Windows y además puede realizar pings ICMP, escaneos TCP y UDP, resolver nombres de host, mostrar tiempos de respuesta de host y número de saltos.

La Tabla 1.30 muestra la información obtenida de cada uno de los objetivos, cuyo escaneo completo consta como Anexo 4.

Equipo	Puerto	Banner
Servidor Proxy Secundaria	TCP: 25	[220 localhost.localdomain ESMTP Sendmail 8.12.8/8.12.8; Thu, 3 Jun 2010 12:50:20 -0500 500 5.5.1 Command unrecognized: "" 500 5.5.1 Command unrecognized: ""]
	TCP: 80	[HTTP/1.0 503 Service Unavailable Server: squid/2.5.STABLE1 Mime-Version: 1.0 Date: Thu, 03 Jun 2010 17:50:20 GMT Content-Type: text/html Content-Length: 1031]
	TCP: 110	[+OK POP3 [192.168.101.1] v2001.78rh server ready]
	TCP :3128	[HTTP/1.0 503 Service Unavailable Server: squid/2.5.STABLE1 Mime-Version: 1.0 Date: Thu, 03 Jun 2010 17:50:21 GMT Content-Type: text/html Content-Length: 1031]
	TCP: 10000	[HTTP/1.0 403 Access denied for 192.168.101.230 Server: MiniServ/0.01 Date: Thu, 3 Jun 2010 17:53:29 GMT Content-type: text/html Connection: close <h1>Error -]
Servidor Proxy Primaria	TCP: 22	[SSH-1.99-OpenSSH_3.5p1]
	TCP: 3128	[HTTP/1.0 400 Bad Request Server: squid/2.5.STABLE Mime-Version: 1.0 Date: Sun, 06 Jun 2010 20:21:38 GMT Content Type: text/html Conten-Length:1182 Expires]
	TCP:10000	[HTTP(1.0 200 Document follows]
Router 1 Secundaria	TCP: 80	[HTTP/1.1 401 Unauthorized Date: Thu, 07 Mar 2002 03:19:41 GMT Server: cisco-IOS Accept-Ranges: none WWW-Authenticate: Basic realm=”level_15_access” 401 Unaut]

Tabla 1.30 Identificación del Banner

Fuente: Escaneo con ScanLine, 2009

1.3.2.2.6 I8: Identificación Sigilosa del Router

El tester intenta identificar el router usado por la institución, su funcionalidad dentro de la red, así como el sistema operativo, el fabricante y el modelo.

Resultados esperados:	Direcciones IP de los routers Función de los routers en la red Sistema operativo, fabricante y modelo de router

Requerimientos:

- Información básica de la red e identificación de sistemas

Los números IP asignados a los routers de la sección secundaria son: 201.218.3.93 y 190.95.172.97, su funcionalidad dentro de la sección secundaria es conectar al servicio de Internet respectivamente a los usuarios normales y a los directivos.

El IP asignado al router de la sección primaria es: 201.218.3.89 y su funcionalidad dentro de esta sección es conectar a los usuarios al servicio de Internet.

Además se detectaron dos router internos más cuya funcionalidad es conectar las redes de ambas secciones, las direcciones IP son: 192.168.101.254 y 192.168.110.254. La Figura 1.26 muestra la estructura descrita.

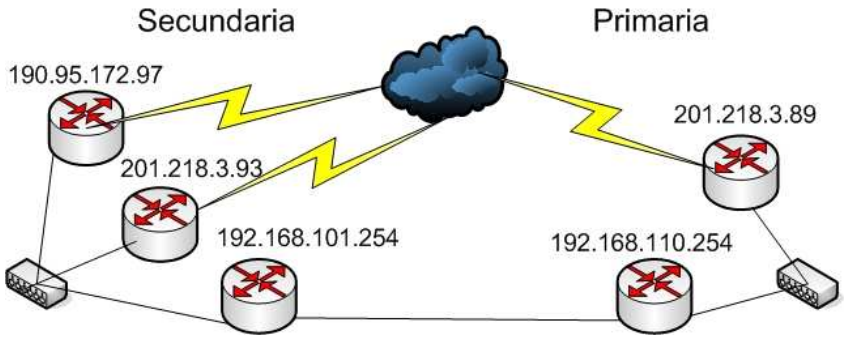


Figura 1.26 Routers de la red de datos de la Unidad Educativa

Pasos de Prueba:

- Seguir cautelosamente las rutas con el comando traceroute.

Para verificar la ruta se realizó un traceroute al servidor Web de la institución y otro a google.com, desde el servidor Proxy de la sección secundaria, los resultados aparecen en la Tabla 1.31.

Servidor Web	google.com
1 - 190.95.172.97	1 - 190.95.172.97
2 - 10.201.21.125	2 – 10.201.21.125
3 - 10.201.21.222	3 - 10.201.21.105
4 - 10.201.11.249	4 - 10.201.11.125
5 - 200.93.238.2	5 - 10.201.11.182
6 - 200.93.238.10	6 – 130.94.195.29
7 - 200.93.192.99	7 – 129.250.2.23
	8 – 129.250.2.23

Tabla 1.31 Análisis de Rutas desde red institución educativa

Fuente: COMIL10 “Abdón Calderón”. Resultado comando tracert, 2009

Analizando los resultados podemos deducir que uno de los routers de la sección secundaria tiene asignada la dirección IP 190.95.172.97, la cual le permite salir al Internet.

Se realiza otros traceroute, pero esta vez desde una máquina externa conectada al Internet, obteniéndose los resultados que se muestran en la Tabla 1.32.

Proxy Secundaria IP: 201.218.3.94	Proxy Secundaria IP: 190.95.172.98	Proxy Primaria IP: 201.218.3.90
1 – 192.168.1.1 2 – 186.42.0.1 3 - 190.152.127.81 4 – 190.152.127.81 5 – 190.11.18.65 6 – 190.11.18.82 7 - 200.1.6.6 8 - 10.201.21.125 9 - 190.95.171.174 10- 190.95.171.174 Destino de red inalcanzable	1 – 192.168.1.1 2 – 186.42.128.1 3 – 190.152.127.37 4 – 190.152.127.37 5 – 190.11.18.65 6 – 190.11.18.82 7 – 200.1.6.6 8 – 10.201.21.215 9 – 201.218.62.6 10- 190.95.172.98	1 – 192.168.1.1 2 – 186.42.0.1 3 – 190.152.127.37 4 – 190.152.127.37 5 – 190.11.18.65 6 – 190.11.18.82 7 – 200.1.6.6 8 – 10.201.21.215 9 – 190.95.171.173 10- 201.218.3.90

Tabla 1.32 Análisis de Rutas desde el exterior

Fuente: Resultado comando tracert , 2009

Como puede observarse en la tabla, la dirección del servidor Proxy de la sección primaria y una de las direcciones del servidor Proxy de la sección secundaria son ruteables en 10 saltos, la otra dirección en el salto 10 nos da el mensaje de “Destino de red inalcanzable”, al tener la certeza que esta dirección es correcta se cree que existe algún tipo control en el servidor que no le permite responder al tracert.

- Analizar las rutas de los paquetes IP

Considerando que el servidor proxy de la secundaria tiene asignadas dos direcciones IP públicas: 201.218.3.94 y 190.95.172.98, podemos identificar que para acceder al equipo podemos hacerlo mediante dos rutas, una a través de ip.colegio-abdon-calderon-michelena-i.uio.telconet.net con IP 190.95.171.174 y otra a través de ip1.colegio-abdon-calderon.recoleta-d.uio.telconet.net con IP 201.218.62.6.

1.3.2.2.7 I10:Identificación Sigilosa del Firewall

No se realiza esta prueba por cuanto la red de datos de la institución educativa no tiene firewall.

1.3.2.2.8 I12: Investigación de Vulnerabilidades

La información obtenida en los pasos anteriores, tal como: puertos abiertos, aplicaciones, sistemas operativos, banners es analizada en busca de vulnerabilidades, utilizando varias herramientas.

Resultados esperados:	Lista de vulnerabilidades potenciales

Requerimientos

- Conocimiento profundo de puertos abiertos, servicios ofrecidos, aplicaciones y sistemas operativos usados.

Pasos de Prueba:

- Usar los escaners de vulnerabilidades más poderosos

Luego de un análisis se han escogido las siguientes herramientas de escaneo de vulnerabilidades:

- NESSUS
- GFILANguard

NESSUS es un programa de escaneo de vulnerabilidades muy reconocido, consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. Nessus comienza escaneando los puertos para buscar puertos abiertos y después intentar varios exploits. Las pruebas de vulnerabilidad disponibles son una larga lista de plugins que son actualizados constantemente.

El escaneo con NESSUS se realizó utilizando la versión libre. Los resultados completos aparecen en el presente proyecto como Anexo 5.

GFILANguard es un galardonado escáner de seguridad de red, escanea la red y puertos para detectar, evaluar y corregir vulnerabilidades de seguridad.

El escaneo con GFILANguard se realizó utilizando la versión libre que permite escanear un máximo de cinco IPs. Los resultados completos del escaneo aparecen en el presente proyecto como Anexo 6.

A continuación se presenta un resumen de la información destacada que incluye, el equipo, el protocolo y puerto, las vulnerabilidades y los correspondientes identificadores CVE (Common Vulnerabilities and Exposures).

Un identificador CVE es un código asignado a una vulnerabilidad que le permite ser identificada de forma univoca, ayuda al usuario a conocer de una forma más objetiva una vulnerabilidad y tiene la forma: CVE-año-numero, donde el número que aparece junto a la vulnerabilidad suele ser un número que se asigna en bloque para un producto y por tanto solo es una referencia.

Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
UDP: Varios	Alto	69 puertos abiertos comúnmente usados por troyanos	-----
TCP: 3128	Medio	El proxy remoto puede ser vulnerable a denegación de servicio.	-----
	Bajo	El servidor remoto Proxy web acepta pedidos.	-----
	Bajo	El proxy HTTP acepta requerimientos Gopher.	CVE-2002-0371
TCP: 10000	Medio	El servidor web fuga una dirección IP privada a través de sus cabeceras HTTP.	CVE-2000-0649
	Bajo	Un servidor Web está corriendo en el host remoto.	-----
TCP: 23	Bajo	El servicio cierra la conexión sin enviar ningún dato.	-----
TCP: 25	Bajo	Un servidor SMTP está corriendo en este puerto.	-----
	Bajo	El servidor SMTP está configurado para permitir email relaying.	-----
TCP: 80	Bajo	El servidor remoto proxy web acepta pedidos.	-----
	Bajo	El proxy HTTP acepta requerimientos Gopher.	CVE-2002-0371
	Bajo	Un servidor web se encuentra corriendo en este puerto.	-----
TCP: 110	Medio	El certificado SSL del servidor ha expirado. El certificado SSL es para un host diferente.	-----
	Bajo	Un servidor POP3 está escuchando en ese puerto	-----
ICMP General	Bajo	El host responde a un requerimiento timestamp ICMP.	-----

Tabla 1.33 Escaneo de Vulnerabilidades en Proxy Secundaria

Ver Anexo 5 Escaneo con NESSUS (A5-1, A5-55)
Ver Anexo 6 Escaneo con CGILANguard (A6-1)

Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP: 22	Medio	El servicio remoto ofrece un protocolo inseguro de criptografía.	CVE-2001-0361
	Bajo	Detecta un servidor SSH escuchando en ese puerto.	-----
UDP: Varios	Alto	69 puertos abiertos comúnmente usados por troyanos	-----
TCP: 3128	Bajo	Un servidor Web está corriendo en este puerto.	-----
	Bajo	El servidor Web acepta requerimientos no autenticados HTTP.	-----
	Bajo	Un Proxy HTTP está corriendo en este puerto	-----
	Bajo	El Proxy HTTP acepta requerimientos gopher.	CVE-2002-0371
	Bajo	Alguna información sobre la configuración HTTP remota pudo ser extraída.	-----
TCP: 10000	Bajo	Un servidor Web está corriendo en este puerto.	-----
	Bajo	Un servicio de administración está corriendo en el Web remoto.	-----
TCP General	Bajo	El host remoto implementa TCP timestamp.	-----
ICMP General	Bajo	Fue posible detectar el seteo exacto del tiempo en el host remoto.	CVE-1999-0524

Tabla 1.34 Escaneo de Vulnerabilidades en Proxy Primaria
Ver Anexo 5 Escaneo con NESSUS (A5-35)
Ver Anexo 6 Escaneo con CGILANguard (A6-33)

Examinando los resultados del escaneo de vulnerabilidades de los servidores Proxy, se puede determinar que existen servicios corriendo que no corresponden a su función, servicios no seguros y 69 puertos UDP abiertos que comúnmente son usados por troyanos.

Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP: 445	Crítico	Código arbitrario puede ser ejecutado en el host remoto debido a un error en la implementación SMB.	CVE-2005-1206
	Crítico	El host remoto está corriendo una versión de Windows que tiene un defecto en la interface RPC	CVE-2003-0715 CVE-2003-0528 CVE-2003-0605
	Crítico	Código arbitrario puede ser ejecutado en el host remoto debido a un error en el servicio LSASS.	CVE-2003-0533
	Crítico	El host remoto tiene una biblioteca ASN.1 que podría permitir ejecutar código arbitrario en este host.	CVE-2003-0818
	Crítico	El host remoto es vulnerable al desbordamiento del buffer en el servicio del servidor.	CVE-2006-3439
	Crítico	El host remoto parece estar infectado por una variante del gusano Conficker.	-----
	Crítico	El host remoto está afectado por una vulnerabilidad de divulgación de información SMB.	CVE-2005-1206
	Crítico	El host remoto es vulnerable a la corrupción de la memoria en SMB.	CVE-2008-4834 CVE-2008-4835 CVE-2008-4114
	Alto	El host remoto es vulnerable al desbordamiento de pila en el servicio del servidor.	CVE-2006-1314 CVE-2006-1315
	Bajo	Es posible iniciar una sesión en el host remoto como invitado, dando credenciales o con una sesión nula.	CVE-1999-0504 CVE-1999-0505 CVE-1999-0506 CVE-2000-0222 CVE-2002-1117 CVE-2005-3595

TCP: 445	Bajo	Es posible enumerar los recursos compartidos de la red remota.	-----
	Bajo	Es posible obtener información de la red.	-----
	Bajo	Un servicio DCE/RPC está corriendo en el host remoto.	-----
	Bajo	Es posible obtener información sobre el sistema operativo remoto.	-----
	Bajo	Un servicio de archivo o impresora compartida está escuchando en el host.	-----
	Bajo	Es posible logearse en el host remoto Windows con una sesión NULL.	CVE-1999-0519 CVE-1999-0520 CVE-2002-1117
UDP: Varios	Alto	69 puertos abiertos comúnmente usados por troyanos	-----
TCP: 135	Bajo	Es posible enumerar los servicios DCE corriendo en el puerto remoto.	-----
UDP: 137	Bajo	Es posible obtener el nombre de red del host remoto.	-----
TCP: 139	Bajo	Un servicio de archivo o impresora compartida está escuchando en el host.	-----
TCP:1025	Bajo	U n servicio DCE/RPC está corriendo en el host remoto.	-----
TCP: 1026	Bajo	Un servicio DCE/RPC está corriendo en el host remoto.	-----

Tabla 1.35 Escaneo de Vulnerabilidades en Servidor Bases de Datos 1 Secundaria
Ver Anexo 5 Escaneo con NESSUS (A5-23)
Ver Anexo 6 Escaneo con CGILANguard (A6-10)

Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP: 139	Crítico	El host remoto es vulnerable al desbordamiento de la pila en el servicio del servidor.	CVE-2006-1314 CVE-2006-1315
	Crítico	El host remoto es vulnerable al desbordamiento del buffer en el servicio del servidor	CVE-2008-4250
	Crítico	El host remoto es vulnerable a la corrupción de la memoria en SMB	CVE-2008-4834 CVE-2008-4835 CVE-2008-4114
TCP: General	Alto	El sistema operativo remoto ya no está respaldado por su proveedor.	-----
	Bajo	Al menos una cuenta de usuario ha sido deshabilitada.	-----
	Bajo	Al menos un usuario nunca ha cambiado su password.	-----
	Bajo	Al menos un usuario nunca se ha logeado con su cuenta.	-----
	Bajo	Al menos un usuario tiene una password que no expira.	-----
	Bajo	Hay al menos un usuario en el grupo Administrators.	-----
	Bajo	Hay al menos un usuario en el grupo Domain Administrators.	-----
	Bajo	Al menos una cuenta de usuario local ha sido deshabilitada.	-----
	Bajo	Al menos un usuario local nunca se ha logeado en su cuenta.	-----
	Bajo	Al menos un usuario local tiene un password que nunca expira.	-----
UDP: Varios	Alto	69 puertos abiertos comúnmente usados por troyanos	-----
TCP: 135	Bajo	Un servicio DCE/RPC está corriendo en	-----

		el servidor remoto.	
TCP: 137	Bajo	Es posible obtener el nombre de la red desde el host remoto usando NetBios o SMB.	-----
TCP: 139	Bajo	Es posible logearse en el host remoto.	CVE-1999-0504 CVE-1999-0505 CVE-1999-0506 CVE-2000-0222 CVE-2005-3595
	Bajo	Es posible enumerar los recursos compartidos.	-----
	Bajo	Es posible obtener información de la red.	-----
	Bajo	Es posible obtener el dominio SID.	CVE-2000-1200
	Bajo	Es posible enumerar los usuarios del dominio.	CVE-2000-1200
	Bajo	Es posible obtener información sobre el sistema operativo remoto.	-----
	Bajo	Es posible enumerar los usuarios locales.	CVE-2000-1200
	Bajo	Un servicio de archivo o impresora compartido está escuchando en el host remoto.	-----
	Bajo	Es posible obtener la política de password del host remoto.	-----
	Bajo	Es posible logearse en el host remoto con una sesión nula.	CVE-1999-0519 CVE-1999-0520 CVE-2002-1117
TCP: 1027	Bajo	Un servicio DCE/RPC está corriendo en el servidor remoto.	-----

Tabla 1.36 Escaneo de Vulnerabilidades en Servidor Bases de Datos 2 Secundaria
Ver Anexo 5 Escaneo con NESSUS (A5-2)
Ver Anexo 6 Escaneo con CGILANguard (A6-19)

Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP: 445	Crítico	Código arbitrario puede ser ejecutado en el host remoto debido a un error en la implementación SMB.	CVE-2005-1206
	Crítico	El host remoto es vulnerable al desbordamiento del buffer en el servicio del servidor.	CVE-2006-3439
	Crítico	El host remoto es vulnerable a la corrupción de la memoria en SMB.	CVE-2008-4834 CVE-2008-4835 CVE-2008-4114
	Crítico	El host remoto parece estar infectado por una variante del gusano Conficker.	-----
	Alto	El host remoto es vulnerable al desbordamiento de pila en el servicio del servidor.	CVE-2006-1314 CVE-2006-1315
	Alto	Es posible acceder a los recursos compartidos de la red	CVE-1999-0519 CVE-1999-0520
	Medio	Es posible logearse en el host remoto como usuario invitado.	CVE-1999-0505
	Bajo	Es posible iniciar una sesión en el host remoto como invitado, dando credenciales o con una sesión nula.	CVE-1999-0504 CVE-1999-0505 CVE-1999-0506 CVE-2000-0222 CVE-2002-1117 CVE-2005-3595
	Bajo	Es posible enumerar los recursos compartidos de la red remota.	
	Bajo	Es posible obtener información de la red.	
		Es posible obtener información sobre el sistema operativo remoto.	
	Bajo	Es posible obtener el dominio SID.	CVE-2000-1200
	Bajo	Es posible enumerar los usuarios locales.	CVE-2000-1200

TCP: 445	Bajo	Un servicio de archivo o impresora compartida está escuchando en el host.	-----
	Bajo	Es posible logearse en el host remoto Windows con una sesión NULL.	CVE-1999-0519 CVE-1999-0520 CVE-2002-1117
UDP: Varios	Alto	69 puertos abiertos comúnmente usados por troyanos	-----
UDP: 123	Bajo	Un servidor NTP está corriendo en este puerto.	-----
UDP: 137	Bajo	Es posible obtener el nombre de red del host remoto.	-----
TCP: 139	Bajo	Un servicio de archivo o impresora compartida está escuchando en el host.	-----
TCP General	Bajo	Se pudo identificar el sistema operativo corriendo en el host remoto.	-----
	Bajo	El servicio remoto implementa TCP timestamp.	-----
ICMP General	Bajo	El servicio remoto implementa TCP timestamp.	CVE-1999-0524

Tabla 1.37 Escaneo de Vulnerabilidades en Servidor Bases de Datos Primaria
Ver Anexo 5 Escaneo con NESSUS (A5-36)
Ver Anexo 6 Escaneo con CGILANguard (A6-41)

Examinando los resultados del escaneo de vulnerabilidades en los servidores de bases de datos, se puede determinar que las vulnerabilidades detalladas son ocasionadas en su mayoría por: la falta de parches, la inexistente política de contraseñas, la operación con software en forma ilegal, la utilización de sistemas operativos que ya no tienen soporte del fabricante, la existencia de servicios que no responden a la función de los equipos, lo que los hace susceptibles a todo tipo de ataques que hagan uso de esas vulnerabilidades y constituye un riesgo muy alto de seguridad.

Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP General	Bajo	Es posible resolver el nombre del host remoto	-----

Tabla 1.38 Escaneo de Vulnerabilidades Router Primaria y Router 1 Secundaria
Ver Anexo 5 Escaneo con NESSUS (A5-61, A5-69)
Ver Anexo 6 Escaneo con CGILANguard (A6-52, A6-55)

Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP General	Bajo	Es posible identificar el Sistema Operativo	-----
	Bajo	Es posible resolver el nombre del host remoto	-----
TCP 80	Bajo	Un servidor web está corriendo es este puerto	-----

Tabla 1.39 Escaneo de Vulnerabilidades Router 2 Secundaria
Ver Anexo 5 Escaneo con NESSUS (A5-52)
Ver Anexo 6 Escaneo con CGILANguard (A6-50)

Examinando los resultados del escaneo de vulnerabilidades de los routers, se puede determinar que las vulnerabilidades encontradas no representan mayor riesgo de seguridad.

- Consultar bases de datos de vulnerabilidades

Las bases de datos consultadas mantienen información más detallada de las vulnerabilidades, su nivel de riesgo, las posibles soluciones que podrían ser implementadas para superarlas y varios links con información adicional.

Entre los recursos utilizados para la consulta de vulnerabilidades, tenemos:

http://www.securityspace.com/smysecure/search.html
http://www.securityfocus.com/vulnerabilities

http://nvd.nist.gov/
http://secunia.com/
http://www.nessus.org/plugins/index.php?view=search

1.3.2.2.9 I13: Identificación de las Interfaces de Aplicación

El objetivo de este módulo es identificar las interfaces que pueden ser accedidas desde el Internet, en particular las que han sido desarrolladas por el Centro de Informática para buscar vulnerabilidades potenciales.

Resultados esperados:	Lista de vulnerabilidades potenciales en las interfaces de aplicación

Requerimientos

- Información de las aplicaciones y sistemas usados.

Pasos de Prueba:

- Escanear los servicios ofrecidos en la página Web de la Unidad Educativa, en búsqueda de vulnerabilidades potenciales.

La herramienta utilizada para escanear los servicios ofrecidos en la Web fue ParosProxy 3.2.13, un software gratuito, escrito en Java que permite evaluar la seguridad de aplicaciones Web.

A través del ParosProxy, todos los HTTP y HTTPS de datos entre el servidor y el cliente, incluyendo las cookies y campos de formulario, pueden ser interceptados y modificados.

La página Web de la Institución no contiene alertas importantes, sin embargo la referencia externa que ofrece el servicio de Teleacadémico contiene una advertencia de seguridad, detallada en la Tabla 1.40. Las pruebas fueron realizadas con ParosProxy 3.2.13 y constan en el Anexo 7.

Riesgo	Vulnerabilidad
Medio	El atributo AUTOCOMPLETE no está deshabilitado en el formulario de entrada html y contiene un tipo de dato password. Los passwords podrían ser almacenados en el browser y recuperados.

Tabla 1.40 Escaneo de Vulnerabilidades – Interfaz Web

Fuente: Escaneo con ParosProxy, Enero 2010

1.3.2.3 Fase 3: Análisis de información y riesgos

1.3.2.3.1 Definición de Prioridades

La prioridad para ejecutar la fase 4 es garantizar la seguridad y disponibilidad del servicio de Internet y acceso a las aplicaciones, con respecto a los usuarios internos, así como la disponibilidad 24/7 del servicio de información que brinda a través del Internet para los usuarios externos a la institución, sin embargo tomando en cuenta la naturaleza de estas pruebas, los servicios y aplicaciones podrían llegar a comprometerse, lo que repercutiría en la credibilidad y confianza.

1.3.2.3.2 Riesgos Asociados

Entre los riesgos asociados con la ejecución de los módulos tenemos:

- Denegación de servicio (DoS) en los servidores Proxy, causando que el servicio de Internet no esté disponible.
- Desbordamiento de pila o buffer en los servidores de Bases de Datos, causando que los usuarios de la red no tengan disponible el servicio que proporcionan estos equipos.
- Denegación de servicio y desbordamiento del buffer de los routers, causando que la Unidad Educativa no tenga acceso al Internet.
- Denegación de servicio en el servidor Web, causando que la información sobre eventos a realizarse, horarios, inscripciones y el servicio de teleacadémico no esté disponible.

1.3.2.3.3 Limitación de Sistemas y Módulos

Tomando en cuenta las prioridades y riesgos asociados ya mencionados, se decide realizar únicamente un test “Pasivo”, donde los módulos de la fase 4 no serán ejecutados.

1.3.2.4 FASE 5: ANÁLISIS FINAL

En esta sección se describirán las amenazas y vulnerabilidades detectadas en la Unidad Educativa.

1.3.2.4.1 Determinación de Amenazas

- Amenazas Físicas
  - Acceso no controlado a las instalaciones de la Unidad Educativa.
  - Acceso no autorizado a áreas sensibles y datos.
  - Robo de información a través de dispositivos de almacenamiento portátiles.
  - Fallas en el cableado estructurado. Ver Anexo 2 Fotográfico de las instalaciones de red de la Unidad Educativa (A2-1).
  - Robo, mal uso de equipos informáticos.
  - Factores ambientales.
  - Cortes de luz, variaciones de voltaje.

- Amenazas lógicas
  - Programas maliciosos, virus, gusanos, troyanos y similares.
  - Botnets y zombies.
  - Redes sociales y video online.
  - Desbordamiento de buffer.
  - Denegación de Servicio (DoS).

1.3.2.4.2 Determinación de Vulnerabilidades

Las vulnerabilidades se establecen en base a las condiciones que favorecen la ocurrencia de una amenaza. Las vulnerabilidades detectadas en la red de datos son:

- Vulnerabilidades Físicas
  - Cuarto de servidores con humedad y sin ventilación. Ver literal i) del Anexo 2 Fotográfico de las instalaciones de red de la Unidad Educativa (A2-12).
  - Cableado estructurado con falencias y no certificado. Ver Anexo 2 Fotográfico de las instalaciones de red de la Unidad Educativa (A2-1).
  - Seguridades incipientes en puertas de acceso a áreas sensibles. Ver literales a) y b) del Anexo 2 Fotográfico de las instalaciones de red de la Unidad Educativa (A2-9).
  - Inexistente almacenamiento de respaldo.
  - Inexistencia de políticas y procedimientos de seguridad.
  - Falta de personal propio que realice las funciones de control de ingreso a las instalaciones de la Institución.
  - Inexistencia de sistema detector de incendios.

- Vulnerabilidades Lógicas
  - Se utiliza software en forma ilegal.
  - No está implementada una zona desmilitarizada.
  - No existe software para el filtrado de páginas Web y asignación de perfiles de usuario.
  - No existe un sistema de detección de intrusos.
  - Los servicios se encuentran mal configurados.
  - El software está desactualizado.
  - Inexistencia de software antivirus.
  - Falla en la asignación de responsabilidades claras al personal del Centro de Informática.

- Utilización de sistemas operativos y hardware no apropiados para servidores.
- Inexistencia de planes de contingencia en general.
- Inexistente control sobre los servicios informáticos que prestan terceros.
- Inexistencia de cultura en seguridad informática.
- Inexistencia de políticas y procedimientos de seguridad.

1.4 DEFINICIÓN DE REQUERIMIENTOS DE SEGURIDAD

Para definir los requerimientos de seguridad se tomó en cuenta la información obtenida del análisis previo de la red de la Institución, la determinación de vulnerabilidades y amenazas y la información proporcionada por los usuarios de la red y por los miembros del Centro de Informática.

Los requerimientos de seguridad identificados se detallan a continuación:

1.4.1 REQUERIMIENTOS FÍSICOS

1.4.1.1 Control de Acceso Físico y de Seguridad

- Adecuar el área destinada a los servidores y comunicaciones, con el objetivo de brindar la seguridad apropiada a los equipos activos de red tales como: servidores, switches, routers, UPS, etc.

- Controlar el acceso físico a las áreas críticas, especialmente al Centro de Informática y cuarto de servidores y comunicaciones, mediante la implementación de controles de acceso como tarjetas magnéticas o claves que permitan el acceso solo al personal autorizado.

1.4.1.2 Estructura del Cableado

- Corregir las falencias del cableado, aplicando estándares de referencia como el EIA/TIA-568A, EIA/TIA-569, EIA/TIA-606, EIA/TIA-607, que permitan administrar el cableado dependiendo de los requerimientos y de la evolución tecnológica en la institución y certificarlo, de esta manera se contará con un medio de transmisión óptimo.

- Disponer de la documentación de señalización e identificación de puntos de red en la estructura de la institución.

1.4.1.3 Sistema Emergente de Energía

- Actualizar el equipo UPS con la finalidad de hacer el funcionamiento de los servidores inmune a la intransigencia de apagones espontáneos y protegerlos contra perturbaciones repentinas de la red eléctrica.

- Incorporar una planta de energía eléctrica auxiliar para las instalaciones administrativas, cuarto de telecomunicaciones y Centro de Informática.

1.4.1.4 Planes de Contingencia

1.4.1.4.1 Desastres naturales

- Elaborar, probar y actualizar periódicamente el plan de contingencia para el Centro de Informática, donde se incluyan: aplicaciones críticas, sistemas de cómputo y de comunicaciones, con el objetivo de minimizar los daños frente a desastres naturales.

- Elaborar y socializar planes de contingencia que respondan a las actividades críticas que realiza cada uno de los departamentos de la institución.

1.4.1.4.2 Desastres del Entorno

- Instalar detectores de humo, para prevenir incendios que puedan comprometer los equipos, la información y sobre todo la vida de los empleados de la institución.

- Regular las condiciones ambientales de temperatura y humedad dentro del cuarto de servidores y telecomunicaciones utilizando ventiladores o un equipo de aire acondicionado.

- Planificar y cumplir con el plan de mantenimiento preventivo de equipos informáticos.

1.4.2 REQUERIMIENTOS LÓGICOS

1.4.2.1 Control de Acceso Lógico y de Seguridad

- Implementar controles de acceso para el sistema operativo, las bases de datos, software institucional y recursos compartidos, para evitar que puedan ser utilizados, modificados o eliminados sin autorización.

- Monitorear a intervalos regulares el acceso a los sistemas operativos, los servidores y las aplicaciones dentro y fuera de la red de datos.

1.4.2.1.1 Identificación y Autenticación

- Definir perfiles de acceso a los diferentes recursos de la red dependiendo de la función que cumple cada usuario dentro de la institución.

1.4.2.1.2 Control de Acceso Interno

- Utilizar contraseñas fuertes para proteger los datos, aplicaciones y equipos.

- Mantener actualizada la lista de registro de usuarios (grupos de usuarios, equipos y servicios) a quienes se les ha proporcionado acceso para utilizar los recursos del sistema.

1.4.2.1.3 Control de Acceso Externo

- Instalar, configurar y monitorear el firewall para evitar accesos no autorizados a la red interna.

- Monitorear el router de salida al Internet, para evitar posibles ataques tales como: DoS, desbordamiento de buffer, reinicio del dispositivo, etc.

1.4.2.2 Protección de Datos

- Crear y probar un sistema de respaldos que permita recuperar la información en caso necesario.

1.4.2.3 Seguridad en los Servicios

1.4.2.3.1 Active Directory

- Instalar el servicio de Active Directory para organizar, controlar y administrar centralizadamente el acceso a los recursos de la red.

1.4.2.3.2 Acceso al Internet

- Instalar y configurar hardware o software para realizar un filtrado Web que impida el acceso a páginas prohibidas.

- Establecer perfiles, horarios, políticas y procedimientos para el uso del servicio de Internet.

1.4.2.3.3 Correo Electrónico

- Instalar y configurar software o equipo para filtrado de correo basura para evitar la saturación del servidor de correo.

1.4.2.3.4 Antivirus

- Instalar y configurar un software antivirus permanentemente actualizado.

1.4.3 REQUERIMIENTOS DE RED Y COMUNICACIÓN

- Implementar los servidores necesarios para brindar los servicios de red requeridos.

- Desarrollar un diseño de un esquema de seguridad para la red de la institución que minimice el riesgo de un ataque y que incluya entre otras cosas:
  - ✓ Implementación de una zona desmilitarizada o DMZ.
  - ✓ Instalación y configuración de un sistema de detección de intrusos.
  - ✓ Verificación permanente de la no existencia de programas tipo sniffer instalados en equipos no autorizados.
  - ✓ Instalación y configuración de un firewall para el control de la seguridad.

1.4.4 REQUERIMIENTOS DE GESTIÓN

- Capacitar a los usuarios en aspectos de cultura y seguridad informática

- Desarrollar políticas y normas de seguridad que permitan direccionar el manejo interno y externo de la institución y que incluyan, entre otras:
  - ✓ Políticas para uso de software.
  - ✓ Políticas para contratación de servicios informáticos.
  - ✓ Políticas y procedimientos para el acceso y manejo de información.
  - ✓ Políticas para el respaldo de la información

- ✓ Políticas de gestión de usuarios en la red
- ✓ Políticas para el acceso físico a las distintas áreas de la institución.

1.4.5 REQUERIMIENTOS DE LICENCIAS

- Legalizar el uso de software propietario en base a un estudio técnico de las necesidades reales, establecidas conjuntamente por el Centro de Informática y el responsable de cada área o departamento.

CAPÍTULO 2

DISEÑO DEL ESQUEMA DE SEGURIDAD

2.1 DISEÑO DE LA SEGURIDAD FÍSICA

ISO/IEC 27002 es un estándar de seguridad de la información que proporciona recomendaciones de las mejores prácticas para la gestión de seguridad de la información.

Para el diseño de la seguridad física se siguieron los lineamientos de la norma ISO/IEC 27002 referentes a la seguridad física y del entorno.

Los objetivos que se plantearon para el diseño de la seguridad física son:

- Proteger los activos de la Unidad Educativa de los riesgos de actos accidentales, malintencionados y/o desastres naturales.
- Minimizar la pérdida de información y garantizar la recuperación de la misma oportunamente.
- Asegurar que las condiciones ambientales sean las más favorables para el buen funcionamiento de los equipos.

2.1.1 ÁREAS SEGURAS

Objetivo: Evitar el acceso físico no autorizado, daños o intromisiones en las instalaciones y a la información de los sistemas en todos las áreas de la Unidad Educativa, especialmente donde se maneja datos sensibles.

2.1.1.1 Perímetro de seguridad física

El acceso a la Unidad Educativa deberá ser controlado en primer lugar por el personal militar de prevención en la sección secundaria y por los conserjes en la

sección primaria, en segundo lugar por la secretaria de cada área en horas laborables; se prohíbe el acceso a la Unidad Educativa en jornadas no laborables.

El área que ocupa el Centro de Informática deberá permanecer cerrada, en el caso que ningún miembro se encuentre en la misma.

El área de los servidores debe ser cerrada desde el piso al techo, debe contar con instalaciones eléctricas y ventilación apropiadas, solo se permitirá el acceso a las personas autorizadas del Centro de Informática, tales como: administradores de red, bases de datos o aplicaciones.

Se deberá crear normas y procedimientos de seguridad para el acceso y uso de los laboratorios de Informática y de los equipos informáticos de la biblioteca.

Todas las puertas externas del Centro de Informática, área de servidores, laboratorios de Informática y biblioteca deben estar adecuadamente protegidas contra accesos no autorizados mediante mecanismos de control, barras, alarmas, mecanismos de cierre, etc.

Se deberá designar a una persona responsable del monitoreo continuo de las cámaras de seguridad existentes en la Unidad Educativa.

2.1.1.2 Controles físicos de entrada

El área de información debe estar ubicada al ingreso del edificio comando en la sección secundaria y al ingreso de la entrada principal en la sección primaria, de tal manera que todos los visitantes que requieran información para realizar algún trámite la obtengan allí y no deban recorrer toda la institución en busca de ayuda.

Todo visitante que ingrese a la institución deberá registrar su información en un documento que será manejado por el personal de prevención en la sección secundaria y por el personal de conserjes en la sección primaria, donde deberá registrar su nombre, hora de ingreso, área a la que se dirige, además deberá

entregar su documento de identidad.

Todas las personas que se encuentren en la institución, deberán llevar visible su tarjeta de identificación que los acredite como funcionarios de la institución o visitantes.

Los visitantes a áreas seguras deberán ser supervisados e instruidos y su fecha y hora de entrada y salida registrada. Se deberá otorgar solo permisos de accesos para propósitos específicos y autorizados y deberán ser provistos con instrucciones sobre los requerimientos de seguridad del área y sobre los procedimientos de emergencia.

Deben implementarse sistemas de detección de intrusos adecuados para cubrir todas las puertas externas y ventanas accesibles, instalados por profesionales y probados regularmente.

2.1.1.3 Seguridad de oficinas, despachos y recursos

Cada piso en el edificio comando deberá contar con un acceso principal con cerradura, el conserje cerrará cada acceso principal con llave luego que haya verificado que todo el personal se haya retirado, además deberá supervisar que las ventanas se encuentren cerradas.

Los conserjes de la sección primaria serán los encargados de supervisar que las áreas estén aseguradas y que todas las ventanas se encuentren cerradas una vez se hayan concluido las actividades diarias.

Todas las áreas deberán permanecer cerradas con llave, cuando el personal se movilice a otro lugar para cumplir con su trabajo, participar en ceremonias, reuniones de trabajo o actividades de esparcimiento.

Todas las áreas deben tener un extintor de incendios para que pueda reaccionar ante cualquier novedad de este tipo.

Las áreas donde se procesan datos, tales como: registro de notas y la Secretaría General, no deben ser accesibles al público todo el tiempo, se deberá fijar horas de atención.

2.1.1.4 Aislamiento de las zonas de carga y descarga

La bodega de la Unidad Educativa, donde se encuentra todos los suministros de oficina, debe contar con un listado de personas o proveedores autorizados para el acceso a la misma, además debe contar con un acceso exterior a la institución, para que en la entrega de los suministros, el personal externo no acceda a otros departamentos.

2.1.2. SEGURIDAD DE LOS EQUIPOS

Objetivo: Proteger físicamente a los equipos, para reducir la pérdida, daño, robo o puesta en peligro de los activos, que ocasionen la interrupción de las actividades normales de la Unidad Educativa.

2.1.2.1 Ubicación y protección de los equipos

En cada área, los equipos deberán ser ubicados en lugares adecuados, donde no puedan ser afectados por amenazas físicas y ambientales tales como: lluvia, polvo o robo.

Se deberá realizar un monitoreo de las condiciones ambientales en los departamentos, especialmente en los de procesamiento de datos para prevenir cualquier problema en los equipos.

La Unidad Educativa tendrá en cuenta como una de sus políticas de seguridad, la prohibición de comer, beber o fumar cerca de las instalaciones de los equipos, especialmente en el área de procesamiento de datos.

Las instalaciones de procesamiento y almacenamiento de la información que manejan datos sensitivos deberán estar ubicadas estratégicamente, para reducir el riesgo de descuidos durante su uso.

Mantener un inventario y descripción de los recursos de hardware y de redes instalados, que incluyan entre otros datos: número de serie, fecha de adquisición, proveedor, periodo de garantía, situación actual del equipo.

Establecer responsables de los equipos en cada área, así como establecer quienes son los usuarios de los mismos.

Evitar la posibilidad de arranque desde diskettes en equipos considerados críticos, así como implementar seguridad para verificar si se accesó al hardware del equipo.

2.1.2.2 Suministro eléctrico

El área de los servidores y equipos de comunicación debe contar con equipos contra fallos en el suministro de energía u otras anomalías eléctricas, UPS, extintor de incendios, detector de humo, conexión a tierra y deberá estar ubicada en un área restringida y sin humedad.

Todas las instalaciones de la Unidad Educativa, contarán con una puesta a tierra para proteger a los equipos de los rayos.

Las cajas donde se encuentran los interruptores de energía deberán ser colocadas en lugares fuera del alcance de personas externas, y bajo llave, para evitar interrupción de energía a las instalaciones de la Unidad Educativa.

Los UPS deberán ser revisados periódicamente, para asegurar que tienen la capacidad adecuada y probada de acuerdo a las especificaciones del fabricante.

Deberá ser considerada la provisión de un generador de energía, si el

procesamiento debe continuar en caso de una prolongada falla de la energía.

2.1.2.3 Seguridad del cableado

El cableado de la red debe garantizar la correcta transmisión de datos, para lo cual necesita estar protegido por canaletas y ubicado en lugares que no interrumpan el paso normal de las personas, para evitar daños al cable y por consiguiente la interrupción de los servicios de red.

Los cables de energía eléctrica deberán estar separados de los cables de comunicaciones para prevenir interferencias, de acuerdo a las recomendaciones del fabricante y de los estándares en vigencia.

Cumplir las normas que rigen el sistema de cableado estructurado.

2.1.2.4 Mantenimiento de equipos

El Centro de Informática, debe contar con un plan de mantenimiento preventivo de los equipos, que será realizado según el cronograma establecido por áreas. El mantenimiento correctivo será realizado inmediatamente sean reportadas las fallas.

El Centro de Informática deberá llevar un registro de los daños más frecuentes en los equipos.

El Centro de Informática deberá contar con un sistema de backups distribuido para asegurar la información sensible de los usuarios.

2.1.2.5 Seguridad de los equipos fuera de la organización

La Unidad Educativa debe contar con una cobertura de seguros para todos los equipos portátiles dentro y fuera de la institución.

En caso de que un equipo portátil salga de la institución a un lugar público, no debe ser dejado sin vigilancia, debe ser transportado en valijas de mano y camufladas como sea posible cuando se viaja y deben seguirse permanentemente las instrucciones del fabricante para la protección del mismo.

2.1.2.6 Seguridad en la reutilización o eliminación de equipos

Los equipos que vayan a ser reutilizados para otra área o usuario deberán ser formateados y configurados de acuerdo a las necesidades del nuevo usuario, no sin antes haber sacado los respaldos respectivos y ser entregados a su antiguo dueño.

2.1.2.7 Traslado de activos

Ningún equipo informático, información o software podrá salir de la institución sin una autorización escrita del Señor Rector y bajo conocimiento y aprobación del Jefe del Centro de Informática y del responsable de activos fijos.

2.2 DISEÑO DE LA SEGURIDAD LÓGICA

Los objetivos de la seguridad lógica son:[9]

- Definir y controlar los permisos y accesos a los programas y archivos.
- Asegurar que los datos sean utilizados por el proceso adecuado y con los procedimientos correctos.
- Asegurar que los datos y programas que no correspondan a un departamento sean modificados por los usuarios de dicho departamento.
- Asegurar que la información transmitida sea recibida por el destinatario al cual fue enviada.
- Asegurar que la información recibida sea la misma que fue transmitida.

[9] CHAUCA Chimbo Cristina Alexandra; VILLALBA Lindado Samira Paola, “Diseño de un esquema de seguridad para la intranet del CONESUP”, 2007

2.2.1 DISEÑO DE LA RED

Para el diseño de la seguridad de la red se consideró la arquitectura de seguridad SAFE de CISCO para empresas medianas.

"SAFE es una arquitectura de seguridad. Debe evitar que la mayor parte de los ataques afecten a los recursos más valiosos de la red. Los ataques que consiguen pasar la primera línea de defensa o que parten desde dentro de la red deben detectarse con precisión y contenerse rápidamente para minimizar su efecto. Sin embargo además de ser segura, la red debe seguir ofreciendo todos los servicios que los usuarios esperan de ella. Es posible ofrecer al mismo tiempo una buena seguridad y funcionalidad de red. La arquitectura SAFE no es una forma revolucionaria de diseñar redes, sino meramente un modelo para asegurarlas.

Aunque las redes en la mayoría de las empresas evolucionan con los crecientes requisitos de tecnología de información de la empresa, la arquitectura SAFE utiliza un enfoque modular. El enfoque modular tiene dos ventajas principales. En primer lugar, permite a la arquitectura afrontar la relación de seguridad entre los distintos bloques funcionales de la red, y en segundo lugar permite a los diseñadores evaluar e implementar la seguridad módulo a módulo, en lugar de intentar completar la arquitectura en una sola fase"[10].

La Figura 2.2 muestra el modelo detallado, en el que se puede apreciar tres módulos: Módulo de Campo, Módulo de Internet y Módulo WAN.

[10] Extending the Security Blueprint to Small, Midsize, and Remote-User Networks. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf, 2001

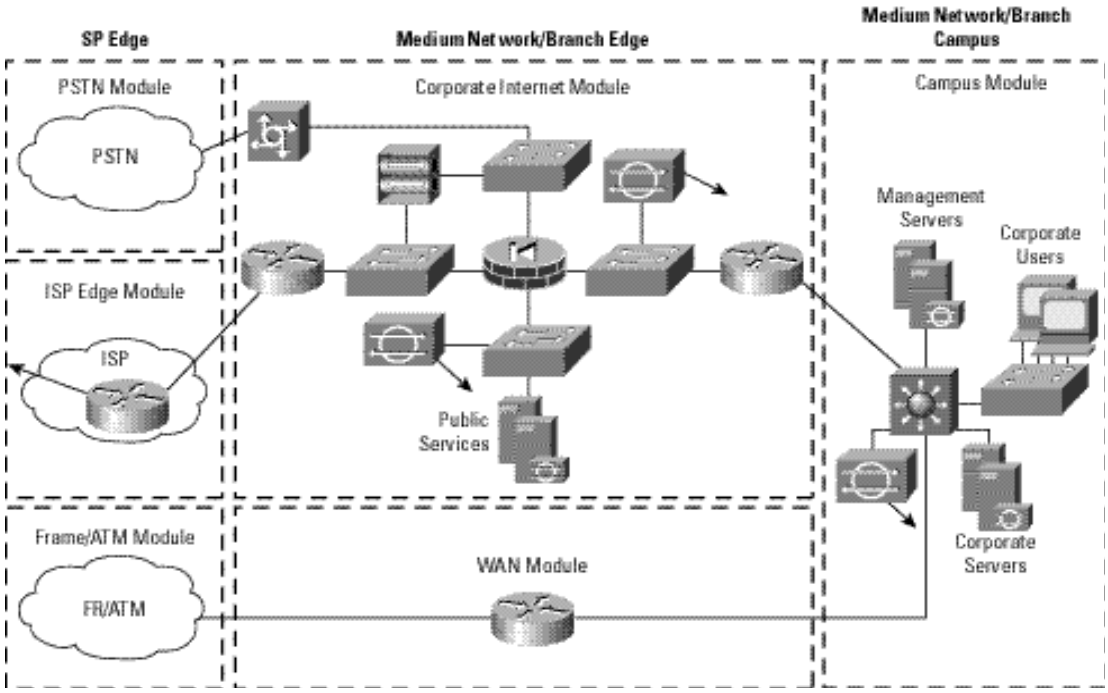


Figura 2.1 Modelo Detallado SAFE para empresas medianas

Fuente: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf, 2001

2.2.1.1 Módulo de Internet[11]

Este módulo proporciona a los usuarios internos conectividad a los servicios de Internet y el acceso a los usuarios a los servicios públicos de la DMZ. Además termina el tráfico VPN desde usuarios y sitios remotos, así como el tráfico de los tradicionales dial-in. No está diseñado para servir aplicaciones de comercio electrónico.

Dentro de los componentes principales están:

- Servidor dial-in
- Servidor DNS
- Servidor FTP/HTTP
- Firewall
- Switches capa 2

[11] Extending the Security Blueprint to Small, Midsize, and Remote-User Networks. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf, 2001

- Aparato NIDS
- Servidor SMTP
- Concentrador VPN
- Router de borde

Dentro de las amenazas que combaten están:

- Acceso no autorizado
- Ataques a la capa de aplicación
- Ataques de virus y caballos de Troya
- Ataques de contraseñas
- Denegación de servicio
- IP spoofing
- Sniffers
- Exploración de la red
- Abuso de confianza
- Redirección de puertos

2.2.1.2 Módulo de Campo[12]

Este módulo contiene estaciones de trabajo de usuarios finales, servidores de la intranet corporativos, los servidores de administración y la infraestructura asociada de capa 2 y capa 3 requerida para soportar los dispositivos.

Dentro de los dispositivos principales están:

- Switch capa 3
- Switches capa 2
- Servidores corporativos
- Usuarios de estaciones de trabajo
- Host de gestión SNMP
- Host NIDS
- Host syslog

[12] Extending the Security Blueprint to Small, Midsize, and Remote-User Networks. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf, 2001

- Servidor de control de acceso
- Servidor One-Time Password
- Sistema de Administración de host
- Aparato NIDS

Dentro de las amenazas que combate están:

- Sniffers
- Aplicaciones virus y caballo de Troya
- Acceso no autorizado
- Ataques de contraseña
- Ataques a la capa de aplicación
- IP spoofing
- Abuso de confianza
- Redirección de puertos

2.2.1.3 Módulo WAN[13]

El módulo WAN es incluido solo cuando las conexiones a lugares remotos en una red privada son requeridas. Este requisito puede producirse cuando los requerimientos de calidad de servicio QoS no pueden ser satisfechos por una VPN IPSec.

Dentro de los dispositivos principales están:

- Router IOS

Dentro de las amenazas que combate están:

- Falsificación de direcciones IP
- Acceso no autorizado

[13] Extending the Security Blueprint to Small, Midsize, and Remote-User Networks. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf, 2001

2.2.1.4 Diseño de la red de la Unidad Educativa

Las Figuras 2.2 y 2.3 muestran el diseño de las seguridades lógicas de la red de la Unidad Educativa para las secciones secundaria y primaria respectivamente, elaborado en base a la arquitectura modular SAFE de CISCO, la cual permitirá crecer dependiendo de las necesidades futuras que pudieran presentarse.

Este diseño incluye la implementación de nuevos servidores que permitirán brindar los servicios adicionales que necesita la Institución.

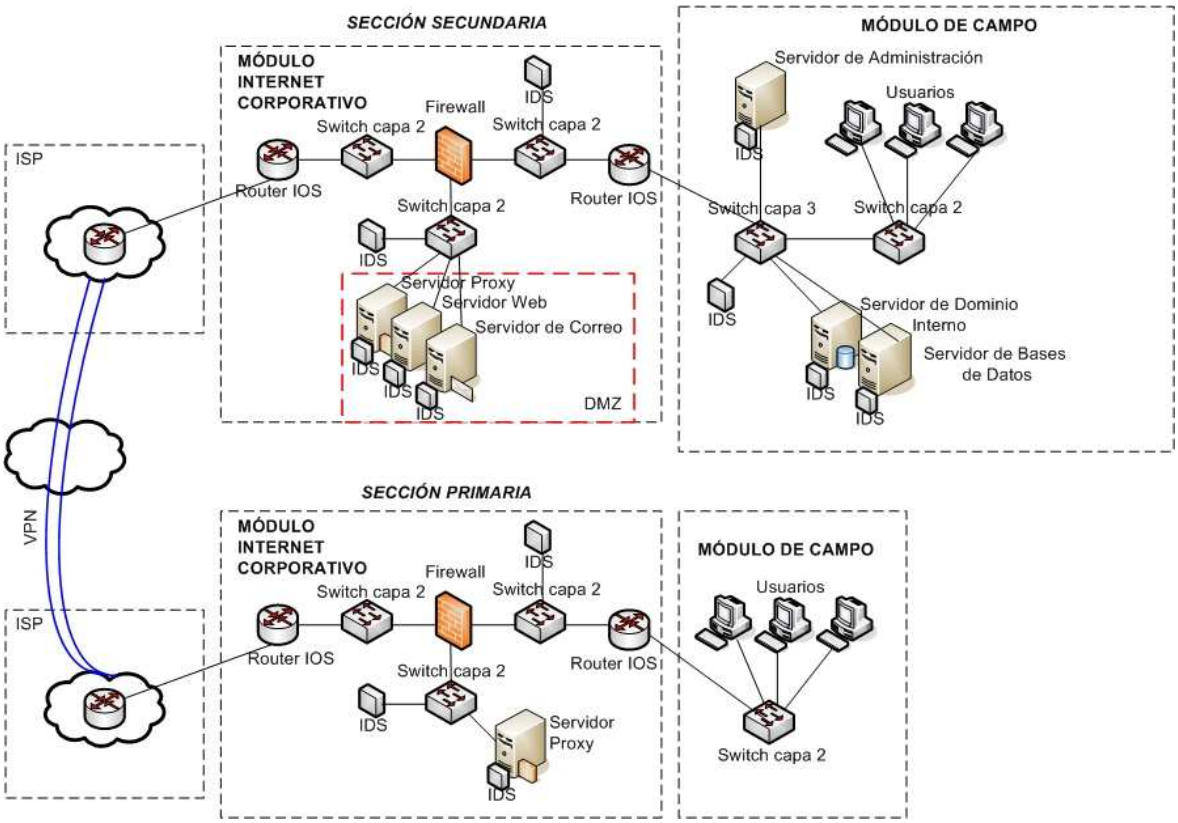


Figura 2.2 Diseño de Seguridad de la Red de la Unidad Educativa

El diseño no incluye el Módulo WAN por cuanto se opta por implementar una VPN sitio a sitio en lugar de un enlace WAN dedicado.

El diseño del esquema de direccionamiento IP será el que la institución determine.

La Tabla 2.1 describe los módulos y los equipos necesarios para la implementación del diseño de seguridad sugerido en ambas secciones.

Sección	Módulos “SAFE” de Cisco	Cantidad	Equipos
Secundaria	Módulo Internet Corporativo	1	Routers IOS
		1	Router con protección firewall
		1	Firewall
		1	Servidor Proxy
		1	Servidor Web
		1	Servidor de Correo
		1	NIDS
		3	Switch capa 2
	Módulo de Campo	1	Servidor de Administración
		1	Servidor de Dominio Interno
		1	Servidor de Bases de Datos
		1	Switch capa 2
		1	Switch capa 3 IDS
Primaria	Módulo Internet Corporativo	1	Routers IOS
		1	Router con protección firewall
		1	Firewall
		3	Switch capa 2
		1	Servidor Proxy
		1	NIDS
	Módulo de Campo	1	Switch capa 2

Tabla 2.1 Equipos requeridos para el diseño seguro de la red

La especificación técnica de los equipos se detalla en el capítulo 3.

2.3 PROPUESTA DE POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

2.3.1 POLÍTICAS DE SEGURIDAD

El objetivo de la política es proteger los activos de información de la organización de todos los intentos de amenazas internas, externas, deliberadas o accidentales y proporcionar la guía y apoyo del Centro de Informática para la seguridad de la información en relación a los requisitos de la institución y a las leyes y regulaciones relevantes.

Las políticas de seguridad garantizan que:

- La información estará protegida contra cualquier acceso no autorizado.
- La confidencialidad de la información será garantizada.
- La integridad de la información se mantendrá.
- La disponibilidad de información para los procesos de la Institución se mantendrá.
- Los requisitos legales y reglamentarios se cumplirán.
- Los planes de continuidad de negocio se desarrollarán, el mantenimiento y prueba de formación seguridad de la información estará disponible para todos los empleados.
- Todas las violaciones de seguridad, reales o presuntivas serán reportadas al Jefe del Centro de Informática y serán investigadas a fondo.

La norma ISO/IEC 27002 representa una compilación de las mejores prácticas para la gestión de la seguridad de la información que toda organización debería tomar en cuenta al momento de la implementación de las políticas de seguridad. Esta norma se enfoca en los siguientes controles:[14]

- Política de seguridad
- Aspectos organizativos para la seguridad

[14] http://www.iso27000.es/download/ControlesISO17799-2005.pdf

- Gestión de activos
- Seguridad ligada a los recursos humanos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Adquisición, desarrollo y mantenimiento de sistemas de información
- Gestión de incidentes de seguridad
- Gestión de continuidad del negocio
- Conformidad

Esta propuesta está desarrollada en base a la los lineamientos anteriormente mencionados y además toma en cuenta las falencias detectadas en el análisis de riesgos.

2.3.1.1 Organización de la seguridad de la información

2.3.1.1.1 Organización Interna

La Unidad Educativa deberá contar con una política de seguridad de la información, impulsada por el Centro de Informática, apoyada por el grupo responsable de la gestión de seguridad, aprobada y respaldada por el Rector de la institución.

2.3.1.1.2 Terceros

Los acuerdos con terceras partes que impliquen el acceso, proceso, comunicación o gestión de información de la Unidad Educativa o de las instalaciones del Centro de Informática o la adición de productos o servicios, deberán cumplir todos los requisitos de seguridad relevantes, ser registrados por el Centro de Informática y contar con la aprobación del Rectorado.

2.3.1.2 Gestión de activos

2.3.1.2.1 Responsabilidad sobre los activos

Todos los activos de información de la Institución tendrán asignado un responsable, el cual comunicará al jefe inmediato superior en caso de fallas, virus informáticos o cualquier otra novedad.

Se llevará un inventario detallado de todos los equipos informáticos que posee la Unidad Educativa y del software que haya sido adquirido, utilizando software específico para tal propósito.

Solo el personal del Centro de Informática, será el responsable de las reparaciones de los equipos informáticos y tendrá la obligación de registrar el reemplazo de partes y piezas dañadas.

2.3.1.2.2 Clasificación de la información

La información será clasificada y tratada de acuerdo a su sensibilidad y criticidad, siguiendo los parámetros establecidos en el procedimiento detallado en el punto 2.3.2.5 sobre el manejo de la información.

2.3.1.3 Seguridad ligada a los Recursos Humanos

2.3.1.3.1 Seguridad en la definición del trabajo y los recursos.

Cada posición dentro de la Institución tendrá una descripción del trabajo a realizar, esta descripción contendrá todos los elementos importantes del trabajo, tales como: las principales tareas y responsabilidades, relación con otras posiciones, las habilidades y la experiencia necesarias para calificar y será elaborada y actualizada por el jefe del departamento donde pertenece la posición y aprobada por el Jefe del Departamento de Recursos Humanos.

2.3.1.3.2 Inclusión de la seguridad en las responsabilidades laborales

Si la posición requiere tratar con información sensible o crítica se añadirá información adicional concerniente a los requisitos de seguridad tales como: las funciones y responsabilidades con respecto a la seguridad de la información.

Empleados, contratistas y terceros firmarán contratos elaborados por el abogado de la Institución, donde se establezcan claramente sus obligaciones y se especifiquen sus responsabilidades respecto a la seguridad de la información.

Todo empleado, contratista y tercero que maneje información sensible o crítica deberá firmar además un acuerdo de confidencialidad; es decir, deberá comprometerse a no divulgar a nadie, la totalidad o parte de esta información, en el curso de su empleo o contrato y en cualquier momento después de su terminación.

2.3.1.3.3 Finalización o cambio del puesto de trabajo

Todo empleado que sea notificado de pase, baja, despido o retiro voluntario, no podrá mantenerse en su puesto con las mismas atribuciones que tenía previa a la notificación, no podrá tener acceso a las instalaciones, equipos, material, programas o archivos, debiéndose restringir el acceso físico y a la información.

Si un empleado, contratista o tercero saliente conociera contraseñas para acceso a algún servicio, estas deberán ser cambiadas una vez finalizado o cambiado el empleo, contrato o acuerdo.

2.3.1.4 Seguridad Física y del Entorno

2.3.1.4.1 Áreas Seguras

Los proveedores, padres de familia, visitantes en general, deberán registrarse para poder ingresar a la Unidad Educativa, siguiendo el procedimiento descrito en

el punto 2.3.2.9.

El área de los servidores y equipos de comunicación contará con equipos contra fallos en el suministro de energía u otras anomalías eléctricas, UPS, extintor de incendios, detector de humo, conexión a tierra y estará ubicada en un área restringida y sin humedad.

Solo se permitirá el acceso al área de los servidores a los miembros del Centro de Informática autorizados.

Todas las áreas deberán permanecer cerradas bajo llave cuando el personal se movilice a otro lugar para participar en ceremonias, reuniones de trabajo o actividades de esparcimiento.

Se atenderá a los señores padres de familia, cadetes, proveedores y visitantes solo en las áreas autorizadas y dentro del horario establecido para tal propósito.

2.3.1.4.2 Seguridad de los equipos

Todos los visitantes deberán registrar cualquier equipo de cómputo que ingrese a la Institución, para lo cual deberán seguir el procedimiento especificado en el punto 2.3.2.11.

Los empleados de la Institución podrán permanecer en la misma solo durante su jornada de trabajo, salvo autorización escrita del señor Rector de la Institución y registro de la fecha, hora de entrada y salida por parte del personal militar de prevención y/o de los señores conserjes.

Para sacar equipos informáticos de la institución se seguirán el procedimiento especificado en el punto 2.3.2.12 y deberán ser transportados con todas las medidas de seguridad pertinentes.

2.3.1.5 Gestión de Comunicaciones y Operaciones

2.3.1.5.1 Procedimientos y responsabilidades de operación

El Jefe del Centro de Informática será el responsable de establecer y vigilar que las responsabilidades de sus subalternos se cumplan, segregando las tareas por lo menos en las áreas de: desarrollo de software, administración de la base de datos, help desk, mantenimiento de equipos, administración de la red y gestión de seguridad.

El responsable del mantenimiento de equipos será el encargado de elaborar y ejecutar el cronograma para el mantenimiento preventivo de todos los equipos informáticos de la Institución, que se realizará de preferencia en los períodos vacacionales.

El Jefe del Centro de Informática será el encargado de aprobar el cronograma de mantenimiento y comunicar del mismo a los diferentes departamentos.

Todos los procedimientos de operación serán documentados y puestos a disposición de todos los usuarios que los necesiten.

El Centro de Informática no podrá cerrarse en el período vacacional, deberá permanecer por lo menos una persona responsable del mismo.

2.3.1.5.2 Supervisión de los servicios contratados a terceros

El Centro de Informática deberá monitorear a intervalos regulares, los servicios informáticos proporcionados por terceros, para verificar el cumplimiento de los acuerdos de prestación de servicios.

En caso de encontrarse novedades en el monitoreo de los servicios, el Jefe del Centro de Informática, una vez conocida y verificada la novedad, deberá solicitar y controlar que se realicen los cambios necesarios, con el fin de asegurar que los

servicios que presta el tercero, cumplan con todos los requerimientos acordados**.**

2.3.1.5.3 Planificación y aceptación del sistema

El Jefe del Centro de Informática planificará el desarrollo o la adquisición o del software en base a las necesidades de la Institución y será el responsable realizar una evaluación exhaustiva del mismo, antes de ponerlo en marcha o realizar la compra.

Todo el software que se utilice en la Institución deberá contar con las licencias respectivas, los discos originales permanecerán bajo responsabilidad del Centro de Informática.

Se prohíbe instalar y correr programas que no sean necesarios para realizar las actividades laborales y sin la autorización escrita del Centro de Informática.

2.3.1.5.4 Protección contra código malicioso y código móvil

El Centro de Informática adquirirá por lo menos dos antivirus para el control de todos los equipos de la red, los cuales deberán ser actualizados en línea en forma periódica.

Todos los equipos móviles de propiedad de los empleados o de visitantes deberán registrarse en el Centro de Informática para obtener la autorización de funcionamiento y conexión a la red, antes de utilizarlos dentro de las instalaciones de la Unidad Educativa.

2.3.1.5.5 Gestión interna de soportes y recuperación

Todos los usuarios deberán realizar frecuentemente copias de seguridad de la información importante y probar su correcta recuperación.

La información sensible y crítica deberá respaldarse siguiendo el procedimiento

detallado en el punto 2.3.2.15

2.3.1.5.6 Gestión de redes

El administrador de la red contará con un esquema físico y lógico de la red, donde se detallen cada uno de los puntos de red, sus conexiones y direcciones.

Todos los puntos de la red serán certificados para evitar fallas en la transmisión de la información.

Se agregarán puntos de red previo un análisis de factibilidad y bajo la aprobación del administrador de la red, respetando las normas de cableado estructurado.

En caso de deterioro de los puntos de red, el responsable del departamento o área, comunicará el particular al Jefe del Centro de Informática, para que se proceda a la inmediata reparación.

Se implementarán todos los controles necesarios para proteger la información sensible que pasa por las redes públicas.

El administrador de la red será el responsable de generar reportes semanales sobre las actividades no autorizadas detectadas en la red y entregarlos al Jefe del Centro de Informática, para que se tomen las medidas pertinentes

2.3.1.6 Control de Accesos

2.3.1.6.1 Acceso Físico

Los equipos deberán estar ubicados bajo condiciones que ofrezcan seguridades físicas, eléctricas y medio ambientales y además que permitan el acceso físico sin ninguna restricción al personal del Centro de Informática.

En casos emergentes a más del personal autorizado del Centro de Informática,

las autoridades de la institución podrán ingresar al cuarto de servidores.

2.3.1.6.2 Acceso a la información (archivos y documentos)

Los equipos portátiles serán protegidos por software de control de acceso, antivirus y firewalls para evitar que cuando salgan de la institución regresen con problemas ocasionados por virus, software no deseado o mal manejo del equipo.

Todos los usuarios deberán cerrar la sesión de su computador personal cuando no lo estén utilizando o activar un protector de pantalla con contraseña.

Si el usuario detectara la infección de su equipo con algún virus, deberá notificar inmediatamente al Centro de Informática y desconectar al equipo de la red, hasta solucionar el inconveniente.

2.3.1.6.3 Respaldos y recuperación de archivos, aplicaciones y bases de datos

El personal del Centro de Informática será el responsable de realizar los backups de la información almacenada en los equipos portátiles.

El Centro de Informática será quien garantice la protección de la información del usuario que se encuentra almacenada en los servidores de bases de datos, servidores de aplicaciones, asegurando su integridad y disponibilidad de acuerdo a sus normas establecidas.

2.3.1.6.4 Acceso a los servicios de red

El Centro de Informática se responsabilizará de la administración, operación y correcto funcionamiento de los servicios de la red.

El Centro de Informática será quien otorgue permisos a los empleados para el acceso a la información y los servicios de la red, dependiendo del perfil de cada uno.

El Centro de Informática será el que controle que el acceso a la red de servicios públicos de la Institución y a la información que estará disponible las 24 horas del día.

El Centro de Informática se responsabilizará de la administración de las IPs públicas y privadas.

El Centro de Informática será quien asegure la disponibilidad de los servicios para los usuarios de ambas secciones.

El Centro de Informática será quien realice el monitoreo de la red y si encontrara alguna actividad sospechosa ocasionada por un computador dentro de la red, lo desconectará de la red hasta solucionar el problema.

2.3.1.6.5 Administración de usuarios

El Centro de Informática será quien cree las cuentas de los nuevos usuarios en la red, con su respectivo nombre de usuario y contraseña.

Cada usuario en su primer ingreso podrá cambiar su contraseña, la cual será única e intransferible.

El Centro de Informática podrá crear cuentas temporales con el respectivo control de acceso y dependiendo del perfil solicitado.

El Centro de Informática será el encargado de dar mantenimiento a las cuentas de usuario, es decir realizar modificaciones o eliminarlas, previo requerimiento del jefe del departamento solicitante.

2.3.1.6.6 Correo electrónico e Internet

El Centro de Informática será quien administre la información que ingresa por el

servidor de correo.

El Centro de Informática será quien controle la navegación de los usuarios y ponga límite al acceso a páginas de Internet que no tengan ningún vínculo con las funciones de la Institución y las actividades de empleados y estudiantes.

El Centro de Informática será quien definirá el tamaño máximo de archivos que podrá enviar o recibir cada usuario, dependiendo de las funciones y normas del departamento en el que labora.

El usuario no deberá abrir correos electrónicos enviados por remitentes desconocidos, no responderá estos mensajes y bajo ningún concepto ejecutará archivos adjuntos en dichos correos.

2.3.1.7 Adquisición, desarrollo y mantenimiento de sistemas de información

El Centro de Informática analizará las posibilidades de desarrollo o adquisición de software, en base a las necesidades de la institución y el presupuesto disponible, será el responsable de evaluar exhaustivamente la aplicación antes de ponerla en marcha o realizar la compra.

Todo software desarrollado en el Centro de Informática tendrá su respectiva documentación (manual de usuario, manual de programación y manual de instalación).

Todo software desarrollado en el Centro de Informática deberá seguir una metodología con sus respectivas normas y procedimientos seleccionados.

Toda modificación de software deberá tener su pedido formal proveniente del departamento o área que hace uso de la aplicación, adjuntando su justificación y estará guiada por el Jefe del Centro de Informática.

2.3.1.8 Gestión de Incidentes de Seguridad de la Información

El Centro de Informática será el responsable de monitorear, evaluar y gestionar en su totalidad los incidentes en la seguridad de la información.

Para el caso de un colapso total de aplicaciones o de bases de datos, se deberá definir un procedimiento de restauración de los respaldos de las mismas.

2.3.1.9 Capacitación del personal

El Centro de Informática deberá contar con un presupuesto y un plan de entrenamiento, que le posibilite capacitar a su personal en lenguajes para el desarrollo de software, nuevas aplicaciones que faciliten el trabajo de los usuarios, la administración de la red, la seguridad y el mantenimiento de los equipos.

2.3.2 PROCEDIMIENTOS

En la Tabla 2.2 se muestran las políticas de seguridad propuestas con sus respectivos procedimientos categorizados siguiendo los controles contemplados en las normas ISO /IEC 27002.

POLÍTICAS	PROCEDIMIENTOS
POLÍTICAS PARA LA ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN	
Organización Interna	Creación de nuevas políticas de seguridad y revisión de las políticas de seguridad existentes
Terceros	Permisos para el acceso de archivos
POLÍTICAS PARA LA GESTIÓN DE ACTIVOS	
Responsabilidad sobre los activos	Adquisición de nuevos equipos
	Adquisición de partes de hardware

	Instalación y/o cambio físico de equipos
	Registro y/o actualización de los datos del equipo y sus partes
Clasificación de la información	Manejo de la información
POLÍTICAS DE SEGURIDAD LIGADAS A LOS RECURSOS HUMANOS	
Seguridad en la definición del trabajo y los recursos. Inclusión de la seguridad en las responsabilidades laborales.	Contratación de personal o terceros
Finalización o cambio del puesto de trabajo	Cambio del puesto de trabajo Finalización de la relación laboral o contractual
POLITICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO	
Áreas Seguras	Ingreso a la Unidad Educativa
Seguridad de los equipos	Instalación y/o cambio físico de los equipos Dar de baja a un equipo Para ingresar equipos informáticos a la institución Para sacar un equipo fuera de la institución
POLÍTICAS PARA LA GESTIÓN DE COMUNICACIONES Y OPERACIONES	
Procedimientos y responsabilidades de operación	----------
Planificación y aceptación del sistema	----------
Supervisión de los servicios contratados	----------

a terceros	
Protección contra código malicioso y código móvil	----------
Gestión de redes	----------
Gestión interna de soportes y recuperación	----------
POLÍTICAS DE SEGURIDAD PARA EL CONTROL DE ACCESO A LOS SISTEMAS DE INFORMACIÓN	
Acceso Físico	Acceso al área de servidores.
Acceso a la información (archivos y documentos)	Permiso para el acceso a los archivos.
Respaldos y recuperación de archivos, aplicaciones y bases de datos	Respaldo de archivos, aplicaciones y bases de datos. Restauración de respaldos de archivos, aplicaciones y bases de datos.
Acceso a los servicios de red	Acceso a las aplicaciones. Acceso a las bases de datos. Acceso al correo e Internet. Acceso remoto.
Administración de usuarios	Creación de usuarios. Actualización (modificación y eliminación de usuarios) Bloqueo y desbloqueo de usuarios
Correo e Internet	Mantenimiento de correo electrónico Permisos y restricciones del acceso a páginas de Internet.
POLITICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN	
Adquisición, instalación y actualización	Actualización y/o instalación de

	software en los equipos Adquisición y registro del nuevo software en el Centro de Informática
Seguridad para el desarrollo de software	Metodologías establecidas por el Centro de Informática para el desarrollo de software
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
Seguridad ante desastres	Plan de restauración de aplicaciones y bases de datos
POLITICAS DE SEGURIDAD PARA LA CAPACITACIÓN DE PERSONAL	
Capacitación del personal	Plan de Capacitación

Tabla 2.2 Políticas y procedimientos de seguridad

Los procedimientos son detallados a continuación:

2.3.2.1 Creación de nuevas políticas de seguridad y revisión de las políticas de seguridad existentes

1. El Centro de Informática crea las políticas de seguridad informáticas en base a los requerimientos de la Unidad Educativa, cumpliendo con las fases de planificación, investigación, documentación y coordinación de las políticas.
2. El Jefe del Centro de Informática somete a revisión las políticas creadas al grupo de gestión de seguridad, conformado por los jefes de todas las áreas de la Unidad Educativa.
3. El Jefe del Centro de Informática entrega las políticas al Rectorado para su aprobación.
4. El Jefe del Centro de Informática coordinará las reuniones indispensables para difundir las políticas a todos los grupos afectados directamente por la misma, tales como: autoridades, personal administrativo, docente y alumnos.
5. Las políticas serán implementadas bajo la supervisión de los miembros del

grupo de gestión de seguridad.

6. El Jefe del Centro de Informática revisa las excepciones que pudieran aparecer una vez implementada la política.
7. El Jefe del Centro de Informática junto con los miembros del grupo de gestión de seguridad concienciarán a los usuarios de la necesidad del uso de las políticas realizando charlas informativas, cursos de entrenamiento, colocando afiches, circulares, etc.
8. Los miembros del grupo de gestión de seguridad monitorean junto con el Jefe del Centro de Informática el cumplimiento de las políticas establecidas.
9. En caso de incumplimiento de las políticas, se sanciona a o los usuarios no comprometidos con la seguridad.
10. El Jefe del Centro de Informática deberá revisar periódicamente las políticas para garantizar que estén actualizadas.
11. En caso de una política deba ser retirada, se deberá documentar la decisión anexando la siguiente información: fecha de retiro, motivo, persona que autoriza.

2.3.2.2 Adquisición de nuevos equipos

1. El Jefe del Centro de Informática recibe el pedido del jefe del área solicitante.
2. El Jefe del Centro de Informática analiza el requerimiento y de ser aprobado lo pasa al departamento administrativo, anexando un detalle de las características específicas del equipo, para que se realicen las cotizaciones respectivas en por lo menos tres empresas.
3. El departamento administrativo envía la cotización ganadora junto con el requerimiento al departamento financiero para la asignación de la partida presupuestaria. En caso de no existir presupuesto informa al Jefe del Centro de Informática del particular, caso contrario continúa el siguiente numeral.
4. El proveedor entrega el equipo al Jefe del Departamento Administrativo, y éste al Jefe del Centro de Informática.
5. El Jefe del Centro de Informática asigna un técnico para que configure el

equipo y realice las pruebas necesarias.

6. El técnico entrega el equipo al usuario correspondiente.

2.3.2.3 Adquisición de partes de hardware

1. El Jefe del Centro de Informática recibe el pedido de revisión de equipo por alguna falla.
2. El Jefe del Centro de Informática asigna a un técnico para que revise el equipo en cuestión.
3. El técnico identifica la pieza dañada e informa al Jefe de Centro de Informática para que verifique la existencia de dicha pieza en la bodega del Centro de Informática. En caso de no existencia continúa el siguiente numeral, en caso de existencia continúa el numeral 9.
4. El técnico genera una solicitud de material, donde se detalla con precisión las características de la pieza.
5. El Jefe del Centro de Informática envía esta solicitud para el departamento administrativo.
6. El departamento administrativo cotiza la pieza en por lo menos tres empresas y envía la mejor cotización al departamento financiero para verificar si existe el presupuesto.
7. En caso de existir el presupuesto, el departamento administrativo realiza la compra.
8. La parte o pieza es entregada al Jefe del Centro de Informática para que sea verificada e ingresada a la bodega del Centro de Informática.
9. El Jefe del Centro de Informática comunica al técnico la existencia de la pieza en la bodega.
10. El técnico registra la salida de la pieza de la bodega del Centro de Informática.
11. Reemplaza la pieza dañada y prueba el funcionamiento del equipo.
12. El técnico entrega el equipo al usuario.

2.3.2.4 Instalación y/o cambio físico de equipos

1. El Jefe del Centro de Informática recibe la solicitud del jefe del departamento o área solicitante.
2. El Jefe del Centro de Informática asigna un técnico para analizar la solicitud.
3. El técnico identifica si es cambio físico de equipo o instalación.
4. El técnico verifica si existen las instalaciones eléctricas y de red apropiadas en el lugar donde se va a ubicar el equipo.
5. Si no existieran las instalaciones, siga el siguiente numeral, caso contrario vaya al numeral 7.
6. El técnico informa la novedad al Jefe del Centro de Informática.
7. El Jefe del Centro de Informática solicita al departamento de mantenimiento que se realicen las instalaciones eléctricas.
8. El Jefe del Centro de Informática solicita a la empresa que proporciona los servicios de cableado se realice las instalaciones de red.
9. El técnico realiza la instalación o cambio físico del equipo.
10. El técnico informa al Jefe del Centro de Informática los resultados del proceso, para la actualización del esquema de red.

2.3.2.5 Manejo de la información

1. Cada jefe departamental clasificará a la información que maneja o genera en las siguientes categorías: secreta, confidencial y pública.
2. Se asignará la calificación de secreta (S) a la información más sensible, destinada estrictamente para uso interno, generalmente solo de conocimiento de las autoridades más altas de la Institución debido a que la divulgación no autorizada de información de este tipo tendría un serio y desfavorable impacto en el funcionamiento de la Institución.
3. Se asignará la calificación de confidencial (C) a la información menos sensible, pero destinados a uso interno debido a que la divulgación no autorizada de este tipo de información podría afectar desfavorablemente a la Institución.

4. Se asignará la calificación de pública (P) a la información de los resultados académicos de los estudiantes o las que el responsable de las relaciones públicas haya aceptado de forma explícita para su distribución pública, tales como folletos, revistas y comunicados de prensa.
5. Para el procesamiento de la información se usarán las medidas de seguridad detalladas en la Tabla 2.3.

Procesamiento requerido		Clasificación información		
Procesamiento	Medidas de seguridad	S	C	P
Medios de almacenamiento	Encripción o controles de acceso tangibles	x	x	
	Encripción no recomendada			x
Copia	La obtención del consentimiento del propietario es necesaria	x	x	
	No hay restricción			x
Envío de faxes	Dispositivos de recepción deben estar protegidos por contraseña o direcciones presentes para recepción	x	x	
	No hay restricción			x
Transmisión a través de redes públicas	Encripción	x	x	
	Encripción no recomendada			x
Destrucción	Trituración o eliminación en un lugar seguro para este fin	x	x	
	Tarro de basura			x
Divulgación a terceros	Consentimiento del propietario y acuerdo de confidencialidad	x	x	
	Sin restricción			x
Etiquetado de los	Etiquetado interno y externo	x	x	

medios electrónicos cuando sea necesario	Fecha de divulgación y clasificación			x
Etiquetado de documento cuando sea necesario	En cada página si no estuviera atado y sobre la portada y contraportada.	x	x	
	Fecha de divulgación y clasificación			
Embalaje de correo interno y externo	Dirigida a un destinatario específico y colocada dentro de dos sobres, con la etiqueta de clasificación en el sobre interior solamente.	x	x	
	Un sobre simple sin ningún tipo específico de etiquetado			x
Concesión de derecho de acceso	Solo al propietario del activo.	x	x	
	Sin restricciones			x
Pista de auditoria	Destinatario, número de copias realizadas, localización, dirección, destrucción, testigos.	x	x	
	Solo requerida si es privado.		x	
	No se recomienda			x

Tabla 2.3 Medidas de seguridad para el procesamiento de información según su clasificación

2.3.2.6 Contratación de personal o terceros

1. El Jefe del Departamento de Recursos Humanos recibe un requerimiento del jefe del departamento solicitante.
2. El Jefe del Departamento de Recursos Humanos verifica la descripción del puesto de trabajo a ser ocupado.
3. El Jefe del Departamento de Recursos Humanos solicita utilizando los medios de comunicación que considere adecuados el personal.
4. El Jefe del Departamento de Recursos Humanos recepta las carpetas de

los aspirantes y verifica la información de los mismos.

5. El Jefe del Departamento de Recursos Humanos junto con el jefe del departamento solicitante, revisan las carpetas recibidas y evalúan las misma teniendo en cuenta títulos y experiencia.
6. El Jefe del Departamento de Recursos Humanos cita a los 5 aspirantes mejores puntuados al rendimiento de pruebas sicológicas y de conocimientos prácticos sobre el puesto a ser ocupado.
7. Los dos aspirantes que obtengan las mejores puntuaciones deberán presentarse a una entrevista con el Señor Rector.
8. El señor Rector comunica el Departamento de Recursos Humanos el nombre de la persona seleccionada para ocupar el cargo.
9. El abogado de la institución elabora el contrato laboral, donde se especifique sus obligaciones y de ser necesario por sus funciones deberá elaborarse también un acuerdo de confidencialidad.
10. El aspirante seleccionado firma el contrato y acuerdo de confidencialidad.

2.3.2.7 Cambio del puesto de trabajo

1. El Jefe del Departamento de Recursos Humanos notifica al jefe del departamento donde laboraba el empleado sobre su cambio de puesto de trabajo.
2. El jefe del departamento donde laboraba el empleado solicita al Jefe del Centro de Informática la eliminación del usuario.
3. El jefe del departamento donde laborará el empleado solicita al Jefe del Centro de Informática la creación del usuario.
4. EL Jefe del Centro de Informática sigue el proceso indicado para esta solicitud, detallado en el punto 2.3.2.22.

2.3.2.8 Finalización de la relación laboral o contractual

1. El Jefe del Departamento de Recursos Humanos notifica al jefe del departamento donde laboraba el empleado sobre su pase, baja, despido o retiro voluntario.

2. El jefe del departamento donde laboraba el empleado solicita al Jefe del Centro de Informática la eliminación del usuario.
3. El Jefe del Centro de Informática sigue el proceso indicado para esta solicitud, detallado en 2.3.2.23

2.3.2.9 Ingreso a la Unidad Educativa

El personal militar de prevención se encargará del control de acceso a los visitantes, utilizando el siguiente procedimiento:

1. Registrará el número de cédula de los visitantes, la fecha, hora de ingreso y el motivo de la misma.
2. Solicitará la autorización de ingreso vía telefónica al departamento a ser visitado.
3. Si el acceso es autorizado, entregará al visitante una tarjeta que indique el área a la cual solicitó el acceso.
4. Retendrá la cédula hasta que la persona haya salido de la Institución.
5. Colocará la hora de salida y entregará la cédula al visitante.
6. En caso que se ingrese con vehículo deberá registrarse también el número de placa del automotor.

2.3.2.10 Dar de baja a un equipo

1. El Jefe del Centro de Informática elabora el informe, indicando que el equipo ya no es funcional.
2. El encargado de activos fijos recibe y tramita el informe, solicitando que el equipo sea trasladado a la bodega de equipos dados de baja.
3. El Jefe del Centro de Informática solicita a un técnico revise que el equipo no contenga información no pública y si es el caso formatee los discos.
4. El técnico lleva el equipo a la bodega de equipos dados de baja.
5. El encargado de la bodega de equipos dados de baja firma el documento de entrega recepción.
6. El encargado de activos fijos da de baja el equipo.

2.3.2.11 Para ingresar equipos informáticos a la institución

1. El personal militar de prevención recibe el pedido verbal de ingreso de un equipo informático a la institución.
2. El personal militar de prevención llena la hoja de registro de ingreso de equipos informáticos, en el que consta las características de hardware del equipo.
3. El visitante revisa la hoja de registro para comprobar la información registrada.
4. El visitante ingresa con el equipo informático.
5. Cuando el visitante desea salir, el personal militar verifica las características del equipo anotadas en la hoja de registro.
6. Si coinciden, permite la salida del equipo, caso contrario reporta la novedad a su jefe inmediato superior.

2.3.2.12 Para sacar un equipo de la Unidad Educativa fuera de la institución

1. El Jefe del Centro de Informática recibe un requerimiento de parte del jefe departamental solicitante.
2. El Jefe del Centro de Informática autoriza la salida del equipo y asigna un técnico para que ejecute el requerimiento.
3. El técnico respalda la información del equipo.
4. El técnico instala todas las aplicaciones de seguridad necesarias para el equipo.
5. El técnico entrega la autorización de salida de equipos informáticos y el equipo al usuario.
6. El usuario abandona la institución con el equipo.

2.3.2.13 Acceso al área de servidores

Cuando exista algún problema o chequeo rutinario del cableado de datos y/o eléctrico que implique acceso al área de servidores por parte de terceros:

1. El Jefe del Centro de Informática solicita al departamento de administrativo la emisión de una orden de trabajo al servicio técnico contratado para este trabajo.
2. El Jefe del Centro de Informática acompaña al personal del servicio técnico durante toda la revisión y/o reparación que se realice en las instalaciones del cuarto de servidores.
3. Una vez realizada la revisión y/o reparación, el Jefe del Centro de Informática valida el trabajo, realizando todas las pruebas de funcionamiento que estime convenientes.
4. El Jefe del Centro de Informática notifica al departamento administrativo, los resultados del trabajo de reparación, para que se proceda al pago respectivo.

2.3.2.14 Permisos para el acceso a los archivos

Cuando exista algún problema en algún sistema desarrollado por parte de terceros:

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante para la solución de problemas en algún sistema desarrollado por terceros.
2. El Jefe del Centro de Informática solicita al departamento de administrativo la emisión de una orden de trabajo para la empresa o personal externo.
3. El Jefe del Centro de Informática proporciona el permiso para el acceso a los archivos requeridos por parte del personal externo.
4. Una vez concluido el trabajo por parte del personal externo, el Jefe del Centro de Informática realiza las validaciones necesarias para verificar el correcto funcionamiento junto con el jefe del área solicitante.
5. El Jefe del Centro de Informática notifica al departamento administrativo, los resultados del trabajo de reparación, para que se proceda al pago respectivo.

2.3.2.15 Respaldo de archivos, aplicaciones y bases de datos

1. El Jefe del Centro de Informática asigna a un técnico como responsable de la realización de respaldos de la información de la Unidad Educativa, que incluye los archivos, las aplicaciones y las bases de datos.
2. El Jefe del Centro de Informática define que información debe ser respaldada y con que periodicidad se realizará el proceso, tomando en cuenta la criticidad de la información.
3. El técnico asignado etiquetará los dispositivos backup antes de realizar los respaldos, respetando el formato escogido por el Centro de Informática.
4. El técnico realiza los respaldos.
5. El técnico realiza un informe que muestra el contenido de los dispositivos backup.
6. El técnico entrega los respaldos realizados y el informe al Jefe del Centro de Informática.
7. El Jefe del Centro de Informática procede al almacenamiento seguro de los respaldos realizados.

2.3.2.16 Restauración de respaldos de archivos, aplicaciones y bases de datos

1. El Jefe del Centro de Informática asigna a un técnico para que realice la restauración de los respaldos.
2. Si el backup se encuentra guardado fuera de la institución, el Jefe del Centro de Informática solicitará al departamento administrativo que gestione la salida del mismo.
3. Si el backup se encuentra almacenado localmente, el Jefe del Centro de Informática entrega el mismo al técnico para que sea restaurado.
4. El técnico restaura el backup solicitado y realiza las validaciones respectivas.
5. El técnico comunica al Jefe del Centro de Informática el resultado de la restauración del respaldo.

2.3.2.17 Acceso a las aplicaciones

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática crea el perfil para el acceso a la aplicación.
3. El Jefe del Centro de Informática asigna un técnico para instalar y configurar el equipo del usuario con la aplicación solicitada.
4. El técnico instala y configura el equipo del usuario con la aplicación solicitada.
5. El técnico realiza las pruebas correspondientes del funcionamiento de la aplicación.
6. El técnico informa al Jefe del Centro de Informática de los resultados obtenidos.

2.3.2.18 Acceso a la Base de Datos

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática crea los perfiles de usuario para el acceso solicitado.
3. El Jefe del Centro de Informática asigna a un técnico para que instale y configure el software cliente en el equipo del usuario para el acceso a la base de datos.
4. El técnico instala y configura el software cliente en el equipo del usuario para el acceso a la base de datos.
5. El técnico realiza las pruebas de funcionamiento necesarias para verificar el acceso a la base de datos solicitada.
6. El técnico informa al Jefe del Centro de Informática de los resultados obtenidos.

2.3.2.19 Acceso al correo electrónico

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática verifica la existencia o no de la cuenta solicitada, en caso de no estarlo la crea.
3. El Jefe del Centro de Informática informa al jefe del departamento solicitante el resultado de su solicitud.

2.3.2.20 Acceso al Internet

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática asigna a un técnico para que configure el acceso a Internet en el equipo del usuario
3. El técnico configura el servicio de Internet en el equipo del usuario.
4. El técnico realiza las pruebas necesarias para verificar el funcionamiento del servicio.
5. El técnico informa al Jefe del Centro de Informática de los resultados obtenidos.

2.3.2.21 Acceso remoto

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática realiza un análisis de la solicitud.
3. El Jefe del Centro de Informática comunica por escrito el resultado de la solicitud, anexando el justificativo correspondiente para la aprobación o negación de la misma. En caso de ser aprobada se continuará con el siguiente numeral.
4. El Jefe del Centro de Informática configura la cuenta de usuario de acuerdo a las políticas de acceso de los usuarios a los servicios de red.
5. El Jefe del Centro de Informática entrega la contraseña del usuario al jefe

del área solicitante del acceso remoto.

6. El jefe solicitante entrega la contraseña al usuario autorizado para realizar acceso remoto.

2.3.2.22 Creación de usuarios

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática crea el usuario y asigna el perfil y grupo que le corresponde, tomando en cuenta el área y cargo del usuario.
3. El Jefe del Centro de Informática asigna una contraseña temporal, la cual deberá ser cambiada la primera vez que el usuario accese a la red.
4. La contraseña tendrá una longitud de mínimo 6 caracteres, deberá contener por lo menos un caracter especial, uno numérico y un caracter alfabético en mayúscula.
5. La contraseña no podrá utilizar nombres comunes personales o fechas significativas para el usuario.
6. La contraseña será única e intransferible.

2.3.2.23 Actualización (modificación y eliminación) de usuarios

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática procede a realizar la actualización solicitada, modificación o eliminación de la cuenta de usuario.
3. El Jefe del Centro de Informática notificará al director solicitante que la solicitud ha sido realizada.

2.3.2.24 Bloqueo y desbloqueo de usuarios

En caso de vacaciones, comisiones de servicio fuera de la institución por más de un día, reincorporación luego de cualquier evento anterior o cuando algún jefe de cualquier área de la Unidad Educativa lo estime necesario podrá solicitar un

bloqueo o desbloqueo cuentas de usuario:

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. El Jefe del Centro de Informática bloquea la cuenta del usuario.
3. El Jefe del Centro de Informática recibe la solicitud para el desbloqueo de la cuenta de parte del jefe del área que había solicitado el bloqueo previo.
4. El Jefe del Centro de Informática desbloquea la cuenta del usuario.

2.3.2.25 Mantenimiento de correo electrónico

1. El Jefe del Centro de Informática realizará un monitoreo periódico en forma semanal para identificar los siguientes eventos:
   a) Correos tipo spam y los URL que los generan
   b) Tamaño de los mensajes mayor a 10 MB de las cuentas de usuarios.
2. Una vez identificados los URL que generan correos tipo spam, el Jefe del Centro de Informática los agregará a las listas negras en el servidor de correo.
3. Una vez identificadas las cuentas con tamaño de mensajes mayor a 10 MB, el Jefe del Centro de Informática notifica al usuario de dicha cuenta para que tome las acciones correctivas.

2.3.2.26 Permisos y restricciones del acceso a páginas de Internet

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante.
2. Si es una solicitud de restricción de acceso a páginas de Internet, el Jefe de Sistemas la agrega el URL a la lista de páginas no permitidas del firewall y continúa con el paso 6.
3. Si es una solicitud de permiso de acceso para páginas web, el Jefe de Sistemas valida en forma técnica si el acceso solicitado no provoca problemas en la red tales como: consumo excesivo de ancho de banda, posible descarga de virus, gusanos, troyanos, etc.

4. Si la solicitud no es aprobada continúa con el paso 6.
5. El Jefe del Centro de Informática agrega el URL solicitado en la lista de acceso permitido por el firewall.
6. El jefe del Centro de Informática notifica al jefe del departamento solicitante que la solicitud ha sido procesada, en caso de haber negado el acceso al URL solicitado, adjunta la justificación técnica respectiva.

2.3.2.27 Plan de restauración de aplicaciones y bases de datos

1. El Jefe del Centro de Informática determina la magnitud del daño en la pérdida de información (aplicaciones o bases de datos).
2. Si el daño incluye el hardware pase al numeral siguiente, caso contrario al numeral 4.
3. El Jefe del Centro de Informática instala y configura un equipo de las mismas características al dañado de tenerlo disponible o un equipo que soporte la información a restaurar.
4. Para la restauración de la aplicación o las bases de datos se sigue el procedimiento del punto 2.3.2.16.

2.3.2.28 Actualización y/o instalación de software en los equipos

1. El Jefe del Centro de Informática recepta el requerimiento por parte del jefe del área solicitante.
2. El Jefe del Centro de Informática asigna un técnico para que realice el análisis del requerimiento.
3. El técnico determina si el proceso es de actualización o instalación de nuevo software, si es actualización siga con el siguiente numeral, caso contrario vaya al 5.
4. El técnico pide permiso al Jefe del Centro de Informática para acceso a las páginas del fabricante del software, para actualizarlas en línea, siga con el numeral 11.
5. El técnico verifica en el registro de software la existencia o no del software requerido, si no existe continúa con el siguiente numeral.

6. El técnico informa al Jefe del Centro de Informática que no se cuenta con el software requerido.
7. El Jefe del Centro de Informática solicita al departamento administrativo la adquisición del software, adjuntando un detalle específico del mismo y el justificativo correspondiente.
8. El departamento administrativo realiza la adquisición y entrega el software al Jefe del Centro de Informática.
9. El Jefe del Centro de Informática entrega el software al técnico designado anteriormente.
10. El técnico instala el software en la máquina del usuario solicitante.
11. El técnico realiza las pruebas necesarias sobre el software para validar su correcto funcionamiento.
12. El técnico entrega el equipo al usuario solicitante, adjuntando un documento de entrega – recepción.
13. El técnico informa al Jefe del Centro de Informática el resultado de la operación realizada.

2.3.2.29 Adquisición y registro del nuevo software en el Centro de Informática

1. El Jefe del Centro de Informática recibe el requerimiento del jefe del área solicitante o un técnico del centro de informática.
2. El Jefe del Centro de Informática analiza el requerimiento.
3. El Jefe del Centro de Informática justifica el requerimiento y envía una solicitud al departamento administrativo, adjuntando en detalle las características del software a ser adquirido.
4. El departamento administrativo envía la solicitud al departamento financiero para que le sea asignada una partida presupuestaria.
5. Una vez asignada la partida, el departamento administrativo realiza la compra.
6. El departamento administrativo entrega el software al centro de informática, previo el registro del software por parte del encargado de activos.
7. El Jefe del Centro de Informática asigna un técnico para que registre el software en sus activos y realice copias de seguridad del software.

8. El técnico almacena los CDS originales en una caja de seguridad
9. El técnico instala el software en las máquinas solicitantes.
10. El técnico informa al Jefe del Centro de Informática el resultado de la operación realizada.

CAPITULO 3

ESPECIFICACIÓN Y CÁLCULO DE COSTOS DE LOS COMPONENTES DEL ESQUEMA DE SEGURIDAD

Este capítulo comprende el detalle de los equipos y software recomendados por el modelo de seguridad “SAFE” de Cisco para la implementación del diseño lógico y la especificación de los equipos necesarios para la implementación del diseño físico descritos en los capítulos anteriores. Además el cálculo del costo referencial del proyecto.

3.1 ESPECIFICACIÓN DE LOS COMPONENTES DEL ESQUEMA DE SEGURIDAD

A continuación se detallan las especificaciones técnicas, de la infraestructura y los equipos requeridos para la seguridad física, de los equipos activos y del software para la implementación del esquema de seguridad.

3.1.1 DE LA SEGURIDAD FISICA

Para la implementación del diseño de la seguridad física, la institución necesita los equipos detallados en la Tabla 3.1

Sección	Equipo	Cantidad requerida
Secundaria	Generador eléctrico	1
	Tablero de transferencia automática	1
	UPS	1
Primaria	UPS	1

Tabla 3.1 Especificación de los equipos requeridos – Seguridad Física

Las características mínimas requeridas para los equipos especificados anteriormente son:

Generador eléctrico:

- Cumplir con normas ecológicas.
- Potencia stand by: 15KW
- Fase: Monofásico
- Frecuencia: 60Hz
- Combustible: Diesel
- Tanque de combustible: 10 galones
- Silenciador tipo industrial
- Manual de operación y mantenimiento
- Batería y cables de batería
- Sistema de enfriamiento del motor diesel
- Motor de arranque 12V
- Batería independiente.

Tablero de transferencia automática:

- 125 amperios.
- Mecanismo de transferencia conectado a un breaker
- Frecuencia: 50-60 Hz
- Supervisión de sobre y bajo voltaje

UPS Sección Secundaria:

- Cantidad: 1
- Potencia: 6KVA, escalable.
- Tecnología: On line.
- Frecuencia: 50-60 Hz.
- Tomas de corriente: mínimo 5.
- Gabinete metálico con conexión a tierra.
- Protocolo remoto: SNMP.
- Monitoreo de software.

- Compatible y configurable con todos los sistemas operativos
- Permite múltiples disipaciones, apagado programado y notificación por difusión.

UPS Sección Primaria:

- Cantidad: 1
- Potencia: 3KVA, escalable.
- Tecnología: On line.
- Frecuencia: 50-60 Hz.
- Tomas de corriente: mínimo 5.
- Gabinete metálico con conexión a tierra.
- Protocolo remoto: SNMP.
- Monitoreo de software.
- Compatible y configurable con todos los sistemas operativos
- Permite múltiples disipaciones, apagado programado y notificación por difusión.

Además de los equipos anteriormente mencionados se necesita contar con la siguiente infraestructura mínima:

a) Adecuación del área destinada a las comunicaciones.
b) Control de acceso al área de servidores y Centro de Informática.
c) Sistema de Cableado Estructurado.
d) Sistema contra incendios.

a) Adecuación del área de servidores y telecomunicaciones

Sección Secundaria:

- Dimensiones: 4mts de largo por 2 metros de ancho
- Corregir fallas de humedad
- Colocar techo y piso falso
- Revisión del sistema eléctrico
- Refuerzo de vidrios de ventanas con láminas de seguridad antiatraco

b) Control de acceso al área de servidores y comunicaciones:
   - Lector de Banda Magnética (Lector de ranura)

c) Sistema de Cableado Estructurado
   - Estándares internacionales
   - Puntos: 134
   - Cable: UTP categoría 5e

d) Sistema contra incendios

   Sección Secundaria:
   - Instalación bajo la norma NFPA-72 (Nacional Fire Protection Association)
   - Sensores fotoeléctricos
   - Alarmas audibles y/o visibles
   - Tipo de activación: manual y/o automática
   - Agentes extintores: polvo químico, espuma, dióxido de carbono (CO_2)
   - Sistema independiente, es decir, que cuenta con su fuente propia de energía, transformador y batería.
   - Equipos aprobados por NFPA y UL SmokAlarm-USA

   Sección Primaria:
   - Rack climatizado con sensor de humo.

3.1.2 DE LOS EQUIPOS ACTIVOS

En esta sección se detalla las especificaciones técnicas de los equipos activos para la implementación del esquema de seguridad propuesto en el capítulo anterior.

Para cumplir con las recomendaciones dadas por la metodología “SAFE” de Cisco, se deberá adquirir algunos dispositivos específicos que no posee actualmente la Institución.

En la tabla 3.2 se detallan los equipos requeridos para la implementación del diseño sugerido.

Sección	Módulo "SAFE" de Cisco	Cantidad	Equipos Existentes	Equipos Requeridos	Equipo
Secundaria	Módulo Internet Corporativo	1	0	1	Router [(a)]
		1	0	1	Router con protección firewall [(b)]
		1	0	1	Firewall [(c)]
		1	1	0	Servidor Proxy
		1	0	1	Servidor Web [(d)]
		1	0	1	Servidor Correo [(e)]
		3	0	3	Switch capa 2 [(f)]
	Módulo de Campo	1	0	1	Servidor de Administración [(g)]
		1	0	1	Servidor de Dominio [(h)]
		1	0	1	Servidor de Bases de Datos [(i)]
		1	0	1	Switch capa 3 IDS [(j)]
		1	1	0	Switch capa 2
Primaria	Módulo Internet Corporativo	2	0	2	Routers IOS
		1	0	1	Router con protección firewall
		1	0	1	Firewall
		3	0	3	Switch capa 2
		1	1	0	Servidor Proxy
Secundaria	Módulo de Campo	1	1	0	Switch capa 2

Tabla 3.2 Especificación de los equipos requeridos – Equipos Activos

Los equipos requeridos para el diseño deberán cumplir con las siguientes especificaciones técnicas mínimas:

a) Router:
   - Tipo appliance
   - Memoria Ram: 32 MB
   - Memoria Flash: 8 MB
   - Protocolo de Interconexión: Ethernet, Fast Ethernet
   - Monitoreo: SNMP, HTTP
   - Soporte VPN, Multiprotocolos
   - Interfaces habilitadas: 2 x red – Ethernet 10Base-T/100Base-TX-RJ45¦ 1 x gestión – consola – RJ-45¦ 1 x red – auxiliar – RJ-45

b) Router con protección firewall:
   - Memoria RAM: 128 MB
   - Memoria Flash: 32MB
   - Tecnología de conectividad: Cableado
   - Protocolo de interconexión de datos: Ethernet, Fast Ethernet
   - Capacidad: Conexiones SSL concurrentes: 10
   - Indicadores de estado: Actividad de enlace, alimentación
   - Características: Diseño modular, protección firewall, cifrado de hardware, asistencia técnica VPN, soporte MPLS, filtrado URL
   - Interfaces habilitadas: 2 x red – Ethernet 10Base-T/100Base-TX-RJ45¦ 1 x gestión – consola – RJ-45¦ 1 x red – auxiliar – RJ-45
   - Algoritmo de cifrado: DES, Triple DES, AES
   - Método de autentificación: Secure Shell v.2 (SSH2)
   - Cumplimiento de normas
   - Monitoreo: SNMP, HTTP

c) Firewall:
   - 4 puertos 10/100Base-TX
   - 1 puerto 10/100Base-TX para conexión DSL/Cable MODEM

- 1 puerto configurable DMZ
- Puerto consola (RS-232)
- Throughput: 80 Mbps (firewall), 25 Mbps (VPN)
- Hasta 12.000 sesiones simultáneas
- Hasta 100 túneles VPN dedicados
- WAN Balanceo de carga
- Autenticación de usuario vía Servidor RADIUS, Microsoft IAS, LDAP o base de datos interna (hasta 150 usuarios)
- Hasta 8 VLANs 802.1Q
- IGMP v3
- Stateful Packet Inspection (SPI) y Denegación de Servicio (DoS)
- Filtrado de contenidos (URL keyword blocking, Java/ActiveX/Cookie/Proxy blocking)
- Bloqueo IM/P2P
- Configuración basada en Web
- SNMP v1, Soporte v2c
- Administración del ancho de banda

d, e) Servidor Web, Correo:

- Procesador Xeon 2.00 GHz
- Memoria: 6GB
- 512 MB SAS RAID
- 2 discos hot plug 300 GB

f) Switch capa 2

- Nivel de conmutación: 2
- Tipo appliance
- Velocidad de conmutación (Throughput): 13 Mbps
- Capacidad de conmutación (Backplane): 17 Gbps
- MAC soportadas: 8000
- ACLs de L2
- VLANs

- Manejo de enlaces Trunking
- Monitoreo: SNMP v1/v2/v3, MIB, RMON (4 grupos: Alarmas, Eventos, Estadísticas e Historial), Interfaz WEB
- Spanning Tree
- Network Login
- QoS
- Número de colas por puerto:4
- Tráfico Multicast
- Soporte stacking y uplink
- MTBF mínimo
- Número de puertos habilitados: 48 10/100 Base –TX, 2 puertos 10/100/1000 Base -T

g, h, i) Servidor de Administración, Dominio y Bases de Datos

- Procesador Xeon 2.40 GHz
- Memoria: 6GB
- 512 MB SAS RAID
- 3 discos hot plug 300 GB

j) Switch capa 3 IDS:

- Nivel de conmutación: 3
- Incorporado módulo IDS
- Tipo appliance
- Velocidad de conmutación (Throughtput): 9 Mbps
- Capacidad de conmutación (Backplane): 12 Gbps
- ACLs de L2/L3/L4
- VLANs
- Manejo de enlaces Trunking
- Monitoreo: SNMP v1/v2/v3, MIB, RMON (4 grupos: Alarmas, Eventos, Estadísticas e Historial), Interfaz WEB, Telnet
- Spanning Tree
- Network Login

- QoS
- Número de colas por puerto:8
- Tráfico Multicast
- Soporte stacking y uplink
- MTBF mínimo
- Número de puertos habilitados: 1 puerto de consola, 8 puertos 10/100/1000 Base -T

3.1.3 DEL SOFTWARE

Con el objetivo de monitorear y detectar eventos ocurridos en la red que comprometan la seguridad, se sugiere el uso de NIDS, de acuerdo a la distribución de la Tabla 3.3.

Sección	Módulo "SAFE" de Cisco	Cantidad	Equipos Existentes	Equipos Requeridos	Equipos
Secundaria	Módulo Internet corporativo	1	0	1	NIDS
Primaria	Módulo Internet corporativo	1	0	1	NIDS

Tabla 3.3 Software Requerido para monitoreo de eventos

El software NIDS (Sistema de detección de intrusiones basado en red) debe contar con las siguientes características mínimas:

- Esté disponible bajo licencia GPL (GNU Public Licence).
- Sea distribuido, ligero, confiable, robusto, escalable y distinga de lo que es un ataque a un comportamiento normal del sistema.
- Sea multiplataforma.
- Posea una interfaz de línea de comandos (consola).
- Permita administración gráfica, remota y segura.
- Detecte ataques de capa 2 a capa 7 en el modelo OSI.

- Detecte tráfico anómalo.
- Permita implementar políticas en tiempo real.
- Permita guardar paquetes, analizarlos o ambas cosas.
- Tenga la capacidad para interactuar con bases de datos “Open Source”.
- Permita la actualización de firmas del IDS en línea.
- Genere alertas por medio de syslog, eventlog y consola.
- Detecte al menos los siguientes tipos de ataques: suplantación IP, inundación SYN, ping de la muerte, rastreo de puertos, backdoor, finger, paquetes malformados, malware, barrido de puertos, exploits, fallos en protocolos.
- Identifique y analice los protocolos (TCP/IP, UDP, ICMP, HTTP, NETBIOS, GRE, NNTP, DNS, RPC).

Para proteger a la red de la Unidad Educativa contra virus, troyanos, gusanos, adware, spyware, phising, rootkits, se necesitará adicionalmente un software antivirus para los equipos de la Unidad Educativa, que debe contar con las siguientes características mínimas:

- Detección de sistema operativo no actualizado.
- Protección integrada para estaciones y servidores.
- Análisis inteligente de archivos y red.
- Visualización de actividad gráfica del sistema de archivos y red.
- Bloqueo y detección proactiva de malware en dispositivos externos.
- Protección proactiva contra amenazas desconocidas.
- Antispam compatible con varios clientes de correo.
- Escalabilidad en licenciamientos y estaciones.
- Sistema de autodefensa.
- Actualización automática de bases de datos.
- Rescate de sistemas operativos altamente infectados.
- Escaneo automático de archivos, Internet y correo.
- Cuarentena en archivos infectados.
- Estadísticas gráficas de protección.

- Consola de administración centralizada.

Se sugiere además utilizar para los servidores de correo y Web la última versión estable del sistema operativo Linux Red Hat o Centos y para los servidores de Administración, Dominio y Bases de Datos el sistema operativo Windows 2008 Server.

3.1.4 DE LAS LICENCIAS

Con el objetivo de evitar las consecuencias producidas por el uso de software propietario sin licencia se sugiere que el Centro de Informática proceda a su legalización, partiendo de un estudio que tome en cuenta las reales necesidades de cada área, comenzando por la legalización del uso del sistema operativo.

3.1.5 GENERALES

Los requerimientos generales que deben cumplir tanto los equipos activos como el software antes mencionado, son los siguientes:

- Los equipos adquiridos deben cumplir con las características mínimas descritas y se debe garantizar compatibilidad, integración y operación entre los equipos ofertados con los equipos de comunicación de la institución.

- Las versiones del sistema operativo de todos los equipos deben ser las últimas versiones liberadas por el fabricante a la fecha de compra.

- Todos los equipos deben ser capaces del envío de registros de eventos y alarmas al equipo de Administración de la red.

- Se deberá incluir considerar las actualizaciones parches, IOS, firmas de virus, firmas de intrusiones y ataques así como los cables de conectividad, administración, manuales y CD’s.

3.2 CÁLCULO DE COSTOS DE LOS COMPONENTES DEL ESQUEMA DE SEGURIDAD

En esta sección se detallará los costos referenciales de los componentes necesarios para la implementación de la seguridad en la red de la Institución.

3.2.1 DETALLE DE LAS EMPRESAS

En base a los requerimientos obtenidos, se solicitó proformas con costos referenciales a empresas representativas del medio y especializadas en equipos e infraestructura para la seguridad física, equipos de red, software y licencias.

En lo referente al software, se tomó en cuenta soluciones que impliquen el uso de software libre debido a la política gubernamental en este tema especialmente en instituciones consideradas públicas.

Las empresas de las cuales se obtuvieron proformas, costos referenciales y documentación son las siguientes:

- Equipos e infraestructura para la seguridad física:
  - ✓ Comatecnica
  - ✓ Protecompu
  - ✓ http://www.sigmatron.com.ec
  - ✓ http://www.surge.com

- Equipos de Red:
  - ✓ Zona Tecnológica
  - ✓ Tecnoplus
  - ✓ http://www.cisco.com/web/LA/productos/
  - ✓ http://h71028.www7.hp.com/enterprise/cache/418226-0-0-64-470.html

- Software:
  - ✓ http://www.ecualug.org/
  - ✓ www.snort.org
  - ✓ Tecnoplus

- Licencias:
  - ✓ Zona Tecnológica
  - ✓ Enlace digital

3.2.2 CÁLCULO DEL COSTO REFERENCIAL (APROXIMADO)

A continuación se presenta un análisis referencial de costo aproximado analizado hasta el mes de julio de 2010.

3.2.2.1 Detalle del Costo – Seguridad Física

En las Tablas 3.4 y 3.5 se detalla el costo referencial de la seguridad física para la red de datos de la Institución que incluye el equipo, instalación y configuración. El detalle completo de las proformas se encuentra en el Anexo 8.

Sección	Equipo	Cantidad	Costo
Secundaria	Generador eléctrico	1	10.925,00
	Tablero de transferencia automática	1	855,00
	UPS 6KVA	1	4.350,00
Primaria	UPS 3KVA	1	1.964,00
	Total sin IVA		**18.094,00**

Tabla 3.4 Costo de los Equipos – Seguridad Física

Sección	Detalle	Costo
Secundaria	Adecuación área de servidores (techo falso, luminarias, piso falso, láminas de seguridad ventanas)	2.070,00
	Control de acceso en 2 puertas con instalación	1.272,50
	Aire acondicionado de precisión con instalación y mano de obra	9.923,00
	Sistema contra incendios área de servidores con instalación	5.424,28
Primaria	Adecuación área de servidores (RACK Mini Centro de Computo Climatizado con sensor de humo)	5.405,00
	Control de acceso en 1 puerta con instalación	636,25
Ambas	Implementación sistema de cableado certificado (134 puntos)	4.020,00
	Total sin IVA	**28.751,03**

Tabla 3.5 Costo de requerimientos adicionales – Seguridad Física

El costo total para la implementación de la seguridad física es de $46.845,03 (cuarenta y seis mil ochocientos cuarenta y cinco dólares con 03 centavos).

3.2.2.2 Detalle del Costo – Equipos Activos

En la Tabla 3.6 se detalla el costo referencial de los equipos activos necesarios para la implementación del diseño lógico de seguridad. El detalle completo de las proformas se encuentra en el Anexo 8.

Sección	Módulo "SAFE" de Cisco	Cant.	Equipos	Descripción del Equipo	Costo Unitario	Costo Total
Secundaria	Módulo Internet Corporativo	1	Router	Cisco 1801	1.260,00	1.260,00
		1	Router con protección firewall	Cisco 2801 Security Bundle, Adv. Security 64/256D	2.784,00	2.784,00
		1	Firewall	D-Link DFL-260	665,00	665,00
		1	Servidor Web	HP ProLiant DL 360G6	3.324,00	3.324,00
		1	Servidor de Correo	HP ProLiant DL 360 G6	3.324,00	3.324,00
		3	Switch capa 2	3Com 4210 26 Puertos	396,00	1.188,00
	Módulo de Campo	1	Servidor de Administración	HP ProLiant ML 350G6	3.840,90	3.840,90
		1	Servidor de Dominio	HP ProLiant ML 350G6	3.840,90	3.840,90
		1	Servidor de Bases de Datos	HP ProLiant ML 350G6	3.840,90	3.840,90
		1	Switch capa 3 IDS	3Com 5500G-EI 24 Puertos	3.984,00	3.984,00
Primaria	Módulo Internet Corporativo	1	Router	Cisco 1801	1.260,00	1.260,00
		1	Router con protección firewall	Cisco 2801 Security Bundle, Adv. Security 64/256D	2.784,00	2.784,00
		1	Firewall	D-Link DFL-260	665,00	665,00
		3	Switch capa 2	3Com 4210 26 Puertos	396,00	1.188,00
				Total sin IVA		**33.948,70**

Tabla 3.6 Costo de la implementación - Equipos Activos

El costo total de los equipos activos es de $33.948,70 (treinta y tres mil novecientos cuarenta y ocho dólares con setenta centavos).

3.2.2.3 Detalle del Costo – Software

En la Tabla 3.7 se detalla el costo referencial del software para los servidores necesarios para la implementación del diseño lógico de la red que permitirán brindar los servicios adicionales requeridos. El detalle completo de las proformas se encuentra en el Anexo 8.

Sección	Descripción	Cantidad	Precio Unitario	Valor Total
Ambas	Windows 2008 Server	3	810,00	2.430,00
	Total sin IVA			**2.430,00**

Tabla 3.7 Costo de la implementación – Software

El costo total del software es de $2.430 (dos mil cuatrocientos treinta dólares)

3.2.2.4 Detalle del Costo – Licencias

En la Tabla 3.8 se detalla el costo referencial de las licencias necesarias para la implementación del diseño lógico de seguridad planteado. El detalle completo de las proformas se encuentra en el Anexo 8.

Sección	Descripción	Cantidad	Precio Unitario	Valor Total
Ambas	Licencias ESET SMART Security 4.0 Business Edition	233	15,50	3.611,50
Ambas	Windows XP	225	156,42	35.194,50
	Total sin IVA			**38.806,00**

Tabla 3.8 Costo de la implementación - Licencias

El costo total del software es de $38.806 (treinta y ocho mil ochocientos seis dólares).

3.2.3 COSTO TOTAL DE LA IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD

El costo total referencial para la implementación del esquema de seguridad sugerido que no incluye IVA, aparece en la Tabla 3.9.

Seguridad Física	Equipos Activos	Software	Licencias	Costo Total
46.845,03	33.948,70	2.430,00	38.806,00	**122.029,73**

Tabla 3.9 Costo Total de la Implementación del Esquema de Seguridad

El costo total aproximado de la implementación del esquema de seguridad planteado es de $122.029,73 (ciento veinte y dos mil veinte y nueve dólares con 73 centavos).

CAPITULO 4

CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el análisis, diseño y propuesta técnica económica del esquema de seguridad para la institución educativa, se concluye y recomienda lo siguiente:

4.1 CONCLUSIONES

- El análisis de riesgos de la red de datos de la institución educativa, basado en el estudio del estado actual de la misma y apoyado en la metodología de Test de Penetración, determina que existen considerables amenazas y vulnerabilidades que afectan la seguridad.

- La carencia de control de acceso a áreas críticas, el uso de cableado sin certificación ni planificación, la falta de equipos que garanticen la seguridad de los equipos del área de servidores, la inexistencia de planes de contingencia, comprometen la seguridad física de la red.

- El uso de software propietario sin licencia, el escaso control de acceso lógico a los equipos y a las aplicaciones, así como también la falta de un software antivirus y de detección de intrusos, comprometen la seguridad lógica de la red.

- La inexistencia de normas y políticas de seguridad informática y el desconocimiento del personal responsable del Centro de Informática en el mismo tema, afectan considerablemente el manejo apropiado de la red de datos y la implantación de una cultura de seguridad informática en la Institución.

- La no utilización del enlace dedicado punto a punto entre la sección primaria y secundaria, ocasiona un gasto mensual innecesario y proporciona una vía para el acceso no controlado a la red de la institución.

- El diseño de un esquema de seguridad para la red de datos de la institución educativa, permite garantizar la integridad, disponibilidad y confidencialidad de la información que transita por la misma.

- Al utilizar las Normas ISO 27002 para el diseño del esquema de seguridad física y de las políticas y procedimientos de seguridad informática de la institución educativa, se toma en cuenta las mejores prácticas en los sistemas de gestión de seguridad de la información.

- La metodología modular y flexible planteada por el modelo de seguridad “SAFE” de Cisco para medianas empresas, permitió diseñar y utilizar un enfoque por fases para asegurar la red de la institución educativa.

- En base al esquema de seguridad propuesto, se realiza el cálculo aproximado de los costos de los componentes de hardware y software necesarios para su implementación, lo cual permitirá a la Institución Educativa decidir la implementación completa o por fases de acuerdo a su capacidad económica.

4.2 RECOMENDACIONES

- Se recomienda implementar el esquema de seguridad de datos diseñado por cuanto contempla todos los aspectos requeridos.

- Se recomienda dar charlas sobre la importancia de la seguridad informática dirigida a usuarios, personal del Centro de Informática y directivos.

- Se recomienda socializar las Políticas y Procedimientos de Seguridad a

todos los usuarios de la red y ponerlas en práctica una vez sean conocidas por todos.

- Se recomienda capacitar al personal del Centro de Informática en: administración de sistemas operativos, protocolos, lenguajes de programación, estándares de cableado, equipos activos, herramientas de hacking y escaneo de vulnerabilidades; con el objetivo de contar con personal idóneo que mantenga asegurada la red de datos.

- Se recomienda planificar la ejecución periódica de un “Test de Penetración” en la red de datos, con la finalidad de evaluar el resultado de los correctivos aplicados. En caso de ejecutarse intentos activos de intrusión, se recomienda al Centro de Informática tomar todas las medidas de contingencia y precauciones necesarias, para evitar interrupciones en los servicios que mantiene la institución, tanto para usuarios internos como externos.

- Se recomienda al Jefe del Centro de Informática realizar un balance entre la importancia de la información que maneja y el rubro asignado para mantenerla segura.

- Para desarrollar esquemas de seguridad de red, se recomienda ejecutar las fases de análisis de la situación actual de la empresa, la determinación de vulnerabilidades y amenazas y el establecimiento de los requerimientos, para con una visión clara del panorama elaborar un diseño apropiado que se acople a las necesidades de la empresa.

- Se recomienda que antes de contratar los servicios de un ISP, el Jefe del área de Informática realice un estudio previo, tomando en cuenta las necesidades de conectividad, seguridad y la configuración de la red.

- Se recomienda utilizar las normas ISO 27002 para establecer tanto políticas y procedimientos de seguridad informática como para diseñar esquemas de seguridad física, además realizar estudios periódicos respecto a normas o estándares factibles de aplicación en este campo.

- Se recomienda a los diseñadores y administradores de red utilizar el Modelo de Seguridad “SAFE” de Cisco como un referente para el diseño seguro de redes.

BIBLIOGRAFIA

Tesis

- VINUEZA Rhor Mónica de Lourdes, “Estudio y diseño de un sistema de seguridad para la red de datos del colegio Los Pinos”, 2003

- CARRANZA Espinosa Hugo Ruperto; GUTIERREZ Dávila Luis Antonio, “Políticas y estrategias de seguridad para la intranet de PetroEcuador”, 2004

- CHAUCA Chimbo Cristina Alexandra; VILLALBA Lindao Samira Paola, “Diseño de un esquema de seguridad para la intranet y extranet del CONESUP”, 2007

- MAIGUA Yugla Sandra Marisol; OLALLA Arguello Víctor Gabriel, “Análisis, diseño y propuesta técnica económica de un esquema de seguridad para la red de transmisión de datos de una empresa que presta el servicio de seguridad y control vehicular”, 2008

Libros

- KAEO, Merike. Diseño de seguridad en redes. Pearson Education S.A. Madrid, 2003.

- BEHROUZ A. Forouzan. Transmisión de datos y redes de comunicaciones, 4ta. Edición. McGraw Hill, 2006

Páginas Web

- Colegio Militar Nro. 10 “Abdón Calderón”
  http://www.comil10.edu.ec/index.html

- A Penetration Testing Model
  https://www.bsi.bund.de/cae/servlet/contentblob/471368/publicationFile/27983/penetration_pdf.pdf

- OSSTMM 2.1
  http://isecom.securenetltd.com/OSSTMM.es.2.1.pdf

- Extending the Security Blueprint to Small, Midsize, and Remote-User Networks
  http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.pdf

- Guía de Referencia Cisco SAFE
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/SAFE_rg.html

- Normas ISO 27002
  http://iso27000.wik.is/controles_iso_27002
  http://iso27000.wik.is/Area_Normas/ISO%2f%2fIEC_27002

- Portal de ISO 27001 en español
  http://iso27000.es/iso27000.html#section3c

- Términos de glosario
  http://es.wikipedia.org/wiki/

Herramientas de Escaneo

- Wireshark
  http://www.wireshark.org/download.html

- OCSInventory
  http://www.ocsinventory-ng.org/

- Scanline
  http://www.foundstone.com/us/resources/termsofuse.asp?file=scanline.zip

- Nmap
  http://nmap.org/download.html

- GFI LANguard
  http://www.gfi.com/downloads/register.aspx?pid=lanss

- NESSUS
  http://www.nessus.org/download/

- ParosProxy
  http://www.parosproxy.org/download.shtml

GLOSARIO

ACL Access Control List.- Lista de reglas que detallan puertos de servicio o nombres de dominios (de redes) que están disponibles en un terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio.

AMENAZA.- Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

ARP Address Resolution Protocol.- Protocolo de resolución de direcciones. Protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP.

Ataque DoS Denial of Service.- Ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

AVG.- Es un término global para un rango de antivirus y software relacionado con seguridad en Internet disponible para Microsoft Windows, Linux, y FreeBSD, desarrollado AVG Technologies. AVG Anti-Virus Free es la versión gratuita del antivirus AVG.

BOTNET.- Término que hace referencia a un conjunto de robots informáticos o bots, que se ejecutan de manera autónoma y automática con fines normalmente poco éticos. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del IRC. Las nuevas versiones de estas botnets se están enfocando hacia entornos de control mediante HTTP, con lo que el control de estas máquinas será muchos más simple.

Broadcast.- En español difusión, es un modo de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

CDP Cisco Discovery Protocol.- Protocolo de descubrimiento de Cisco, es un protocolo de red propietario de nivel 2, desarrollado por Cisco Systems y usado en la mayoría de sus equipos. Es utilizado para compartir información sobre otros equipos Cisco directamente conectados, tal como la versión del sistema operativo y la dirección IP. CDP también puede ser usado para realizar encaminamiento bajo demanda (ODR, On-Demand Routing), que es un método para incluir información de encaminamiento en anuncios CDP, de forma que los protocolos de encaminamiento dinámico no necesiten ser usados en redes simples.

Conficker.- También conocido como Downup Devian, Downandup y Kido, es un gusano informático que apareció en octubre de 2008, que ataca el sistema operativo Microsoft Windows. El gusano se propaga a sí mismo principalmente a través de una vulnerabilidad del desbordamiento de búfer del servicio Server de Windows. Usa una solicitud RPC especialmente desarrollada para ejecutar su código en el computador objetivo. Cuando ha infectado un computador, Conficker desactiva varios servicios, como Windows Automatic Update, Windows Security Center, Windows Defender y Windows Error Reporting. Luego se contacta con un servidor, donde recibe instrucciones posteriores sobre propagarse, recolectar información personal o descargar malware adicional en el computador víctima. El gusano también se une a sí mismo a ciertos procesos tales como svchost.exe, explorer.exe y services.exe.

CVE (Common Vulnerabilities and Exposures).- Código asignado a una vulnerabilidad que le permite ser identificada de forma univoca. Este código permite a un usuario conocer de una forma más objetiva una vulnerabilidad en un programa o sistema. El código identificador es del modo: CVE-año-numero, donde el número que aparece junto a la vulnerabilidad no tiene nada que ver con

el número de vulnerabilidades encontradas, sino suele ser un número que se asigna en bloque para un producto y por tanto solo es una referencia.

DCE/RPC DCE Remote Procedure Call.- Es un sistema de llamada a procedimiento remoto del conjunto de software Open Software Foundation.

DESBORDAMIENTO DE BUFFER.- Error de software que se produce cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande para contenerlos, sobrescribiendo de esta manera otras zonas de memoria. Esto se debe en general a un fallo de programación. La consecuencia de escribir en una zona de memoria imprevista puede resultar impredecible. Existen zonas de memoria protegidas por el sistema operativo. Si se produce la escritura fuera de una zona de memoria protegida se producirá una excepción del sistema de acceso a memoria seguido de la terminación del programa. Bajo ciertas condiciones, un usuario obrando con malas intenciones puede aprovecharse de este mal funcionamiento o una vulnerabilidad para tener control sobre el sistema.

DHCP Dynamic Host Configuration Protocol.- Protocolo de configuración dinámica de host de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

DIAL IN.- Conexión a Internet que se establece a través de un modem y una línea telefónica. A cada usuario se le asigna un número IP dinámico, válido **sólo** durante la comunicación.

DMZ.- Red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ sólo se permitan a la red externa -- los equipos host en la DMZ no pueden conectar con la red interna. Esto permite que los equipos

(hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

DNS Domain Name System.- Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

Dirección MAC Media Access Control.- Identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una ethernet de red. Se conoce también como la dirección física en cuanto a identificar dispositivos de red. Es individual, cada dispositivo tiene su propia dirección MAC determinada y configurada por el IEEE (los últimos 24 bits) y el fabricante (los primeros 24 bits).

EGB Educación General Básica.- Sigla con la que se denomina a la educación desde primer año hasta décimo año de educación general básica, según la reforma curricular del Ministerio de Educación de 1996, que era conocida anteriormente como educación primaria y ciclo básico.

EIA/TIA-568A.- Estándar de cableado de telecomunicaciones en edificios comerciales.

EIA/TIA-569.- Estándar para ductos y espacios de telecomunicaciones en edificios comerciales.

EIA/TIA-606.- Estándar de Administración para la infraestructura de telecomunicaciones de edificios comerciales.

EIA/TIA-606A – Estándar de etiquetado para redes.

EIA/TIA-607.- Requerimientos para telecomunicaciones de puesta a tierra y puenteado de edificios comerciales.

ESIGEF Sistema Integrado de Gestión Financiera.- Software que utiliza el personal financiero de todas las instituciones catalogadas como públicas para registrar sus actividades presupuestarias y contables.

GFILANguard.- Escáner de seguridad de red, que permite escanear, detectar, evaluar y remediar cualquier vulnerabilidad de seguridad de su red con mínimo esfuerzo administrativo.

GRE Generic Routing Encapsulation.- Protocolo para el establecimiento de túneles a través de Internet. Está definido en la RFC 1701 y en la RFC 1702, pudiendo transportar hasta 20 protocolos de red distintos.

GUSANO.- Malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario. A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos casi siempre causan problemas en la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corrompen los archivos de la computadora que atacan.

Harakit.- Es un gusano que se extiende mediante replicación a las máquinas de la red local o a través de unidades extraíbles, una vez que infecta el sistema, el gusano ejecutará archivos maliciosos cftmen.exe, cfrm.exe y otros en la carga de inicio del sistema. Harakit infecta a los sistemas víctima a través de correo spam, archivos infectados, programas de Chat. Harakit es un gusano dañino que cosecha información privada, daña sistemas de archivos y degrada drásticamente el rendimiento del PC.

Hot plug.- Conexión en caliente, capacidad que tienen algunos periféricos de poder enchufarse o desenchufarse al ordenador, sin apagar el mismo, y funcionar correctamente. Entre las conexiones con capacidad "hot-plug" se encuentran las conexiones USB, Firewire, SATA y SAS.

HTTP Hypertext Transfer Protocol o HTTP.- Protocolo de transferencia de hipertexto, es el protocolo usado en cada transacción de la World Wide Web.

ICMP Internet Control Message Protocol.- Sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IGMP.- Protocolo de red que se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia. La última versión disponible de este protocolo es la IGMPv3 descrita en el RFC 3376.

IP Internet Protocol.- Protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

IP Spoofing.- Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes alterados irán dirigidas a la IP falsificada.

IPSec Internet Protocol security.- Conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

ISO/IEC 27002.- Es un estándar de seguridad de la información publicada por ISO/IEC. Proporciona recomendaciones de mejores prácticas en los sistemas de gestión de seguridad de la información para la preservación de la confidencialidad, integridad y disponibilidad.

ISP Internet Service Provider.- Empresa que ofrece a sus clientes el acceso a Internet. El ISP conecta a sus clientes usando tecnologías apropiadas de transmisión de datos tales como DSL, cable modem, acceso inalámbrico o interconexiones dedicadas de alta velocidad.

LLMNR Link Local Multicast Name Resolution.- Protocolo basado en el formato de paquete DNS que permite tanto host IPv4 como IPv6 para llevar a cabo la resolución de nombres para los hosts del mismo vínculo local. Está incluido en Windows Vista, Windows Server 2008 y Windows 7.

LSASS.- Es un proceso en los sistemas operativos Microsoft Windows que se encarga de aplicar la política de seguridad en el sistema. Este verifica que los usuarios se logeen en una computadora Windows o servidor, maneja cambios de password y crea tokens de acceso, además escribe en el log de seguridad de Windows.

LOTAIP Ley Orgánica de Transparencia y Acceso a la Información Pública.- Ley vigente desde 2004 en nuestro país que otorga a los ciudadanos el derecho a demandar la rendición de cuentas sobre el uso de los fondos públicos. Fue creada pensando que el acceso a la información y la transparencia es una de las herramientas claves para lograr una verdadera democracia. Entre la información que debe presentar cada institución pública está: el distributivo del personal, las remuneraciones mensuales por puesto e ingresos adicionales, el sistema de

compensaciones, información sobre el presupuesto anual con ingresos, gastos, financiamiento y resultados operativos.

MTBF Mean Time Between Failures.- Promedio del tiempo entre fallos de un sistema. El MTBF es típicamente parte de un modelo que asume que el sistema fallido se repara inmediatamente (el tiempo transcurrido es cero), como parte de un proceso de renovación.

NBNS NetBIOS Name Service.- Se utiliza para resolver nombres de equipo a direcciones IP.

NESSUS.- Programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en nessusd, el daemon Nessus, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance y reporte de los escaneos. En operación normal, nessus comienza escaneando los puertos para buscar puertos abiertos y después intentar varios exploits para atacarlo. Las pruebas de vulnerabilidad, disponibles como una larga lista de plugins, son escritos en NASL (Nessus Attack Scripting Language, Lenguaje de Scripting de Ataque Nessus por sus siglas en inglés), un lenguaje scripting optimizado para interacciones personalizadas en redes.

NetBios Network Basic Input/Output System.- Proporciona servicios relacionados con la capa de sesión del modelo OSI, permitiendo a las aplicaciones en computadoras independientes comunicarse a través de una red de área local. Es estrictamente un APU, NetBios no es un protocolo de red.

NFPA National Fire Protection Association.- La autoridad en seguridad de fuego, eléctricidad y construcciones cuyo objetivo es reducir la carga mundial de incendios y otros peligros sobre la calidad de vida, ofreciendo y defendiendo códigos y normativas concensuadas, la investigación, el entrenamiento y la educación.

NMAP.- Programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich). Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática.

NNTP Network News Transport Protocol.- Protocolo inicialmente creado para la lectura y publicación de artículos de noticias en Usenet. Su traducción literal al español es "protocolo para la transferencia de noticias en red".

NIDS.- Sistema de detección de intrusos en una Red. Busca detectar anomalías que inicien un riesgo potencial, tales como ataques de denegación de servicio, escaneadores de puertos o intentos de entrar en un ordenador, analizando el tráfico en la red en tiempo real. Para ello, analiza todos los paquetes, buscando en ellos patrones sospechosos. Los NIDS no sólo vigilan el tráfico entrante, sino también el saliente o el tráfico local, ya que algunos ataques podrían ser iniciados desde el propio sistema protegido.

NOD32.- Es un programa antivirus desarrollado por la empresa ESET, de origen eslovaco. El producto está disponible para Windows, Linux, FreeBSD, Solaris, Novell y Mac OS X (este último en beta) 1 , y tiene versiones para estaciones de trabajo, dispositivos móviles (Windows Mobile y Symbian, servidores de archivos, servidores de correo electrónico, servidores gateway y una consola de administración remota.

OCSInventory Open Computer and Software Inventory Next Generation.- Es un software libre que permite a los usuarios administrar el inventario de sus activos de TI. OCS-NG recopila información sobre el hardware y software de equipos que hay en la red que ejecutan el programa de cliente OCS ("agente OCS de inventario").

OSFingerprinting.- Técnica que cosiste en analizar las huellas que deja un sistema operativo en sus conexiones de red. Está basada en los tiempos de

respuesta a los diferentes paquetes, al establecer una conexión en el protocolo TCP/IP, que utilizan los diferentes sistemas operativos.

OSSTMM Open Source Security Testing Methodology Manual.- Manual de Metodología de Testeo de Seguridad de Código Abierto elaborado por ISECOM Institute for security and Open Methodologies.

ParosProxy.- Software que permite evaluar la seguridad de aplicaciones Web. Es gratuito y completamente escrito en Java. A través del ParosProxy, todos los HTTP y HTTPS de datos entre el servidor y el cliente, incluyendo las cookies y campos de formulario, puede ser interceptados y modificados.

PING-PROBE.- Suite de herramientas de red que incluye: ping, traceroute, TCP port scanner, Network scanner, SNMP browser, bandwidth, monitor, DNS client, Finger Client, Whois Client, LDAP Client.

POP3 Post Office Protocol .- Protocolo que se utiliza en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el Modelo OSI.

PROXY.- Hace referencia a un programa o dispositivo que realiza una acción en representación de otro. Su finalidad más habitual es la de **servidor proxy**, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

QoS Quality of Service.- En español calidad de servicio, tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (throughput). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

REDES SOCIALES.- Las redes sociales son estructuras de relación, dónde las variables principales son los individuos o actores y la relación que existe entre ellos. Wikipedia indica que estas relaciones pueden ser variadas: financieras, amistad, relaciones sexuales, rutas aéreas, y otros. En estas clasificaciones entran las relaciones virtuales: Foros, chats, blogs, sites sociales, y otros.

RJ45.- Es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e, 6 y 6a). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos. Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado.

RPC Remote Procedure Call.- Llamada a Procedimiento Remoto, es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos. El protocolo es un gran avance sobre los sockets usados hasta el momento. De esta manera el programador no tenía que estar pendiente de las comunicaciones, estando éstas encapsuladas dentro de las RPC.

SAFE de CISCO.- Modelo de seguridad para redes de empresas que ofrece información sobre las mejores prácticas a las partes interesadas en el diseño e implementación de redes seguras. SAFE sirve de guía a los diseñadores de red que están planteándose los requisitos de seguridad de su red. SAFE adopta un enfoque de defensa en profundidad para el diseño de la seguridad de las redes, este tipo de diseño se centra en las amenazas que se esperan y en sus medios para combatirlas.

ScanLine.- Escaner de puertos de línea de comandos para todas las plataformas Windows. Puede realizar los tradicionales ping ICMP, puede mostrar los tiempos de respuesta del host y número de saltos, hacer escaneo TCP, escaneos UDP simples, resolver banners y nombres de host. La exploración se realiza de una forma rápida y puede manejar grandes cantidades de rangos de direcciones IP.

SID Security Identifier.- El SID es un nombre único (cadena de caracteres alfanuméricos) que se utiliza para identificar un objeto, como un usuario o un grupo de usuarios en una red de sistemas NT/2000. Windows concede o deniega el acceso y privilegios a los recursos basados en ACLs, las cuales utilizan los SIDs para identificar de forma única a los usuarios y su pertenencia a los grupos.

SIE Sistema Integrado Educativo.- Software institucional que engloba el área académica con el proceso de registro de notas, el área de secretaría con los procesos de inscripción y matrícula y el área de colecturía con los procesos de generación y pago de pensiones.

SISFT Sistema Fuerza Terrestre.- Antiguo software financiero proporcionado por la Fuerza Terrestre.

SiteMapper.- Generador de un mapa de sitio que puede usarse para obtener una buena idea de que tan grande es un sitio Web. También mapea archivos javascripts, hojas de cálculo, archivos media, links externos y links rotos.

SMB Server Message Block.- Protocolo de red que pertenece a la capa de aplicación en el modelo OSI, permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows y DOS.

SMTP Simple Mail Transfer Protocol (SMTP).- Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet.

SNIFFER.- Programa de captura de las tramas de red. Los sniffers tienen diversos usos como monitorear redes para detectar y analizar fallos o ingeniería inversa de protocolos de red. También es habitual su uso para fines maliciosos,

como robar contraseñas, interceptar mensajes de correo electrónico, espiar conversaciones de chat, etc.

SNMP.- El Protocolo Simple de Administración de Red es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento.

SSDP.- Simple Service Discovery Protocol.- Protocolo que sirve para la búsqueda de dispositivos UPnP en una red. Utiliza UDP en unicast o multicast en el puerto 1900 para anunciar los servicios de un dispositivo. Solo la información más importante acerca el dispositivo y el servicio ofrecido está contenido en los mensajes intercambiados. El protocolo se utiliza también para buscar ciertos servicios en la red.

SSH Secure **SH**ell**.-**, Intérprete seguro de órdenes. Es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo. Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

STP Shielded Twisted Pair.- Son las siglas utilizadas para referirse al cable de par trenzado apantallado. Se trata de cables de cobre aislados dentro de una cubierta protectora, con un número específico de trenzas por pie. STP se refiere a la cantidad de aislamiento alrededor de un conjunto de cables y, por lo tanto, a su inmunidad al ruido.

TCP Transmission Control Protocol .- Protocolo de Control de Transmisión, es uno de los protocolos fundamentales en Internet. Fue creado entre los años 1973 y 1974 por Vint Cerf y Robert Kahn. Muchos programas dentro de una red de datos compuesta por computadoras pueden usar TCP para crear conexiones entre ellos a través de las cuales puede enviarse un flujo de datos. El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron. También proporciona un mecanismo para distinguir distintas aplicaciones dentro de una misma máquina, a través del concepto de puerto. TCP da soporte a muchas de las aplicaciones más populares de Internet, incluidas HTTP, SMTP, SSH y FTP.

TELEACADÉMICO.- Sistema que proporciona información académica de los alumnos de varios colegios utilizando una interfaz Web.

TI Tecnología de Información.- Es el estudio, diseño, desarrollo, implementación, soporte o de gestión de sistemas de información. Tecnología de la información es un término general que describe cualquier tecnología que ayuda a producir, manipular, almacenar, comunicar y / o difundir información.

UDP User Datagram Protocol.- Protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

UPS.- Aparato eléctrico que proporciona energía de emergencia cuando la fuente de potencia de entrada falla, por medio de una o más baterías conectadas. El tiempo de duración de las baterías es relativamente corto pero suficiente para permitir acudir a una fuente de alimentación auxiliar en línea o apagar el equipo protegido.

UTP Unshielded Twisted Pair.- Son las siglas utilizadas para referirse al Cable de par trenzado sin apantallar. Son cables de pares trenzados sin apantallar que se utilizan para diferentes tecnologías de red local. Son de bajo costo y de fácil uso, pero producen más errores que otros tipos de cable y tienen limitaciones para trabajar a grandes distancias sin regeneración de la señal.

VPN Virtual Private Network.- Una red privada virtual es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

VIRUS.- Malware que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este. Los virus pueden destruir, de manera intencionada, los datos almacenados en un ordenador, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos. Los virus informáticos tienen, básicamente, la función de propagarse a través de un software, no se replican a sí mismos porque no tienen esa facultad como el gusano informático, son muy nocivos y algunos contienen además una carga dañina (payload) con distintos objetivos, desde una simple broma hasta realizar daños importantes en los sistemas, o bloquear las redes informáticas generando tráfico inútil.

VULNERABILIDAD.- Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza.

WIRESHARK.- Analizador de protocolos de red utilizado para realizar análisis y solucionar problemas en redes. Permite examinar datos de una red viva o de un archivo de captura salvado en disco. Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, y Mac OS X, así como en Microsoft Windows.

ZOMBIE.- Nombre que recibe una computadora que se encuentra infectada con un programa deamon, que permite ser controlada por un pirata informático de forma remota, sin el consentimiento del dueño de la misma. El deamon abre puertos específicos en el sistema, los cuales permiten al hacker enviar comandos y así utilizar la computadora para su beneficio.

ANEXOS

NOTA

El proyecto de titulación impreso presenta un ejemplo por cada herramienta de escaneo utilizada. Los resultados completos del escaneo constan en el dispositivo magnético.

RESUMEN DE CARACTERÍSTICAS DE HARDWARE LEVANTADO CON OcsInventory A1-1

Nro.	DIRECCIÓN IP	COMPUTADOR	DOMINIO USUARIO	SISTEMA OPERATIVO	SERVICE PACK	RAM(MB)	CPU(MHZ)
1	192.168.101.18	JFINANCIERA	JFINANCIERA	Microsoft Windows XP Professional	Service Pack 2	512	3400
2	192.168.101.26	SOCIALES	SOCIALES	Microsoft Windows XP Professional	Service Pack 2	2048	2982
3	192.168.101.41	ADMINISTRATIVO	ADMINISTRATIVO	Microsoft Windows XP Professional	Service Pack 2	512	2394
4	192.168.101.53	TESORERIA	TESORERIA	Microsoft Windows XP Professional	Service Pack 2	512	2992
5	192.168.101.68	ACADEMICO	ACADEMICO	Microsoft Windows XP Professional	Service Pack 2	512	3400
6	192.168.101.71	SECRETARIA2	SECRETARIA2	Microsoft Windows XP Professional	Service Pack 2	2048	2982
7	192.168.101.99	JEFEACADEMICO	JEFEACADEMICO	Microsoft Windows XP Professional	Service Pack 2	512	3400
8	192.168.101.107	JADMINISTRATIVO	JADMINISTRATIVO	Microsoft Windows XP Professional	Service Pack 2	256	3066
9	192.168.101.108	SECRETARIA1	SECRETARIA1	Microsoft Windows XP Professional	Service Pack 2	2048	2982
10	192.168.101.117	ACONTABILIDAD	ACONTABILIDAD	Microsoft Windows XP Professional	Service Pack 2	512	3411
11	192.168.101.131	COMIL-A9B34E83A	COMIL-A9B34E83A	Microsoft Windows XP Professional	Service Pack 2	2048	2982
12	192.168.101.139	COMIL10-4DC69DC	COMIL10-4DC69DC	Microsoft Windows XP Professional	Service Pack 3	1024	2666
13	192.168.101.175	SECREACAD	SECREACAD	Microsoft Windows XP Professional	Service Pack 2	512	3400
14	192.168.101.183	SECRETARIA3	SECRETARIA3	Microsoft Windows XP Professional	Service Pack 3	2048	2982
15	192.168.101.192	INVESTIGACION	INVESTIGACION	Microsoft Windows XP Professional	Service Pack 2	256	2407
16	192.168.101.197	ABOGADO	ABOGADO	Microsoft Windows XP Professional	Service Pack 2	1024	2666
17	192.168.101.201	COLECTURIA	COLECTURIA	Microsoft Windows XP Professional	Service Pack 2	2048	2982
18	192.168.101.215	PRESUPUESTO	PRESUPUESTO	Microsoft Windows XP Professional	Service Pack 2	512	3400
19	192.168.101.226	CONTABILIDADE	CONTABILIDADE	Microsoft Windows XP Professional	Service Pack 3	512	3400
20	192.168.101.231	COMUNICACIÓN	COMUNICACIÓN	Microsoft Windows XP Professional	Service Pack 2	512	3400
21	192.168.101.232	LENGUAJE	LENGUAJE	Microsoft Windows XP Professional	Service Pack 2	2048	2982
22	192.168.101.233	COMIL-3516185C2	COMIL-3516185C2	Microsoft Windows XP Professional	Service Pack 2	2048	2982
23	192.168.101.235	AREACOMERCIO	AREACOMERCIO	Microsoft Windows XP Professional	Service Pack 2	2048	2982
24	192.168.101.236	INGLES	INGLES,INGLES	Microsoft Windows XP Professional	Service Pack 2	2048	2982
25	192.168.101.237	ACIENCIASNAT	ACIENCIASNAT	Microsoft Windows XP Professional	Service Pack 2	2048	2982
26	192.168.101.238	CONTABILIDAD	CONTABILIDAD	Microsoft Windows XP Professional	Service Pack 2	2048	2982
27	192.168.101.243	COMIL10-341EFF6	COMIL10-341EFF6	Microsoft Windows XP Professional	Service Pack 2	512	3400

Nro.	DIRECCIÓN IP	WINPRODID	WINPRODKEY	ÚLTIMO INVENTARIO	NOMBRE USUARIO	SWAP
1	192.168.101.18	55274-640-0421043-23903	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	08/02/10 09:24	J Financiera	1228
2	192.168.101.26	76460-640-0421043-23400	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	29/01/10 06:57	Sociales Mat	3931
3	192.168.101.41	55274-640-4350801-23462	B3P7V-Q2WTH-CRK4R-YHJRF-39H4M	15/10/09 10:10	Administrador	2461
4	192.168.101.53	55274-640-0421043-23562	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	08/02/10 13:28	Maribel	1158
5	192.168.101.68	76460-640-0421043-23603	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	03/02/10 18:25	Académico	1228
6	192.168.101.71	55274-640-0421043-23740	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 10:38	Secretaria 2	3931
7	192.168.101.99	55274-640-0421043-23428	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 07:37	Academico	1228
8	192.168.101.107	55274-640-0421043-23792	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	29/01/10 08:54	Administrativo	466
9	192.168.101.108	55274-640-0421043-23809	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	20/01/10 07:01	Secretaria3	3931
10	192.168.101.117	55274-640-0421043-23807	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	08/02/10 14:33	Aux_Contabilidad	1228
11	192.168.101.131	76460-640-0421043-23256	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	08/02/10 15:14	Matematica Vesp	3931
12	192.168.101.139	55274-640-0421043-23614	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	03/02/10 10:20	Centro Informatica	2392
13	192.168.101.175	55274-640-0421043-23478	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 15:35	Usuario	1227
14	192.168.101.183	55274-640-0421043-23473	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	08/02/10 08:36	Secretaria3	3931
15	192.168.101.192	55274-640-0421043-23215	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 13:45	Anabela	618
16	192.168.101.197	55274-640-0421043-23171	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	15/10/09 08:41	Abogado	2392
17	192.168.101.201	55274-640-0421043-23073	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 13:10	Recaudacion	3931
18	192.168.101.215	55274-640-0421043-23240	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	07/01/10 13:24	Presupuesto	1228
19	192.168.101.226	76460-640-0421043-23420	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	08/02/10 15:19	COMIL	1228
20	192.168.101.231	76460-640-0421043-23145	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 16:10	Comunicacion S	1228
21	192.168.101.232	76460-640-0421043-23375	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	09/02/10 07:29	Lenguaje Mat	3931
22	192.168.101.233	76460-640-0421043-23314	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	09/02/10 09:08	COMIL	3931
23	192.168.101.235	76460-640-0421043-23423	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	09/02/10 09:13	Comercio	3931
24	192.168.101.236	76460-640-0421043-23156	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 07:58	Ingles Matutina	3931
25	192.168.101.237	76460-640-0421043-23762	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	13/01/10 08:32	C Naturales Mat	3931
26	192.168.101.238	76460-640-0421043-23681	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	08/02/10 15:02	Contabilidad Vesp	3931
27	192.168.101.243	55274-640-0421043-23909	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	09/02/10 07:02	Secc Personal	1228

Nro.	DIRECCIÓN IP	DESCRIPCIÓN	TIPO DE CPU	VERSIÓN BIOS
1	192.168.101.18		Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
2	192.168.101.26	Areas C Sociales	Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
3	192.168.101.41	Gonzalo Gallo	Intel(R) Pentium(R) 4 CPU 2.40GHz	BF86510A.86A.0061.P17.0404211558
4	192.168.101.53	Maribel Mejia	Intel(R) Pentium(R) 4 CPU 3.40GHz	BF86510A.86A.0061.P17.0404211558
5	192.168.101.68	SUBP GARRIDO JORGE	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
6	192.168.101.71	Margarita Stacey	Procesador Intel Pentium III Xeon	ECG3510M.86A.0106.2008.0730.1746
7	192.168.101.99		Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
8	192.168.101.107	CAP. GALARRAGA	Mobile Intel(R) Pentium(R) 4 CPU 3.06GHz	PTLTD - 6040000
9	192.168.101.108	NORA YEPEZ	Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
10	192.168.101.117	Microsoft Windows XP P.	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
11	192.168.101.131		Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
12	192.168.101.139	Oscarin	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0216.2007.0502.1916
13	192.168.101.175	SRA ELVIRA SANCHEZ	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
14	192.168.101.183		Procesador Intel Pentium III Xeon	ECG3510M.86A.0106.2008.0730.1746
15	192.168.101.192	Srta. Anabela	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634
16	192.168.101.197	SECRETARIA GENERAL	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519
17	192.168.101.201		Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
18	192.168.101.215	Margarita Benitez	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
19	192.168.101.226	Elizabeth T	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
20	192.168.101.231	Comunicacion Social	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
21	192.168.101.232	Area Lenguaje	Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
22	192.168.101.233	Area Computacion	Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
23	192.168.101.235		Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
24	192.168.101.236	Area Ingles	Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
25	192.168.101.237	Ciencias Naturales	Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
26	192.168.101.238	Area Contabilidad	Procesador Intel Pentium III Xeon	ECG3510M.86A.0084.2008.0523.1528
27	192.168.101.243		Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108

Nro.	DIRECCIÓN IP	FABR. DEL BIOS	BDATE	DOMINIO	VERSIÓN SO	PROPIETARIO	MODEMS	DISKETERA	DISCO
1	192.168.101.18	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	COMIL10	0	1	70GB
2	192.168.101.26	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL10	0	0	230GB
3	192.168.101.41	Intel Corp.	04/21/2004	DOMAIN	5.1.2600	WinuE	2	1	70GB
4	192.168.101.53	Intel Corp.	04/21/2004	DOMAIN	5.1.2600	COMIL10	0	1	70GB
5	192.168.101.68	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	Académico	0	1	70GB
6	192.168.101.71	Intel Corp.	07/30/2008	DOMAIN	5.1.2600	COMIL10	0	0	230GB
7	192.168.101.99	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	COMIL10	0	1	70GB
8	192.168.101.107	TOSHIBA		DOMAIN	5.1.2600	COMIL10	1	0	55GB
9	192.168.101.108	Intel Corp.	05/23/2008	DOMAIN	5.1.2600	COMIL10	0	0	230GB
10	192.168.101.117	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	COMIL10	0	1	70GB
11	192.168.101.131	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL	0	0	230GB
12	192.168.101.139	Intel Corp.	05/02/2007	GRUPO_TRABAJO	5.1.2600	COMIL10	0	1	230GB
13	192.168.101.175	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	WinXp	1	1	70GB
14	192.168.101.183	Intel Corp.	07/30/2008	DOMAIN	5.1.2600	COMIL10	0	0	230GB
15	192.168.101.192	Intel Corp.	10/25/2002	DOMAIN	5.1.2600	Comil-10	0	1	70GB
16	192.168.101.197	Intel Corp.	10/02/2007	DOMAIN	5.1.2600	COMIL10	0	1	230GB
17	192.168.101.201	Intel Corp.	05/23/2008	DOMAIN	5.1.2600	COMIL10	2	0	230GB
18	192.168.101.215	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	FINANCIERO	0	1	70GB
19	192.168.101.226	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	COMIL	2	1	140GB
20	192.168.101.231	Intel Corp.	04/29/2005	DOMAIN	5.1.2600	COMIL	0	1	70GB
21	192.168.101.232	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL10	0	1	230GB
22	192.168.101.233	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL	2	0	230GB
23	192.168.101.235	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL10	0	0	230GB
24	192.168.101.236	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL	0	0	230GB
25	192.168.101.237	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL	0	0	230GB
26	192.168.101.238	Intel Corp.	05/23/2008	AREAS	5.1.2600	COMIL10	0	0	230GB
27	192.168.101.243	Intel Corp.	04/29/2005	GRUPO_TRABAJO	5.1.2600	COMIL10	0	1	70GB

Nro.	DIRECCIÓN IP	CD-ROM	NIC	MAC ADDRESS
1	192.168.101.18	1	1	00:16:76:23:F6:3D
2	192.168.101.26	1	1	00:1C:C0:80:A3:AF
3	192.168.101.41	1	1	00:0F:3D:DE:5B:AE
4	192.168.101.53	1	1	00:0D:88:2E:EF:A5
5	192.168.101.68	1	1	00:13:20:82:1C:EC
6	192.168.101.71	1	1	00:1C:C0:AB:F0:4E
7	192.168.101.99	1	1	00:06:4F:4D:34:51
8	192.168.101.107	1	2	00:11:F5:2C:F9:A5 00:0F:B0:54:F2:3D
9	192.168.101.108	1	1	00:1C:C0:80:08:F3
10	192.168.101.117	1	1	00:16:76:34:E5:A2
11	192.168.101.131	1	1	00:1C:C0:80:9D:AF
12	192.168.101.139	1	1	00:19:D1:F9:72:54
13	192.168.101.175	1	1	00:13:20:78:40:67
14	192.168.101.183	1	1	00:1C:C0:AB:F0:F6
15	192.168.101.192	1	1	00:08:A1:4A:0C:DF
16	192.168.101.197	1	1	00:1C:C0:1C:5F:2A
17	192.168.101.201	1	1	00:1C:C0:80:09:1F
18	192.168.101.215	1	1	00:13:20:6D:D9:84
19	192.168.101.226	1	1	00:11:11:79:85:11
20	192.168.101.231	1	1	00:13:20:6D:D9:AD
21	192.168.101.232	1	1	00:1C:C0:80:0A:16
22	192.168.101.233	1	1	00:1C:C0:80:A7:A6
23	192.168.101.235	1	1	00:1C:C0:80:A4:82
24	192.168.101.236	1	1	00:1C:C0:7F:DA:E5
25	192.168.101.237	1	1	00:1C:C0:7F:F0:21
26	192.168.101.238	1	1	00:1C:C0:80:0A:0A
27	192.168.101.243	1	2	00:13:20:6D:D9:AD 00:14:D1:58:70:AD

Nro.	DIRECCIÓN IP	COMPUTADOR	DOMINIO USUARIO	SISTEMA OPERATIVO	SERVICE PACK	RAM(MB)	CPU(MHZ)
1	192.168.102.101	LAB01PC01	LAB01PC01	Microsoft Windows XP Professional	Service Pack 2	512	3399
2	192.168.102.102	LAB01PC02	LAB01PC02	Microsoft Windows XP Professional	Service Pack 2	512	3400
3	192.168.102.103	LAB01PC03	LAB01PC03	Microsoft Windows XP Professional	Service Pack 2	512	3400
4	192.168.102.104	LAB01PC04	LAB01PC04	Microsoft Windows XP Professional	Service Pack 2	512	3400
5	192.168.102.105	LAB01PC05	LAB01PC05	Microsoft Windows XP Professional	Service Pack 2	512	3400
6	192.168.102.106	LAB01PC06	LAB01PC06	Microsoft Windows XP Professional	Service Pack 2	512	3400
7	192.168.102.107	LAB01PC07	LAB01PC07	Microsoft Windows XP Professional	Service Pack 2	512	3400
8	192.168.102.108	LAB01PC08	LAB01PC08	Microsoft Windows XP Professional	Service Pack 2	512	3400
9	192.168.102.109	LAB01PC09	LAB01PC09	Microsoft Windows XP Professional	Service Pack 2	512	3400
10	192.168.102.110	LAB01PC10	LAB01PC10	Microsoft Windows XP Professional	Service Pack 2	512	3400
11	192.168.102.111	LAB01PC11	LAB01PC11	Microsoft Windows XP Professional	Service Pack 2	512	3400
12	192.168.102.112	LAB01PC12	LAB01PC12	Microsoft Windows XP Professional	Service Pack 2	512	3400
13	192.168.102.113	MAQ13LAB01	MAQ13LAB01	Microsoft Windows XP Professional	Service Pack 2	512	3400
14	192.168.102.114	LAB01PC14	LAB01PC14	Microsoft Windows XP Professional	Service Pack 2	512	3400
15	192.168.102.115	MAQ15LAB01	MAQ15LAB01	Microsoft Windows XP Professional	Service Pack 2	512	3400
16	192.168.102.116	MAQ16LAB01	MAQ16LAB01	Microsoft Windows XP Professional	Service Pack 2	512	3400
17	192.168.102.117	LAB01MAQ17	LAB01MAQ17	Microsoft Windows XP Professional	Service Pack 2	512	3400
18	192.168.102.118	MAQ18LAB01	MAQ18LAB01	Microsoft Windows XP Professional	Service Pack 2	512	3400
19	192.168.102.121	MAQUINA01	MAQUINA01	Microsoft Windows XP Professional	Service Pack 2	256	2407
20	192.168.102.124	MAQUINA04	MAQUINA04	Microsoft Windows XP Professional	Service Pack 2	256	2407
21	192.168.102.125	MAQUINA05	MAQUINA05	Microsoft Windows XP Professional	Service Pack 2	256	2407
22	192.168.102.126	MAQUINA06	MAQUINA06	Microsoft Windows XP Professional	Service Pack 2	256	2407
23	192.168.102.127	MAQUINA07	MAQUINA07	Microsoft Windows XP Professional	Service Pack 2	256	2407
24	192.168.102.128	MAQUINA08	MAQUINA08	Microsoft Windows XP Professional	Service Pack 2	256	2407
25	192.168.102.133	MAQUINA13	MAQUINA13	Microsoft Windows XP Professional	Service Pack 2	256	2808

Nro.	DIRECCIÓN IP	WINPRODID	WINPRODKEY	ÚLTIMO INVENTARIO	NOMBRE USUARIO	SWAP
1	192.168.102.101	76460-640-0421043-23853	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 10:08	Primero Bachillerato	1247
2	192.168.102.102	76460-640-0421043-23148	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	12/02/10 11:20	Abdón Calderón	1226
3	192.168.102.103	76460-640-0421043-23600	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	31/01/10 12:20	Abdón Calderón	1228
4	192.168.102.104	76460-640-0421043-23529	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/02/10 10:13	Abdón Calderón	1228
5	192.168.102.105	76460-640-0421043-23148	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	12/02/10 10:49	Abdón Calderón	1228
6	192.168.102.106	76460-640-0421043-23690	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	10/02/10 17:37	Primero Bachillerato	1054
7	192.168.102.107	76460-640-0421043-23832	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	10/02/10 18:14	Primero Bachillerato	1228
8	192.168.102.108	76460-640-0421043-23550	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	12/02/10 08:18	Abdón Calderón	1228
9	192.168.102.109	76460-640-0421043-23226	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	10/02/10 18:27	Primero Bachillerato	1228
10	192.168.102.110	76460-640-0421043-23978	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	03/02/10 09:21	Primero Bachillerato	1228
11	192.168.102.111	76460-640-0421043-23223	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	10/02/10 18:14	Primero Bachillerato	1227
12	192.168.102.112	76460-640-0421043-23926	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	10/11/09 08:53	Segundo Bachillerato	1228
13	192.168.102.113	76460-640-0421043-23754	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	12/02/10 19:29	Abdón Calderón	1228
14	192.168.102.114	76460-640-0421043-23668	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	11/02/10 17:50	Primero Bachillerato	1228
15	192.168.102.115	76460-640-0421043-23890	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	11/02/10 17:52	Primero Bachillerato	1227
16	192.168.102.116	76460-640-0421043-23435	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	12/02/10 07:10	Tercero Bachillerato	1228
17	192.168.102.117	76460-640-0421043-23992	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	10/02/10 17:55	Primero Bachillerato	1227
18	192.168.102.118	55274-640-0421043-23454	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	12/02/10 08:37	Abdón Calderón	1228
19	192.168.102.121	55274-640-0421043-23690	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	23/09/09 08:10	Abdón Calderón	618
20	192.168.102.124	55274-640-0421043-23690	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	23/09/09 08:06	Abdón Calderón	618
21	192.168.102.125	55274-640-0421043-23690	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	23/09/09 08:03	Abdón Calderón	618
22	192.168.102.126	55274-640-0421043-23690	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	23/09/09 08:53	2do. Bachillerato	618
23	192.168.102.127	55274-640-0421043-23690	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	23/09/09 08:13	Abdón Calderón	618
24	192.168.102.128	55274-640-0421043-23045	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	29/09/09 11:46	3ro. Bachillerato	618
25	192.168.102.133	76460-640-0421043-23862	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	23/09/09 07:54	Abdón Calderón	618

Nro.	DIRECCIÓN IP	DESCRIPCIÓN	TIPO DE CPU	VERSIÓN BIOS
1	192.168.102.101	Maq01Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
2	192.168.102.102	Maq02Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
3	192.168.102.103	Maq03Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
4	192.168.102.104	Laboratorio01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
5	192.168.102.105	Laboratorio01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
6	192.168.102.106	lab01maq06	Intel(R) Pentium(R) 4 CPU 3.40GHz	GC11010N.86A.0311.2006.0420.1525
7	192.168.102.107	Maq07Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
8	192.168.102.108	Maq08Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
9	192.168.102.109	Maq09Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
10	192.168.102.110	Maq10Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
11	192.168.102.111	Maq11Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
12	192.168.102.112	Maq12Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
13	192.168.102.113	lab01PC13	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
14	192.168.102.114	Maq14Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
15	192.168.102.115	lab01pc15	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
16	192.168.102.116	PC16Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
17	192.168.102.117	Maq17Lab01	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
18	192.168.102.118	lab01pc18	Intel(R) Pentium(R) 4 CPU 3.40GHz	EV91510A.86A.0444.2005.0429.2108
19	192.168.102.121	Laboratorio02	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634
20	192.168.102.124	Laboratorio02	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634
21	192.168.102.125	Laboratorio02	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634
22	192.168.102.126	Laboratorio02	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634
23	192.168.102.127	Laboratorio02	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634
24	192.168.102.128	Laboratorio02	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634
25	192.168.102.133	Laboratorio02	Intel(R) Pentium(R) 4 CPU 2.40GHz	MV85010A.86A.0057.P20.0210251634

Nro.	DIRECCIÓN IP	FABRICANTE BIOS	BDATE	DOMINIO	VERSIÓN SO	PROPIETARIO	MODEMS	DISKETERA	DISCO
1	192.168.102.101	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
2	192.168.102.102	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
3	192.168.102.103	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
4	192.168.102.104	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
5	192.168.102.105	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
6	192.168.102.106	Award BIOS for Intel	04/20/2006	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
7	192.168.102.107	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
8	192.168.102.108	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
9	192.168.102.109	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
10	192.168.102.110	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
11	192.168.102.111	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
12	192.168.102.112	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
13	192.168.102.113	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
14	192.168.102.114	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
15	192.168.102.115	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
16	192.168.102.116	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
17	192.168.102.117	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
18	192.168.102.118	Intel Corp.	04/29/2005	LABORATORIOS	5.1.2600	Laboratorio Uno	1	1	40GB
19	192.168.102.121	Intel Corp.	10/25/2002	LABORATORIOS	5.1.2600	Comil-10	1	1	40GB
20	192.168.102.124	Intel Corp.	10/25/2002	LABORATORIOS	5.1.2600	Comil-10	1	1	40GB
21	192.168.102.125	Intel Corp.	10/25/2002	LABORATORIOS	5.1.2600	Comil-10	1	1	40GB
22	192.168.102.126	Intel Corp.	10/25/2002	LABORATORIOS	5.1.2600	Comil-10	1	1	40GB
23	192.168.102.127	Intel Corp.	10/25/2002	LABORATORIOS	5.1.2600	Comil-10	1	1	40GB
24	192.168.102.128	Intel Corp.	10/25/2002	LABORATORIOS	5.1.2600	Comil-10	1	1	40GB
25	192.168.102.133	Intel Corp.	10/25/2002	LABORATORIOS	5.1.2600	Laboratorio Dos	1	1	40GB

RESUMEN DE CARACTERÍSTICAS DE HARDWARE LEVANTADO CON OcsInventory

Nro.	DIRECCIÓN IP	COMPUTADOR	DOMINIO USUARIO	SISTEMA OPERATIVO	SERVICE PACK	RAM(MB)	CPU(MHZ)
1	192.168.103.2	EQUIPO1	EQUIPO1	Microsoft Windows XP Professional	Service Pack 2	997	2666
2	192.168.103.3	EQUIPO2	EQUIPO2	Microsoft Windows XP Professional	Service Pack 2	997	2666
3	192.168.103.4	EQUIPO3	EQUIPO3	Microsoft Windows XP Professional	Service Pack 2	997	2666
4	192.168.103.5	EQUIPO4	EQUIPO4	Microsoft Windows XP Professional	Service Pack 2	997	2666
5	192.168.103.6	EQUIPO5	EQUIPO5	Microsoft Windows XP Professional	Service Pack 2	997	2666
6	192.168.103.8	EQUIPO7	EQUIPO7	Microsoft Windows XP Professional	Service Pack 2	997	2666
7	192.168.103.9	EQUIPO8	EQUIPO8	Microsoft Windows XP Professional	Service Pack 2	997	2666
8	192.168.103.10	EQUIPO9	EQUIPO9	Microsoft Windows XP Professional	Service Pack 2	997	2666
9	192.168.103.11	EQUIPO6	EQUIPO6	Microsoft Windows XP Professional	Service Pack 2	997	2666

Nro.	DIRECCIÓN IP	WINPRODID	WINPRODKEY	ÚLTIMO INVENTARIO	NOMBRE USUARIO	SWAP
1	192.168.103.2	76460-640-0421043-23396	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/05/2010 10:37	Estudiante	2393
2	192.168.103.3	76460-640-0421043-23371	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/05/2010 16:15	Docente	2393
3	192.168.103.4	55274-640-0421043-23876	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/05/2010 10:35	Docente	2393
4	192.168.103.5	55274-640-0421043-23137	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	04/05/2010 18:39	Estudiante	2393
5	192.168.103.6	76460-640-0421043-23371	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/05/2010 15:40	Estudiante	2393
6	192.168.103.8	76460-640-0421043-23931	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	09/12/2009 11:24	Estudiante	2393
7	192.168.103.9	55274-640-0421043-23337	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/05/2010 16:19	Estudiante	2393
8	192.168.103.10	76460-640-0421043-23879	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/05/2010 18:16	Estudiante	2393
9	192.168.103.11	76460-640-0421043-23076	BWBTJ-HQR6K-D4J9H-WH9R7-628XM	05/05/2010 18:59	Comil10	2393

Nro.	DIRECCIÓN IP	TIPO DE CPU	VERSIÓN BIOS	FABRICANTE BIOS	BDATE
1	192.168.103.2	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007
2	192.168.103.3	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007
3	192.168.103.4	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0216.2007.0502.1916	Intel Corp.	05/02/2007
4	192.168.103.5	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007
5	192.168.103.6	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007
6	192.168.103.8	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007
7	192.168.103.9	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007
8	192.168.103.10	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007
9	192.168.103.11	Intel(R) Core(TM)2 Duo CPU E6750 @ 2.66GHz	DPP3510J.86A.0293.2007.1002.1519	Intel Corp.	10/02/2007

Nro.	DIRECCIÓN IP	DOMINIO	VERSIÓN SO	PROPIETARIO	MODEMS	DISKETERA	DISCO	MAC ADDRESS
1	192.168.103.2	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:5F:D4
2	192.168.103.3	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:5F:E2
3	192.168.103.4	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:19:D1:F9:73:9E
4	192.168.103.5	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:5F:B3
5	192.168.103.6	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:6E:40
6	192.168.103.8	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:5F:B7
7	192.168.103.9	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:6D:F0
8	192.168.103.10	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:76:A0
9	192.168.103.11	BIBLIOTECA	5.1.2600	COMIL10	1	0	230GB	00:1C:C0:1C:5F:FC

NOMBRE	ÁREA	CANTIDAD DE EQUIPOS
Adobe Acrobat 5.0	Administrativa	4
Adobe AIR	Administrativa	2
Adobe Anchor Service CS3	Administrativa	2
Adobe Asset Services CS3	Administrativa	2
Adobe Bridge CS3	Administrativa	2
Adobe Bridge Start Meeting	Administrativa	2
Adobe Camera Raw 4.0	Administrativa	2
Adobe Cmaps	Administrativa	2
Adobe Color - Photoshop Specific	Administrativa	1
Adobe Color Common Settings	Administrativa	2
Adobe Color EU Recommended Settings	Administrativa	2
Adobe Color JA Extra Settings	Administrativa	2
Adobe Default Language CS3	Administrativa	2
Adobe Device Central CS3	Administrativa	2
Adobe ExtendScript Toolkit 2	Administrativa	2
Adobe Flash Player 10 ActiveX	Administrativa	24
Adobe Flash Player 10 Plugin	Administrativa	7
Adobe Flash Player 9 ActiveX	Administrativa	1
Adobe Flash Player ActiveX	Administrativa	1
Adobe Fonts All	Administrativa	2
Adobe Help Viewer CS3	Administrativa	2
Adobe Illustrator CS3	Administrativa	2
Adobe Linguistics CS3	Administrativa	2
Adobe Media Player	Administrativa	1
Adobe PDF Library Files	Administrativa	2
Adobe Photoshop CS3	Administrativa	2
Adobe Reader 7.0.8 – Español	Administrativa	2
Adobe Reader 9 – Español	Administrativa	20
Adobe Reader 9.1 – Español	Administrativa	1
Adobe Setup	Administrativa	2
Adobe Shockwave Player	Administrativa	1
Adobe Stock Photos CS3	Administrativa	2
Adobe Type Support	Administrativa	2
Adobe Update Manager CS3	Administrativa	2
Adobe Version Cue CS3 Client	Administrativa	2
Adobe WinSoft Linguistics Plugin	Administrativa	2
Adobe XMP Panels CS3	Administrativa	2
Adobe Photoshop Album Starter Edition 3.0	Administrativa	1
Apple Software Update	Administrativa	1
Ares 2.1.1	Administrativa	2
Asistente Administrativo MILENIO 3 (Pers. Naturales)	Administrativa	1
Asistente para la publicación en Web 1.53 de Microsoft	Administrativa	1

Ask Toolbar	Administrativa	1
Atheros Client Utility	Administrativa	1
Atheros Wireless LAN MiniPCI card Driver	Administrativa	1
ATI - Utilidad de desinstalación de software	Administrativa	1
ATI Control Panel	Administrativa	1
ATI Display Driver	Administrativa	1
AutoCAD 2007 - English	Administrativa	1
Autodesk DWF Viewer	Administrativa	1
Avanquest update	Administrativa	1
AVG 8.0	Administrativa	2
AVG 8.5	Administrativa	2
AVG Free 8.5	Administrativa	1
Barra de herramientas ALOT	Administrativa	1
Barra de Herramientas MSN	Administrativa	1
Barra Yahoo!	Administrativa	2
Biblioteca Nueva Praxis	Administrativa	1
CA AllFusion Process Modeler	Administrativa	5
Canon PIXMA iP1500	Administrativa	1
CCleaner (remove only)	Administrativa	3
Choice Guard	Administrativa	1
CinemaForge	Administrativa	1
Color Planner 2.5	Administrativa	1
ColorClick	Administrativa	1
Compresor WinRAR	Administrativa	20
Datacard e-Guide - SP Series	Administrativa	1
Datacard ID Works Corporativo	Administrativa	1
Dealio Toolbar v4.0.2	Administrativa	1
Desinstalación del escaner Xerox Phaser 8510_8560	Administrativa	2
Detector de suministros de Windows Live Toolbar (Windows Live Toolbar)	Administrativa	1
Digital Photo Navigator 1.5	Administrativa	1
DIMM	Administrativa	1
DIMM Formularios	Administrativa	3
Don"t Touch My Computer 2 Screen Saber	Administrativa	1
DVD Solution	Administrativa	2
DVD Suite	Administrativa	17
DVD-RAM Driver	Administrativa	1
E.M.I.A.G.	Administrativa	1
E.M.I.A.G. (C:/Archivos de programa/Proyecto1/)	Administrativa	1
E.M.I.A.G. (C:/Archivos de programa/Proyecto1/) #3	Administrativa	1
E.M.I.A.G. (C:/Archivos de programa/Proyecto1/) #4	Administrativa	1
E.M.I.A.G. (C:/Archivos de programa/Proyecto1/) #5	Administrativa	1
EasyRecovery Professional	Administrativa	1
Enciclopedia de las Vitaminas	Administrativa	1

Enciclopedia Multimedia	Administrativa	1
Escaneado por Red	Administrativa	2
Extensión de MSN de Windows Live Toolbar (Windows Live Toolbar)	Administrativa	1
FEYDAM	Administrativa	1
Fingerprint Attendance System	Administrativa	1
Firebird SQL Server - MAGIX Edition	Administrativa	1
First Step Guide	Administrativa	1
FLV Player 2.0 (build 25)	Administrativa	1
Galería fotográfica de Windows Live	Administrativa	2
Garfield Midnight Snack Screen Saber	Administrativa	1
Generador de Horarios 2008	Administrativa	1
GFI LANguard 9.0	Administrativa	2
GFI LANguard 9.0 ReportPack	Administrativa	1
GFI ReportCenter Framework	Administrativa	1
Google Chrome	Administrativa	1
Google Earth	Administrativa	1
Google Toolbar for Internet Explorer	Administrativa	3
Google Update Helper	Administrativa	2
Herramienta de carga de Windows Live	Administrativa	2
High Definition Audio Driver Package - KB835221	Administrativa	9
High Definition Audio Driver Package - KB888111	Administrativa	14
Hotfix for Windows XP (KB915865)	Administrativa	3
Hotfix for Windows XP (KB926239)	Administrativa	4
HP Deskjet 6900 series (esn)	Administrativa	1
HP Extended Capabilities 6.0	Administrativa	3
HP Imaging Device Functions 6.0	Administrativa	1
hp LaserJet 1160/1320 series	Administrativa	3
HP LaserJet P2015 Series 1.0	Administrativa	3
HP Photosmart Essential	Administrativa	1
HP Software Update	Administrativa	6
HP Solution Center and Imaging Support Tools 6.0	Administrativa	1
Image Resizer Powertoy for Windows XP	Administrativa	1
ImageMixer VCD2	Administrativa	1
IMBooster	Administrativa	1
InCD	Administrativa	1
IncrediMail	Administrativa	3
IncrediMail 2.0	Administrativa	1
Intel(R) Extreme Graphics Driver	Administrativa	2
Intel(R) Graphics Media Accelerator Driver	Administrativa	23
Intel(R) Management Engine Interface	Administrativa	2
Intel(R) PRO Network Adapters and Drivers	Administrativa	8
Intel(R) PRO Network Connections 12.1.12.0	Administrativa	14
IZArc 4.1	Administrativa	1

JARDIN BOTANICO DE QUITO	Administrativa	1
Java DB 10.4.2.1	Administrativa	1
Java(TM) 6 Update 17	Administrativa	1
Java(TM) 6 Update 18	Administrativa	1
Java(TM) 6 Update 7	Administrativa	1
Java(TM) SE Development Kit 6 Update 17	Administrativa	1
Java(TM) SE Runtime Environment 6	Administrativa	1
Junk Mail filter update	Administrativa	3
KPD	Administrativa	1
L&H Power Translator Pro 7.0	Administrativa	1
L&H TTS3000 Español	Administrativa	1
LaserJet 1020 series	Administrativa	1
LG ODD Auto Firmware Update	Administrativa	13
LimeWire 4.18.8	Administrativa	1
Lime_Line Toolbar	Administrativa	1
Macromedia Dreamweaver 8	Administrativa	1
Macromedia Extension Manager	Administrativa	1
Macromedia Fireworks 8	Administrativa	2
Macromedia Flash 8	Administrativa	1
Macromedia Flash 8 Video Encoder	Administrativa	1
Macromedia Flash Player	Administrativa	1
Macromedia Flash Player 8	Administrativa	1
Macromedia Shockwave Player	Administrativa	1
Magentic	Administrativa	1
MAGIX Music Maker 2008 Producer Edition Trial 13.0.3.1 (ES)	Administrativa	1
MAGIX Screenshare 4.3.6.1987 (ES)	Administrativa	1
McAfee Security Scan	Administrativa	1
Media Player Codec Pack 3.9.2	Administrativa	1
Microsoft .NET Framework 1.1	Administrativa	7
Microsoft .NET Framework 1.1 Hotfix (KB886903)	Administrativa	1
Microsoft .NET Framework 1.1 Spanish Language Pack	Administrativa	3
Microsoft .NET Framework 2.0	Administrativa	7
Microsoft .NET Framework 2.0 with Security Updates	Administrativa	1
Microsoft Choice Guard	Administrativa	2
Microsoft Compression Client Pack 1.0 for Windows XP	Administrativa	4
Microsoft Encarta 2006 Biblioteca Premium	Administrativa	1
Microsoft Encarta 2007 Biblioteca Premium	Administrativa	1
Microsoft Encarta 2009 Biblioteca Premium	Administrativa	1
Microsoft Internationalized Domain Names Mitigation APIs	Administrativa	3
Microsoft Kernel-Mode Driver Framework Feature Pack 1.5	Administrativa	1
Microsoft Kernel-Mode Driver Framework Feature Pack 1.7	Administrativa	1
Microsoft National Language Support Downlevel APIs	Administrativa	3
Microsoft Office Access MUI (Spanish) 2007	Administrativa	17
Microsoft Office Enterprise 2007	Administrativa	34

Microsoft Office Excel MUI (Spanish) 2007	Administrativa	17
Microsoft Office FrontPage 2003	Administrativa	1
Microsoft Office Groove MUI (Spanish) 2007	Administrativa	17
Microsoft Office InfoPath MUI (Spanish) 2007 (Beta)	Administrativa	17
Microsoft Office Live Add-in 1.3	Administrativa	2
Microsoft Office OneNote MUI (Spanish) 2007	Administrativa	17
Microsoft Office Outlook Connector	Administrativa	1
Microsoft Office Outlook MUI (Spanish) 2007	Administrativa	17
Microsoft Office PowerPoint MUI (Spanish) 2007	Administrativa	17
Microsoft Office Professional Edition 2003	Administrativa	12
Microsoft Office Project MUI (English) 2007	Administrativa	1
Microsoft Office Project Professional 2003	Administrativa	1
Microsoft Office Project Professional 2007	Administrativa	2
Microsoft Office Proof (Basque) 2007	Administrativa	17
Microsoft Office Proof (Catalan) 2007	Administrativa	17
Microsoft Office Proof (English) 2007	Administrativa	17
Microsoft Office Proof (French) 2007	Administrativa	17
Microsoft Office Proof (Galician) 2007	Administrativa	17
Microsoft Office Proof (Portuguese (Brazil)) 2007	Administrativa	17
Microsoft Office Proof (Spanish) 2007	Administrativa	17
Microsoft Office Proofing (English) 2007	Administrativa	1
Microsoft Office Proofing (Spanish) 2007	Administrativa	17
Microsoft Office Publisher MUI (Spanish) 2007	Administrativa	17
Microsoft Office Shared MUI (English) 2007	Administrativa	1
Microsoft Office Shared MUI (Spanish) 2007	Administrativa	17
Microsoft Office Shared Setup Metadata MUI (English) 2007	Administrativa	1
Microsoft Office Visio Professional 2003	Administrativa	1
Microsoft Office Word MUI (Spanish) 2007	Administrativa	17
Microsoft Search Enhancement Pack	Administrativa	3
Microsoft Silverlight	Administrativa	2
Microsoft SQL Server 2005 Compact Edition [ENU]	Administrativa	2
Microsoft Sync Framework Runtime Native v1.0 (x86)	Administrativa	2
Microsoft Sync Framework Services Native v1.0 (x86)	Administrativa	2
Microsoft User-Mode Driver Framework Feature Pack 1.0	Administrativa	4
Microsoft User-Mode Driver Framework Feature Pack 1.5	Administrativa	1
Microsoft Visual C++ 2005 Redistributable	Administrativa	16
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17	Administrativa	1
Microsoft Visual Studio 6.0 Edición empresarial (Español)	Administrativa	1
Microsoft VM for Java	Administrativa	1
Microsoft Windows XP Professional	Administrativa	27
Microsoft Winter Fun Pack 2004 for Windows XP	Administrativa	1
Motorola Driver Installation 3.4.0	Administrativa	1
Motorola Phone Tools	Administrativa	1
Mozilla Firefox (3.0.16)	Administrativa	1

Mozilla Firefox (3.0.17)	Administrativa	1
Mozilla Firefox (3.0.3)	Administrativa	2
Mozilla Firefox (3.5.3)	Administrativa	1
Mozilla Firefox (3.5.7)	Administrativa	1
MSN	Administrativa	1
MSN Messenger 7.0	Administrativa	1
MSVC80_x86	Administrativa	1
MSVCRT,3,	Administrativa	3
MSXML 4.0 SP2 Parser and SDK	Administrativa	14
MSXML 6.0 Parser	Administrativa	3
MSXML 6.0 Parser (KB925673)	Administrativa	1
Multimedia Launcher	Administrativa	2
MUSICMATCH Jukebox	Administrativa	1
My Web Search (Popular Screensavers)	Administrativa	1
Natural Health	Administrativa	1
Natural Health (C:/Archivos de programa/Monografia/)	Administrativa	1
Nero 7 Essentials	Administrativa	17
Nero 7.5.9.0	Administrativa	4
Nero 9	Administrativa	1
Nero OEM	Administrativa	1
Nero Suite	Administrativa	1
neroxml	Administrativa	17
Nessus	Administrativa	1
NetBeans IDE 6.7.1	Administrativa	1
Nmap 5.00	Administrativa	1
NOD32 antivirus system	Administrativa	23
NOD32 FiX v2.1	Administrativa	2
Nokia Connectivity Cable Driver	Administrativa	2
Nokia Lifeblog 2.5	Administrativa	1
Nokia NSeries Application Installer	Administrativa	1
Nokia NSeries Content Copier	Administrativa	1
Nokia NSeries Multimedia Player	Administrativa	1
Nokia NSeries Music Manager	Administrativa	1
Nokia NSeries One Touch Access	Administrativa	1
Nokia NSeries System Utilities	Administrativa	1
Nokia PC Suite	Administrativa	3
Nokia Software Launcher	Administrativa	1
OCS Inventory Agent 4.0.5.4	Administrativa	27
OCS Inventory NG	Administrativa	1
OpenOffice.org Installer 1.0	Administrativa	1
OrderReminder HP LaserJet 1020	Administrativa	1
Pack Vista Inspirat 1.1	Administrativa	1
Paquete de compatibilidad para 2007 Office system	Administrativa	1

Paquete de controladores de Windows - Nokia Modem (05/22/2008 3.8)	Administrativa	1
Paquete de controladores de Windows - Nokia Modem (05/22/2008 7.00.0.1)	Administrativa	1
Paquete de controladores de Windows - Nokia pccsmcfd (10/12/2007 6.85.4.0)	Administrativa	1
Paquete de idioma de Microsoft .NET Framework 2.0 - ESN	Administrativa	2
PC Connectivity Solution	Administrativa	2
PDF Settings	Administrativa	2
PDF-to-Word 3.1 Demo	Administrativa	1
Peer2Peer Toolbar	Administrativa	1
Photo Crop Editor 1.15	Administrativa	1
Picasa 3	Administrativa	4
Picture Package	Administrativa	1
Pixia	Administrativa	4
Playrix Gameplayer	Administrativa	1
PowerCinema NE for Everio	Administrativa	1
PowerDirector Express	Administrativa	1
PowerDVD	Administrativa	23
PowerProducer	Administrativa	18
Protección de Yahoo! Búsquedas	Administrativa	1
QuickTime	Administrativa	1
QuickTime Alternative 1.76	Administrativa	1
Readiris Pro 10	Administrativa	1
Real Alternative 1.51 Lite	Administrativa	1
RealPlayer	Administrativa	3
Realtek AC"97 Audio	Administrativa	3
Realtek Fast Ethernet Adapter Driver	Administrativa	1
Realtek High Definition Audio Driver	Administrativa	23
Reproductor de Windows Media 11	Administrativa	2
Samsung SCX-4200 Series	Administrativa	1
Search Settings v1.2.3	Administrativa	1
SearchTheWeb	Administrativa	1
Security Update para Microsoft .NET Framework 2.0 (KB917283)	Administrativa	1
Security Update para Microsoft .NET Framework 2.0 (KB922770)	Administrativa	1
Segoe UI	Administrativa	3
Sentinel System Driver 5.41.1 (32-bit)	Administrativa	1
shARES Toolbar	Administrativa	2
SierraAddressBook 3.0	Administrativa	1
SierraHome Print Artist 15.0	Administrativa	1
SiS 300/305	Administrativa	1
SiS305 V1.14a	Administrativa	1
SITAC	Administrativa	1
SmarThru 4	Administrativa	1

Software de impresora EPSON	Administrativa	9
Solucionario de Baldor	Administrativa	1
Sony Ericsson PC Suite	Administrativa	2
Sony USB Driver	Administrativa	1
Sopa de Letras 2.1	Administrativa	1
SoundMAX	Administrativa	1
Spider-Man 2	Administrativa	1
SweetIM for Messenger 2.7	Administrativa	1
SweetIM Toolbar for Internet Explorer 3.4	Administrativa	1
Sybase SQL Anywhere 5.0	Administrativa	19
TaskSwitchXP	Administrativa	1
teddy_bears_clock	Administrativa	1
TELECOMUNICACIONES	Administrativa	1
Test Drive 6	Administrativa	1
TEST PSICOTECNICOS	Administrativa	1
TEST PSICOTECNICOS (C:/Archivos de programa/Proyecto1/)	Administrativa	1
Text-To-Speech-Runtime	Administrativa	1
TOSHIBA Software Modem	Administrativa	1
Toshiba Tbiosdrv Driver	Administrativa	1
Tr@nslation Plus	Administrativa	1
transformers_cinecanal	Administrativa	1
Utilidad de activación/desactivación del panel t?til	Administrativa	1
Viajemos por la Amazonía	Administrativa	1
VLC media player 1.0.5	Administrativa	1
Webshots Desktop	Administrativa	1
Winamp AudioPlayer	Administrativa	1
Windows Driver Package - Nokia (WUDFRd) WPD (11/03/2006 6.82.26.2)	Administrativa	1
Windows Driver Package - Nokia Modem (11/03/2006 6.82.0.1)	Administrativa	1
Windows Imaging Component	Administrativa	3
Windows Installer 3.1 (KB893803)	Administrativa	5
Windows Internet Explorer 7	Administrativa	1
Windows Internet Explorer 8	Administrativa	1
Windows Live Asistente para el inicio de sesión	Administrativa	3
Windows Live Call	Administrativa	3
Windows Live Communications Platform	Administrativa	3
Windows Live Essentials	Administrativa	6
Windows Live Mail	Administrativa	3
Windows Live Messenger	Administrativa	4
Windows Live Protección Infantil	Administrativa	3
Windows Live Sync	Administrativa	2
Windows Live Toolbar	Administrativa	2
Windows Live Writer	Administrativa	2

Windows Media Format 11 runtime	Administrativa	8
Windows Media Format Runtime	Administrativa	15
Windows Media Player 11	Administrativa	2
Windows XP Service Pack 2	Administrativa	1
Windows XP Service Pack 3	Administrativa	3
WinPcap 4.1 beta5	Administrativa	1
WinZip	Administrativa	9
Wireshark 1.2.1	Administrativa	1
XAMPP 1.6.6a	Administrativa	1
Xerox Phaser 3200MFP	Administrativa	2
XMLinst	Administrativa	9
XPize 4.6 Lite BETA 1	Administrativa	1
Yahoo! Install Manager	Administrativa	1
Yahoo! Software Update	Administrativa	1
Actualización para Windows XP (KB932823-v3)	Laboratorios	1
Adobe Download Manager	Laboratorios	1
Adobe Flash Player 10 ActiveX	Laboratorios	21
Adobe Flash Player 10 Plugin	Laboratorios	5
Adobe Reader 9 – Español	Laboratorios	18
Adobe Reader 9.1 – Español	Laboratorios	5
Asistente para la publicación en Web 1.53 de Microsoft	Laboratorios	25
ATI - Utilidad de desinstalación de software	Laboratorios	1
ATI Catalyst Control Center	Laboratorios	1
ATI Control Panel	Laboratorios	1
ATI Display Driver	Laboratorios	1
ATI HydraVision	Laboratorios	1
Barra Yahoo!	Laboratorios	1
Compresor WinRAR	Laboratorios	4
CorelDRAW Graphics Suite 12	Laboratorios	6
Counter-Strike 1.6	Laboratorios	1
CyberLink PowerDVD 8	Laboratorios	1
FLV Player	Laboratorios	1
Folder Marker v 1.4	Laboratorios	1
Google Toolbar for Internet Explorer	Laboratorios	2
Herramienta de carga de Windows Live	Laboratorios	1
High Definition Audio Driver Package – KB835221	Laboratorios	6
High Definition Audio Driver Package – KB888111	Laboratorios	11
InstallShield for Microsoft Visual C++ 6	Laboratorios	19
Intel Application Accelerator	Laboratorios	1
Intel(R) Graphics Media Accelerator Driver	Laboratorios	16
Intel(R) PRO Network Adapters and Drivers	Laboratorios	17
Interwrite Workspace	Laboratorios	1
Java(TM) 6 Update 17	Laboratorios	1
K-Lite Codec Pack 5.0.0 (Full)	Laboratorios	1

LimeWire 5.3.6	Laboratorios	1
Microsoft .NET Framework 1.1	Laboratorios	1
Microsoft Choice Guard	Laboratorios	1
Microsoft Office Access MUI (Spanish) 2007	Laboratorios	24
Microsoft Office Enterprise 2007	Laboratorios	46
Microsoft Office Excel MUI (Spanish) 2007	Laboratorios	24
Microsoft Office FrontPage 2003	Laboratorios	25
Microsoft Office Groove MUI (Spanish) 2007	Laboratorios	24
Microsoft Office InfoPath MUI (Spanish) 2007 (Beta)	Laboratorios	24
Microsoft Office OneNote MUI (Spanish) 2007	Laboratorios	24
Microsoft Office Outlook MUI (Spanish) 2007	Laboratorios	24
Microsoft Office PowerPoint MUI (Spanish) 2007	Laboratorios	24
Microsoft Office Professional Edition 2003	Laboratorios	2
Microsoft Office Project Professional 2003	Laboratorios	19
Microsoft Office Proof (Basque) 2007	Laboratorios	24
Microsoft Office Proof (Catalan) 2007	Laboratorios	24
Microsoft Office Proof (English) 2007	Laboratorios	24
Microsoft Office Proof (French) 2007	Laboratorios	24
Microsoft Office Proof (Galician) 2007	Laboratorios	24
Microsoft Office Proof (Portuguese (Brazil)) 2007	Laboratorios	24
Microsoft Office Proof (Spanish) 2007	Laboratorios	24
Microsoft Office Proofing (Spanish) 2007	Laboratorios	24
Microsoft Office Publisher MUI (Spanish) 2007	Laboratorios	24
Microsoft Office Shared MUI (Spanish) 2007	Laboratorios	24
Microsoft Office Visio Professional 2003	Laboratorios	24
Microsoft Office Word MUI (Spanish) 2007	Laboratorios	24
Microsoft Visual C++ 2005 Redistributable	Laboratorios	1
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.17	Laboratorios	2
Microsoft Visual Studio 6.0 Edición empresarial (Español)	Laboratorios	25
Microsoft VM for Java	Laboratorios	25
Microsoft Windows XP Professional	Laboratorios	25
Mozilla Firefox (3.6)	Laboratorios	1
MSDN Library - July 2000	Laboratorios	12
MSDN Library - Visual Studio 6.0a (Español)	Laboratorios	1
MSN	Laboratorios	2
MSVCRT	Laboratorios	1
MSXML4 Parser	Laboratorios	2
MySQL Connector/ODBC 3.51	Laboratorios	6
NeoBook 5.6.4a	Laboratorios	1
NOD32 antivirus system	Laboratorios	25
OCS Inventory Agent 4.0.5.4	Laboratorios	20
OCS Inventory NG	Laboratorios	1
P2P_Max_ES Toolbar	Laboratorios	1
PCI Audio Driver	Laboratorios	1

ANEXO 2

FOTOGRÁFICO DE LAS INSTALACIONES DE RED DE LA UNIDAD EDUCATIVA

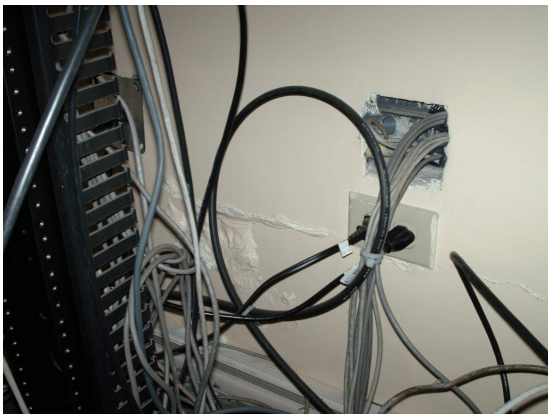
CENTRO DE INFORMÁTICA

a) Fácil acceso al Centro de Informática. La puerta permanece abierta o semi-abierta.

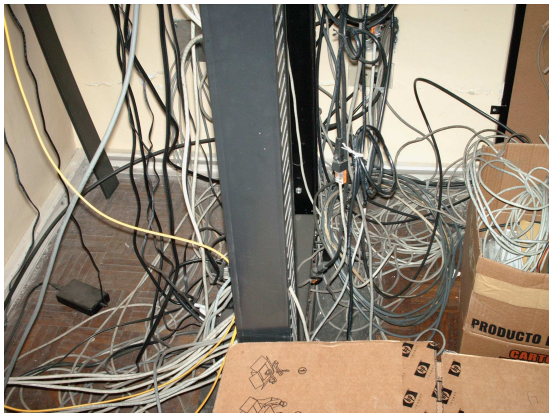
b) Fácil acceso al área de los servidores.

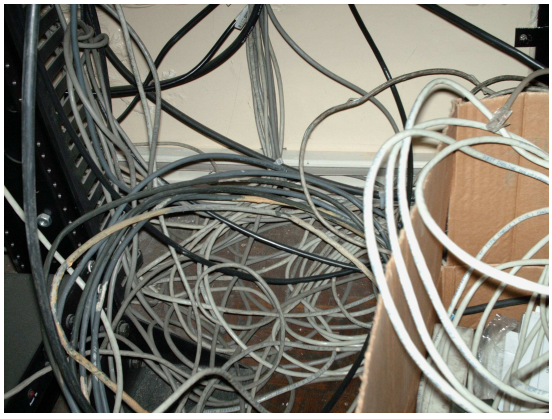
c) El cuarto de comunicaciones se encuentra en el mismo lugar que los servidores.

d) Los cables provenientes de los puntos de red no tienen ningún tipo de identificativo de origen.



e) Los cables forman una completa maraña en la parte inferior del patch panel.

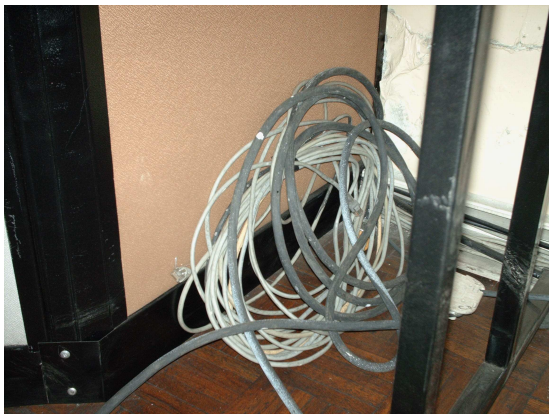


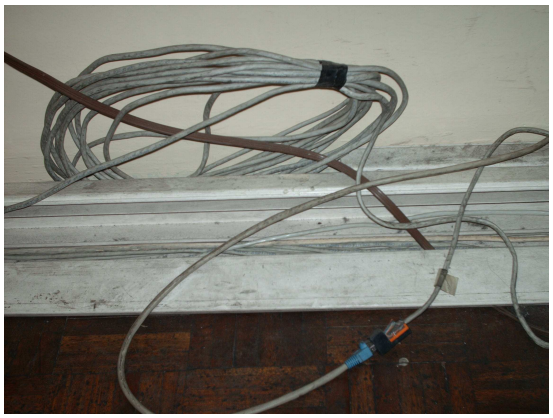


f) Dentro de la misma área funciona una especie de bodega de material defectuoso y en buen estado tal como (discos, fuentes de poder, cable UTP, etc.), el cual reposa en varias cajas colocadas junto al rack.

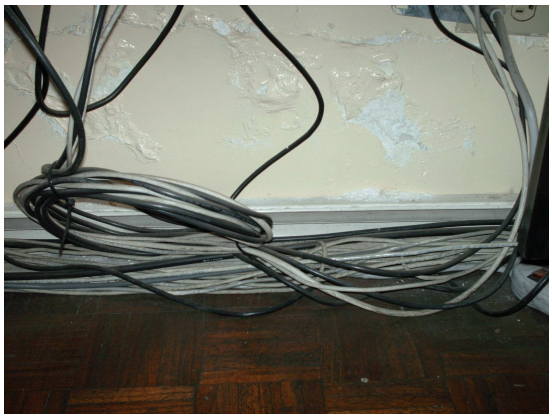
g) No existe conexión a tierra en el rack.

h) Los cables van fuera de la canaleta.





i) Las paredes muestran señales de humedad.



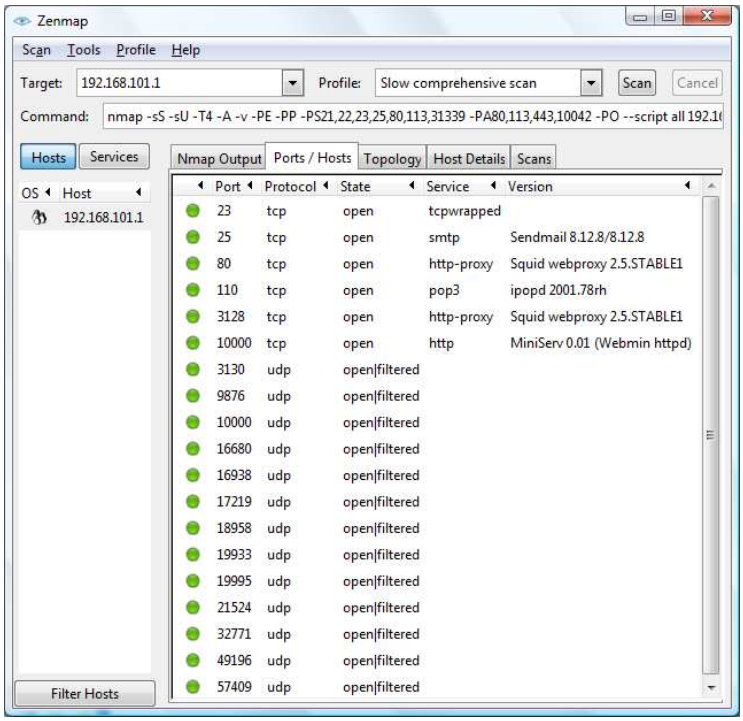
j) El monitor que registra el video de las cámaras de seguridad (estáticas) tiene instalado a su derecha un botellón de agua.

k) No existe sistema de ventilación ni de detección de incendios.

ANEXO 3

ESCANEO CON NMAP

a) Desde el interior de la red de la Unidad Educativa




```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-06-04 11:23 Hora estándar
romance

NSE: Loaded 80 scripts for scanning.
Initiating ARP Ping Scan at 11:23
Scanning 192.168.101.1 [1 port]
Completed ARP Ping Scan at 11:23, 0.03s elapsed (1 total hosts)

Initiating SYN Stealth Scan at 11:23
Scanning 192.168.101.1 [1000 ports]
Discovered open port 25/tcp on 192.168.101.1
Discovered open port 80/tcp on 192.168.101.1
Discovered open port 110/tcp on 192.168.101.1
Discovered open port 23/tcp on 192.168.101.1
Discovered open port 3128/tcp on 192.168.101.1
Discovered open port 10000/tcp on 192.168.101.1
Completed SYN Stealth Scan at 11:23, 1.49s elapsed (1000 total ports)

Initiating UDP Scan at 11:23
Scanning 192.168.101.1 [1000 ports]
Increasing send delay for 192.168.101.1 from 0 to 50 due to
max_successful_tryno increase to 5
Increasing send delay for 192.168.101.1 from 50 to 100 due to
max_successful_tryno increase to 6
Warning: 192.168.101.1 giving up on port because retransmission cap hit
(6).
Increasing send delay for 192.168.101.1 from 100 to 200 due to 11 out of
11 dropped probes since last increase.
```

```
Increasing send delay for 192.168.101.1 from 200 to 400 due to 11 out of
11 dropped probes since last increase.
UDP Scan Timing: About 6.06% done; ETC: 11:32 (0:08:01 remaining)
Increasing send delay for 192.168.101.1 from 400 to 800 due to 11 out of
11 dropped probes since last increase.
UDP Scan Timing: About 9.21% done; ETC: 11:34 (0:10:01 remaining)
UDP Scan Timing: About 12.29% done; ETC: 11:35 (0:10:50 remaining)
UDP Scan Timing: About 30.77% done; ETC: 11:38 (0:10:10 remaining)
UDP Scan Timing: About 38.10% done; ETC: 11:38 (0:09:22 remaining)
UDP Scan Timing: About 43.49% done; ETC: 11:38 (0:08:36 remaining)
UDP Scan Timing: About 49.00% done; ETC: 11:38 (0:07:49 remaining)
UDP Scan Timing: About 55.01% done; ETC: 11:39 (0:07:00 remaining)
UDP Scan Timing: About 60.17% done; ETC: 11:39 (0:06:12 remaining)
UDP Scan Timing: About 65.49% done; ETC: 11:39 (0:05:23 remaining)
UDP Scan Timing: About 70.81% done; ETC: 11:39 (0:04:35 remaining)
UDP Scan Timing: About 76.11% done; ETC: 11:39 (0:03:45 remaining)
UDP Scan Timing: About 81.43% done; ETC: 11:39 (0:02:55 remaining)
UDP Scan Timing: About 86.54% done; ETC: 11:39 (0:02:08 remaining)
UDP Scan Timing: About 91.76% done; ETC: 11:39 (0:01:18 remaining)
UDP Scan Timing: About 96.80% done; ETC: 11:39 (0:00:30 remaining)
Completed UDP Scan at 11:40, 987.00s elapsed (1000 total ports)

Initiating Service scan at 11:40
Scanning 19 services on 192.168.101.1
Service scan Timing: About 36.84% done; ETC: 11:42 (0:01:26 remaining)
Completed Service scan at 11:41, 77.53s elapsed (19 services on 1 host)
Initiating OS detection (try #1) against 192.168.101.1
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is
disabled. Try using --system-dns or specify valid servers with --dns-
servers

NSE: Script scanning 192.168.101.1.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 11:41
NSE Timing: About 97.62% done; ETC: 12:02 (0:00:30 remaining)
NSE Timing: About 97.62% done; ETC: 12:02 (0:00:31 remaining)
NSE Timing: About 97.62% done; ETC: 12:03 (0:00:32 remaining)
NSE Timing: About 97.62% done; ETC: 12:04 (0:00:32 remaining)
NSE Timing: About 97.62% done; ETC: 12:04 (0:00:33 remaining)
NSE Timing: About 97.62% done; ETC: 12:05 (0:00:34 remaining)
NSE Timing: About 97.62% done; ETC: 12:05 (0:00:35 remaining)
NSE Timing: About 97.62% done; ETC: 12:06 (0:00:36 remaining)
NSE Timing: About 97.62% done; ETC: 12:07 (0:00:37 remaining)
NSE Timing: About 97.62% done; ETC: 12:07 (0:00:38 remaining)
NSE Timing: About 97.62% done; ETC: 12:08 (0:00:39 remaining)
NSE Timing: About 97.62% done; ETC: 12:09 (0:00:40 remaining)
NSE Timing: About 97.62% done; ETC: 12:09 (0:00:41 remaining)
NSE Timing: About 97.62% done; ETC: 12:10 (0:00:42 remaining)
NSE Timing: About 97.62% done; ETC: 12:11 (0:00:43 remaining)
NSE Timing: About 97.62% done; ETC: 12:12 (0:00:44 remaining)
NSE Timing: About 97.62% done; ETC: 12:12 (0:00:45 remaining)
NSE Timing: About 97.62% done; ETC: 12:13 (0:00:46 remaining)
NSE Timing: About 97.62% done; ETC: 12:14 (0:00:47 remaining)
NSE Timing: About 97.62% done; ETC: 12:15 (0:00:48 remaining)
NSE Timing: About 97.62% done; ETC: 12:16 (0:00:50 remaining)
NSE Timing: About 97.62% done; ETC: 12:17 (0:00:51 remaining)
NSE Timing: About 97.62% done; ETC: 12:17 (0:00:52 remaining)
NSE Timing: About 97.62% done; ETC: 12:18 (0:00:53 remaining)
NSE Timing: About 97.62% done; ETC: 12:19 (0:00:55 remaining)
NSE Timing: About 97.62% done; ETC: 12:20 (0:00:56 remaining)
```

```
NSE Timing: About 97.62% done; ETC: 12:21 (0:00:58 remaining)
NSE Timing: About 97.62% done; ETC: 12:22 (0:00:59 remaining)
NSE Timing: About 97.62% done; ETC: 12:23 (0:01:01 remaining)
NSE Timing: About 97.62% done; ETC: 12:24 (0:01:02 remaining)
NSE Timing: About 97.62% done; ETC: 12:25 (0:01:04 remaining)
NSE Timing: About 97.62% done; ETC: 12:27 (0:01:05 remaining)
NSE Timing: About 97.62% done; ETC: 12:28 (0:01:07 remaining)
NSE Timing: About 97.62% done; ETC: 12:29 (0:01:08 remaining)
NSE Timing: About 97.62% done; ETC: 12:30 (0:01:10 remaining)

Completed NSE at 12:29, 2909.02s elapsed
NSE: Script Scanning completed.
Nmap scan report for 192.168.101.1
Host is up (0.00069s latency).
Not shown: 1981 closed ports

PORT      STATE         SERVICE        VERSION
23/tcp    open          tcpwrapped
25/tcp    open          smtp           Sendmail 8.12.8/8.12.8
| banner: 220 localhost.localdomain ESMTP Sendmail 8.12.8/8.12.8; Fri, 4
|_Jun 2010 11:35:35 -0500
| smtp-commands: EHLO localhost.localdomain Hello [192.168.101.112],
pleased to meet you, ENHANCEDSTATUSCODES, PIPELINING, 8BITMIME, SIZE,
DSN, ETRN, DELIVERBY, HELP
|_HELP 2.0.0 This is sendmail version 8.12.8 2.0.0 Topics: 2.0.0 HELO
EHLO MAIL RCPT DATA 2.0.0 RSET NOOP QUIT HELP VRFY 2.0.0 EXPN VERB ETRN
DSN AUTH 2.0.0 STARTTLS 2.0.0 For more info use "HELP <topic>". 2.0.0 To
report bugs in the implementation send email to 2.0.0 sendmail-
bugs@sendmail.org. 2.0.0 For local information send email to Postmaster
at your site. 2.0.0 End of HELP info
|_smtp-open-relay: OPEN RELAY found.
80/tcp    open          http-proxy     Squid webproxy 2.5.STABLE1
|_citrix-brute-xml: FAILED: No domain specified (use ntdomain argument)
|_citrix-enum-servers-xml:
|_citrix-enum-apps-xml:
|_http-malware-host: Host appears to be clean
|_http-date: Fri, 04 Jun 2010 16:35:36 GMT; +6h54m13s from local time.
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:  GET HEAD CONNECTION
|_http-iis-webdav-vuln: ERROR: This web server is not supported.
110/tcp   open          pop3           ipopd 2001.78rh
|_pop3-capabilities: OK(K Capability list follows) STLS UIDL LOGIN-
DELAY(180) USER TOP SASL(LOGIN)
|_banner: +OK POP3 [192.168.101.1] v2001.78rh server ready
|_pop3-brute: sysadmin : fuckyou.
3128/tcp  open          http-proxy     Squid webproxy 2.5.STABLE1
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:  GET HEAD CONNECTION
|_http-malware-host: Host appears to be clean
10000/tcp open          http           MiniServ 0.01 (Webmin httpd)
| banner: HTTP/1.0 403 Access denied for 192.168.101.112\x0D\x0AServer: M
|_iniServ/0.01\x0D\x0ADate: Fri, 4 Jun 2010 16:35:35 GMT\x0D\x0AConten...
|_http-iis-webdav-vuln: ERROR: This web server is not supported.
|_http-malware-host: Host appears to be clean
3130/udp  open|filtered squid-ipc
9876/udp  open|filtered sd
10000/udp open|filtered unknown
16680/udp open|filtered unknown
16938/udp open|filtered unknown
17219/udp open|filtered unknown
```

```
18958/udp open|filtered unknown
19933/udp open|filtered unknown
19995/udp open|filtered unknown
21524/udp open|filtered unknown
32771/udp open|filtered sometimes-rpc6
49196/udp open|filtered unknown
57409/udp open|filtered unknown

MAC Address: 00:08:A1:4A:0B:C5 (CNet Technology)
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.18 - 2.4.35 (likely embedded)
Uptime guess: 4.009 days (since Mon May 31 12:16:26 2010)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: localhost.localdomain, 192.168.101.1; OS: Unix

HOP RTT     ADDRESS
1   0.69 ms 192.168.101.1

Read data files from: C:\Archivos de programa\Nmap
OS and Service detection performed. Please report any incorrect results
at http://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 3978.61 seconds
           Raw packets sent: 2418 (86.809KB) | Rcvd: 4024 (240.201KB)
```

ANEXO 4

ESCANEO CON SCANLINE

a) Desde el interior de la red de la Unidad Educativa

```
C:\>sl -b 192.168.101.1
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 1 IP started at Thu Jun 03 12:56:08 2010

------------------------------------------------------------------------
192.168.101.1
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports: 21 23 25 80 110 3128 10000
UDP ports: 68 69 111 123 135 137 138 161 191 192 256 260 407 445 500 514
520 1009 1024 1025 1027 1028 1030 1033 1034 1035 1037 1041 1058 1091 1352
1434 1645 1646 1812 1813 1900 1978 2002 2049 2140 2161 2301 2365 2493
2631 2967 3179 3327 3456 4045 4156 4296 4469 4802 5631 5632 11487 31337
32768 32769 32771 32772 32773 32776 32777 32778 32779 32780 32781 32782
32783 32784 32785 32786 32787 32788 32789 32790 43981

TCP 25:
[220 localhost.localdomain ESMTP Sendmail 8.12.8/8.12.8; Thu, 3 Jun 2010
12:50:20 -0500 500 5.5.1 Command unrecognized: "" 500 5.5.1 Command
unrecognized: ""]

TCP 80:
[HTTP/1.0 503 Service Unavailable Server: squid/2.5.STABLE1 Mime-Version:
1.0 Date: Thu, 03 Jun 2010 17:50:20 GMT Content-Type: text/html Content-
Length: 1031]

TCP 3128:
[HTTP/1.0 503 Service Unavailable Server: squid/2.5.STABLE1 Mime-Version:
1.0 Date: Thu, 03 Jun 2010 17:50:21 GMT Content-Type: text/html Content-
Length: 1031]

TCP 10000:
[HTTP/1.0 403 Access denied for 192.168.101.230]

------------------------------------------------------------------------

Scan finished at Thu Jun 03 12:56:21 2010

1 IP and 267 ports scanned in 0 hours 0 mins 12.88 secs


C:\>sl -b 192.168.101.250
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 1 IP started at Thu Jun 03 12:57:08 2010

------------------------------------------------------------------------
```

```
192.168.101.250
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports: 21 135 139 445 1025 1026
UDP ports: 123 137 138 445 500 1027

------------------------------------------------------------------------------

Scan finished at Thu Jun 03 12:57:17 2010

1 IP and 267 ports scanned in 0 hours 0 mins 9.39 secs

C:\>sl -b 192.168.101.253
ScanLine (TM) 1.01
Copyright (c) Foundstone, Inc. 2002
http://www.foundstone.com

Scan of 1 IP started at Thu Jun 03 12:58:11 2010

------------------------------------------------------------------------------
192.168.101.253
Responded in 0 ms.
0 hops away
Responds with ICMP unreachable: Yes
TCP ports: 21 135 139 1027
UDP ports: 135 137 138

------------------------------------------------------------------------------

Scan finished at Thu Jun 03 12:58:20 2010

1 IP and 267 ports scanned in 0 hours 0 mins 9.16 secs
```

ANEXO 5

ESCANEO CON NESSUS

TENABLE NESSUS 4

Report : 10/06/04 05:25:37 PM - New policy

Scan Time:

Start Time:	Fri Jun 04 17:25:38 2010
End Time:	Fri Jun 04 17:33:52 2010

PolicyUUID:

c094f1a1-e308-4222-9c1f-10dbe1c9d0f3

List of hosts

201.218.3.93	**Low severity problem(s) found!**

[^] Back
[Return to top]

201.218.3.93

Scan Time:

Start Time:	Fri Jun 04 17:25:39 2010
End Time:	Fri Jun 04 17:33:50 2010

Number of vulnerabilities :

Open Ports:	0
Low:	2
Medium:	0
High:	0

Information about the remote host :

Operating System:	(unknown)
NetBIOS Name:	(unknown)
DNS Name:	cpe.comil-abdon-calederon-michelena.uio.telconet.net.\n

List of ports

general/tcp	**Low vulnerability problem(s) found**

[^]Back to 201.218.3.93

general/tcp

Host Fully Qualified Domain Name (FQDN) Resolution

Synopsis :
It was possible to resolve the name of the remote host.

Description :
Nessus was able to resolve the FQDN of the remote host.

Solution :
n/a

Risk factor :

None

Plugin output :
201.218.3.93 resolves as cpe.comil-abdon-calederon-michelena.uio.telconet.net.

Nessus ID : 12053

Nessus Scan Information

Information about this scan :
Nessus version : 4.0.2 (Build 1076) (Nessus 4.2.2 is available - consider upgrading)
Plugin feed version : 201006060034
Type of plugin feed : HomeFeed (Non-commercial use only)
Scanner IP : 192.168.1.2
Port scanner(s) : nessus_syn_scanner
Port range : default
Thorough tests : no
Experimental tests : no
Paranoia level : 1
Report Verbosity : 1
Safe checks : yes
Optimize the test : yes
CGI scanning : disabled
Web application tests : disabled
Max hosts : 40
Max checks : 5
Recv timeout : 5
Backports : None
Scan Start Date : 2010/6/4 17:25
Scan duration : 487 sec

Nessus ID : 19506

ANEXO 6

ESCANEO CON CGILANguard

Filter Information

Filter & security scan details.

Filter name:	Full Report
Scan target:	201.218.3.90 [1 computer(s) meet filter conditions]
Scan profile:	Full scan
Scan date:	06/06/2010 06:37:19 PM
Computer profiles:	On
Items scanned:	1210
Scan duration:	3 minutes, 33 seconds

Summary

Note: click a detail item for quick navigation.

IP Address	Vulnerability Level	Hostname	Operating System	Details
201.218.3.90	N/A	IP.COMIL-ABDON-CALEDERON-RECOLETA.UIO.TELCONET.NET	probably Unix	

201.218.3.90 [IP.COMIL-ABDON-CALEDERON-RECOLETA.UIO.TELCONET.NET] probably Unix

Note: click a detail item for quick navigation.

Scan Errors - 4

Time	Operation	Error Message
06/06/2010 18:40:33	Error: connecting to SSH on the specified port!	Could not connect to SSH.
06/06/2010 18:40:50	Vulnerability assessment - evaluating vulnerabilities	Error: establishing connection to remote host!
06/06/2010 18:40:14	Gathering information.	The SSH connection failed with error ' Authentication failed'.
06/06/2010 18:40:10	UDP ports scanning	UDP scan is not reliable on this machine

Vulnerability Assessment - 2

Vulnerabilities - 2

Medium Security Vulnerabilities - 1

Miscellaneous Vulnerabilities - 1

SSH server accepts Version 1.x connections

SSH protocol Version 1 has various vulnerabilities, this should be disabled and only version 2 clients should be allowed to connect. For more information, visit: http://www.ssh.com/company/newsroom/article/210/

Low Security Vulnerabilities - 1

Services Vulnerabilities - 1

Service running: SSH

If this computer is not administered via secure shell, the SSH service is most likely unnecessary.

Network & Software Audit - 2

Ports - 1

TCP Ports - 1

22 [Description: Secure Shell (SSH) / Service: SSH (Remote Login Protocol)]

System Information - 1

Computer

Time to live : 56(64)

ANEXO 7

ESCANEO CON PAROSPROXY

Paros Scanning Report

Report generated at Wed, 9 Jun 2010 12:31:51.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	0

Alert Detail

Medium (Suspicious)	Lotus Domino default files
Description	Lotus Domino default files found.
URL	http://www.comil10.edu.ec/?Open
URL	http://www.comil10.edu.ec/?OpenServer
Solution	Remove default files.
Reference	

Paros Scanning Report

Report generated at Fri, 11 Jun 2010 13:17:48.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	0

Alert Detail

Medium (Warning)	Password Autocomplete in browser
Description	AUTOCOMPLETE attribute is not disabled in HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.
URL	http://www.c-3.com.ec/segura.asp?id=1
Other information	<input type="password" name="pasword" id="clave" />
URL	http://www.c-3.com.ec/index.asp
Other information	<input type="password" name="pasword" id="clave" />
URL	http://www.c-3.com.ec/segura.asp
Other information	<input type="password" name="pasword" id="clave" />
URL	http://www.c-3.com.ec/abdon.asp?id=1
Other information	<INPUT NAME="pasword" type="password" SIZE="18" face="Tahoma">
URL	http://www.c-3.com.ec/abdon.asp
Other information	<INPUT NAME="pasword" type="password" SIZE="18" face="Tahoma">
URL	http://www.c-3.com.ec/index.asp
Other information	<input type="password" name="pasword" id="clave" />
Solution	Turn off AUTOCOMPLETE attribute in form or individual input elements containing password by using AUTOCOMPLETE='OFF'
Reference	http://msdn.microsoft.com/library/default.asp?url=/workshop/author/forms/autocomplete_ovr.asp

ANEXO 8

PROFORMAS

oferta | **Q10-04220 Ver. 2**

Cliente:	COLEGIO MILITAR N10 ABDÓN CALDERÓN / QUITO	**Fecha:**	23/JUL/2010
Contacto:	ING. VERONICA MARTINEZ	**Mail:**	veromartinez55@hotmail.com
Teléfonos:	2662695	**Fax:**	
Proyecto:	RACK MC SENCILLO		

ITEMS CANTIDADES Y PRECIOS

No.	Descripción	Unidad	Cantidad	Valor Unitario	Valor Tot
1.	RACK MINI CENTRO DE CÓMPUTO- CLIMATIZADO - GABIENTE SENCILLO				
1.1	Producción nacional. Modelo: MC2010 19" Sencillo Dimensiones: Alto 202 cms x ancho 720 cms x 103 profundidad 34 U Disponoble para montaje de equipos REQUERIMIENTOS DE INSTALACIÓN: * El cliente proveerá una acometida eléctrica de dos fases 220 VAC, con su respectivo breaker de 35 Amp. * El cliente proveerá de un punto de drenaje para salida de aire. * En el lugar de ubicación del MC deberá contar con una entrada de aire del ambiente. NOTA: * No se incluye conectividad de ninguno de los equipos a ser ubicados dentro del Rack MC.	UNID	1.00	$ 3,250.00	$ 3,250.(
1.2	Ducto de descarga de calor A/A - distancia máxima estimada de 3mts.	UNID	1.00	$ 450.00	$ 450.(
1.3	Sistema de Monitoreo Blue Box SP2 Marca: AKCP.	UNID	1.00	$ 1,000.00	$ 1,000.(
1.4	UPS Marca: LIEBERT Modelo: GXT 3 KVA Capacidad de respaldo en baterias internas: 7-14 min, dependiendo la carga. Procedencia: Americana.	UNID	1.00	$ 1,964.00	$ 1,964.(
1.5	Sensor de humo, a ser instalado en el sistema de monitoreo AKCP.	UNID	1.00	$ 155.00	$ 155.(
1.6	NOTA: La instalación del MC se lo realiza dentro de los perímetros de la ciudad de QUITO, de ser el caso de realizar la instalación fuera de la ciudad de Quito se cotizara por separado los viáticos y desplazamiento de personal técnico, traslado equipos para la respectiva instalación.				
1.7	Supresor de Transcientes TVSS Capacidad: 100 Kamp 2 F	UNID	1.00	$ 550.00	$ 550.(
1.8	Control de Accesos Biométrico de huella, aproximación o tarjeta. Marca: IGUARD Modelo:LM520 FCS-SP Master biométrico Equipo con registro SOLO DE ENTRADA Incluye Software, protocolo IP/TCP e instalación. No incluye tarjetas requiere de un punto de red MODELO LM-520 FSC.MASTER & ESCLAVO Nota: Para registro de salida solo con tarjeta.	UNID	2.00	$ 1,800.00	$ 3,600.(
1.81	Tarjetas de acceso	UNID	1.00	$ 7.00	$ 7.(
1.81	Cerraduras electroimás a ser ubicadas en puertas existentes	UNID	2.00	$ 180.00	$ 360.(

Tecnoplus Cia. Ltda.
TECNOLOGIA INFORMATICA

Carlos Guerrero N33-53 y Bossano Edf. Bellini II (PB)
Telf: 3333 178 / 3333 179 / 3332 523
Telefax: 3332 524
Quito- Ecuador

CLIENTE: **COLEGIO MILITAR Nro. 10 Abdon Calderon**
ATENCION: **Veronica Martinez**

PROFORMA No. 6668

FECHA: 21 de julio del 2010

PAGINA: 1/1

CANT.	DETALLE	P.UNITARIO	P.TOTAL
1	**Servidor HP Proliant DL360 G6** **DL360 G6:** (1) Intel Xeon Quad-Core: E5530 (2.40 GHz, 8MB L3 Cache, 80 Watts, DDR3-1066, HT Turbo 1/1/2/2) / 6 GB (3 x 2GB) RDIMM (3 X 2 GB) / NO discos (0/4 2.5" SAS ó SATA) / HP Smart Array P410i/256MB Controller (RAID 0/1/1+0/5/5+0) / NC382i Dual Port Multifunction Gigabit (doble puerto)/HP DL360G6 12.7mm SATA DVD-RW Kit / Rack 1U / GARANTIA : 3-3-3 (2) Discos Duros HP 146GB 10K 6G 2.5 SAS, Hot Plug	3.324,00	3.324,00
1	Microsoft Windows 2008 Server Estandar Spanish 1pk DSP OEI DVD 1-4CPU 5 Clt	830,00	830,00
1	Switch 3com 5500-EI 24 port 10/100/1000 N/P: 3CR17250-91	3.984,00	3.984,00
1	Switch 3com 4210 de 26 port 3CR17333A-91	396,00	396,00
1	Router CISCO2801-SEC/K9	2.784,00	2.784,00
1	Firewall Dlink Modelo DFL-210	612,00	612,00
1	Router CISCO1801	1.260,00	1.260,00

Condiciones Comerciales:
- Validez de la oferta: 5 días
- Forma de Pago: 100% contra entrega
- Tiempo de entrega: Bajo pedido 45 días

Subtotal	13.190,00
12% IVA	1.582,80
Total	14.772,80

Sandra Roca M.
TECNOPLUS CIA. LTDA.
sroca@tecnoplus-ec.com