

ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

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

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

SANDRA MARISOL MAIGUA YUGLA

sandy_misol@hotmail.com

VÍCTOR GABRIEL OLALLA ARGUELLO

jackbriel@hotmail.com

DIRECTOR: ING. MSC. GUSTAVO SAMANIEGO

gsamanie@epn.edu.ec

Quito, Diciembre 2008

DECLARACIÓN

Nosotros, Sandra Marisol Maigua Yugla y Víctor Gabriel Olalla Arguello, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros 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.

Sandra Marisol Maigua Yugla

Víctor Gabriel Olalla Arguello

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Sandra Marisol Maigua Yugla y Víctor Gabriel Olalla Arguello, bajo mi supervisión.

Ing. Msc. Gustavo Samaniego
DIRECTOR DE PROYECTO

AGRADECIMIENTO

A Dios por darnos salud y fuerza para culminar una meta más en nuestras vidas.

Al Ing. Msc. Gustavo Samaniego, quien con su conocimiento y sabiduría supo guiarnos durante el desarrollo del presente proyecto de titulación.

A la Ing. Esthela Pazmiño, por su confianza y apoyo incondicional.

A todas las personas y amigos que tuvieron paciencia, tiempo y voluntad para guiarnos.

DEDICATORIA

A ustedes papitos Gustavo y Beatriz, a mis hermanos Jeaneth, Gustavo Javier y a toda mi familia que fueron mis impulsos y me dieron ánimos para terminar esta etapa de mi vida profesional.

A mis amigos del Colegio, de la Universidad Betty, Gaby, Cris, Johana, Danny y en especial a Iván y Víctor por el apoyo recibido en este tiempo difícil.

Sandra Maigua

A mis padres, Jorge y Susana quienes creyeron en mí a pesar de todos los fracasos, equivocaciones y problemas ocasionados; A mi hermano Diego ("El Bro"), simplemente gracias totales.

A mi compañera Alicia ("AVI"), por su dedicación y entrega durante el tiempo que compartimos; a mi hija Nicole ("La Nico"), quien es la razón para cumplir todos mis sueños.

A la familia, por su apoyo y comprensión.

A todos mis amigos de la universidad.

Y a mis queridos amigos Ivan V., Orlando C., Alex D., Johana C. y Sandra M.

Víctor Olalla

CONTENIDO

CONTENIDO	I
ÍNDICE DE TABLAS	V
ÍNDICE DE FIGURAS	VI
PRESENTACIÓN	VII
RESUMEN	VIII
CAPITULO 1.....	1
DESCRIPCIÓN DE LA SITUACIÓN ACTUAL DE LA EMPRESA	1
1.1 INFRAESTRUCTURA, SERVICIOS, PROTOCOLOS Y APLICACIONES DE LA RED DE TRANSMISIÓN DE DATOS.....	1
1.1.1 <i>CARACTERIZACIÓN DE LA EMPRESA.....</i>	<i>1</i>
1.1.1.1 Información General	1
1.1.1.2 Descripción Histórica.....	2
1.1.1.3 Actividad Principal.....	2
1.1.1.4 Plan Estratégico.....	3
1.1.1.4.1 Misión.....	3
1.1.1.4.2 Visión.....	3
1.1.1.4.3 Objetivo	3
1.1.1.5 Orgánico Funcional.....	3
1.1.1.6 Servicios.....	4
1.1.1.6.1 Seguridad Vehicular.....	4
1.1.1.6.2 Control Vehicular	5
1.1.1.7 Análisis de la Unidad Informática.....	6
1.1.1.7.1 Objetivos de la UI.....	6
1.1.1.7.2 Funciones de los Miembros de la UI.....	7
1.1.2 <i>ESTADO ACTUAL DE LA RED DE TRANSMISIÓN DE DATOS.....</i>	<i>8</i>
1.1.2.1 Hardware.....	8
1.1.2.1.1 Equipos de Computación y su Distribución	8
1.1.2.1.2 Servidores	8
1.1.2.2 Software	10
1.1.2.3 Redes y Comunicaciones	11
1.1.2.3.1 Equipos Activos de la Red.....	11
1.1.2.3.2 Diseño Lógico de la Red.....	11
1.1.2.3.3 Análisis de la Red LAN	12
1.1.3 <i>SERVICIOS, PROTOCOLOS Y APLICACIONES.....</i>	<i>14</i>
1.1.3.1 Servicios.....	14
1.1.3.1.1 Acceso al Internet	15
1.1.3.1.2 Correo Electrónico.....	15
1.1.3.1.3 Antivirus	16
1.1.3.1.4 DNS	17
1.1.3.1.5 Directorio Activo	17
1.1.3.1.6 Base de Datos.....	17
1.1.3.1.7 Servidor Web	18
1.1.3.1.8 Servidor de Archivos	18
1.1.3.1.9 Servidor Proxy	18
1.1.3.1.10 Servidor de Aplicaciones	18
1.1.3.1.11 Servidor de Respaldos.....	18
1.1.3.2 Protocolos	19
1.1.3.3 Aplicaciones.....	20
1.1.3.3.1 Spyral.....	20
1.1.3.3.2 Skybase III.....	20
1.1.3.3.3 Sincronizador-BDD	21
1.1.3.3.4 Carlink	21
1.1.3.3.5 UnitData.....	22
1.1.3.3.6 SMS-Sistema, GPRS-Sistema.....	22
1.1.3.3.7 Sitio Web	23
1.1.3.3.8 Control de llamadas	23
1.1.3.3.9 Control de Asistencia.....	23

1.1.4	ADMINISTRACIÓN DE LA RED.....	24
1.1.4.1	Gestión de Hardware.....	24
1.1.4.2	Gestión de Software.....	24
1.1.4.3	Gestión de Usuarios.....	24
1.1.4.4	Plan de Respaldos.....	25
1.1.4.5	Políticas de seguridad.....	25
1.2	DIAGNÓSTICO DE VULNERABILIDADES Y AMENAZAS DE LA RED DE TRANSMISIÓN DE DATOS.....	26
1.2.1	METODOLOGÍA PARA UN TEST DE INTRUSIÓN.....	26
1.2.1.1	Objetivos y Clasificación.....	26
1.2.1.1.1	Objetivos.....	26
1.2.1.1.2	Clasificación.....	27
1.2.1.2	Fases.....	28
1.2.1.2.1	Fase 1: Preparación.....	28
1.2.1.2.2	Fase 2: Reconocimiento.....	28
1.2.1.2.3	Fase 3: Análisis de Información y Riesgos.....	28
1.2.1.2.4	Fase 4: Intentos Activos de Intrusión.....	28
1.2.1.2.5	Fase 5: Análisis Final.....	29
1.2.1.3	Enfoque.....	29
1.2.1.4	Módulos.....	30
1.2.1.4.1	Módulos de Reconocimiento.....	30
1.2.1.4.2	Módulos de Intentos Activos de Intrusión.....	31
1.2.1.4.3	Principio de Exclusión.....	32
1.2.2	EJECUCIÓN DEL TEST DE INTRUSIÓN.....	33
1.2.2.1	Fase 1: Preparación.....	33
1.2.2.2	Fase 2: Reconocimiento.....	35
1.2.2.2.1	I 1. Análisis de Datos Publicados.....	35
1.2.2.2.2	I 2. Consulta Sigilosa de Información Básica de la Red.....	36
1.2.2.2.3	I 4. Escaneo Sigiloso de Puertos.....	40
1.2.2.2.4	I 6. Identificación de Aplicaciones.....	44
1.2.2.2.5	I 7. Identificación de Sistemas.....	46
1.2.2.2.6	I 8. Identificación Sigilosa del Router.....	47
1.2.2.2.7	I 10. Identificación Sigilosa del Firewall.....	49
1.2.2.2.8	I 12. Investigación de Vulnerabilidades.....	50
1.2.2.2.9	I 13. Identificación de las Interfaces de Aplicación.....	56
1.2.2.3	Fase 3: Análisis de Información y Riesgos.....	57
1.2.2.3.1	Definición de Prioridades.....	57
1.2.2.3.2	Riesgos Asociados.....	57
1.2.2.3.3	Limitación de Sistemas y Módulos.....	58
1.2.2.4	Fase 5: Análisis Final.....	58
1.2.2.4.1	Determinación de Amenazas.....	58
1.2.2.4.2	Determinación de Vulnerabilidades.....	59
CAPITULO 2.....		60
ANÁLISIS Y DISEÑO DE UN ESQUEMA DE SEGURIDAD PARA LA RED DE TRANSMISIÓN DE DATOS.....		60
2.1	REQUERIMIENTOS DE SEGURIDAD DE LA EMPRESA.....	60
2.1.1	REQUERIMIENTOS FÍSICOS.....	60
2.1.1.1	Control de Acceso Físico y de Seguridad.....	60
2.1.1.2	Estructura del Cableado.....	61
2.1.1.3	Sistema Emergente de Energía.....	61
2.1.1.4	Planes de Contingencia.....	61
2.1.1.4.1	Desastres Naturales.....	61
2.1.1.4.2	Desastres del Entorno.....	62
2.1.2	REQUERIMIENTOS LÓGICOS.....	62
2.1.2.1	Control de Acceso lógico y de Seguridad.....	62
2.1.2.1.1	Identificación y Autenticación.....	62
2.1.2.1.2	Control de Acceso Interno.....	62
2.1.2.1.3	Control de Acceso Externo.....	63
2.1.2.2	Protección de Datos.....	63
2.1.2.2.1	Respaldos.....	63
2.1.2.3	Seguridad en los Servicios.....	63
2.1.2.3.1	Acceso al Internet.....	63
2.1.2.3.2	Correo Electrónico.....	64

2.1.2.3.3	Antivirus	64
2.1.3	REQUERIMIENTOS DE RED Y COMUNICACIÓN	64
2.1.3.1	Infraestructura de la Red	64
2.1.4	REQUERIMIENTOS DE GESTIÓN	64
2.1.4.1	Gestión de la Seguridad de la Información	64
2.2	DISEÑO DE ESCENARIOS DE SEGURIDAD	65
2.2.1	ESCENARIO DE LA SEGURIDAD FÍSICA	65
2.2.1.1	Control de seguridad en el acceso físico	65
2.2.1.2	Estructura del Cableado	66
2.2.1.3	Sistema Emergente de Energía	66
2.2.1.4	Planes de Contingencia	66
2.2.2	MODELO DE SEGURIDAD “SAFE” DE CISCO	67
2.2.2.1	Visión General de la Arquitectura	67
2.2.2.1.1	Fundamentos del Diseño	67
2.2.2.1.2	Concepto de Módulos	67
2.2.2.1.3	Axiomas de “SAFE” de Cisco	68
2.2.2.2	Módulos de la Empresa	70
2.2.3	ESCENARIO DE LA SEGURIDAD LÓGICA BASADO EN “SAFE” DE CISCO	70
2.2.3.1	Campus Empresarial	71
2.2.3.1.1	Módulo Central	71
2.2.3.1.2	Módulo de Distribución de Edificios	72
2.2.3.1.3	Módulo de Edificios (Usuarios)	72
2.2.3.1.4	Módulo de Servidores	73
2.2.3.1.5	Módulo de Administración	74
2.2.3.1.6	Perímetro de Distribución	76
2.2.3.2	Perímetro Empresarial	76
2.2.3.2.1	Módulo de Comercio Electrónico	77
2.2.3.2.2	Módulo de Internet	78
2.2.3.2.3	Módulo VPN y de Acceso Remoto	79
2.2.3.2.4	Módulo WAN	80
2.2.3.3	Diseño del Esquema de Seguridad para la Red de Datos	81
2.2.3.3.1	Diseño Completo	82
2.2.3.3.2	Diseño Básico	84
2.2.3.3.3	Análisis Comparativo	86
2.3	POLÍTICAS Y NORMAS DE SEGURIDAD	87
2.3.1	POLÍTICAS DE SEGURIDAD	89
2.3.1.1	Políticas de Seguridad en Hardware, Dispositivos Periféricos y otros Equipos	89
2.3.1.1.1	De la Instalación del Equipo de Computo	89
2.3.1.1.2	Del Mantenimiento del Equipo de Cómputo	90
2.3.1.1.3	De la Seguridad Física del Equipo de Cómputo	90
2.3.1.2	Políticas de Seguridad para Control de Acceso a los Sistemas e Información	90
2.3.1.2.1	Del Acceso a las Áreas Críticas	90
2.3.1.2.2	Del Control de Acceso a la Red	90
2.3.1.2.3	Del Accesos al Sistema Operativo	91
2.3.1.2.4	De la Creación, Identificación y Autenticación de los Usuarios	91
2.3.1.2.5	Del Acceso a Documentos y Archivos	91
2.3.1.2.6	Del Acceso Remoto	91
2.3.1.2.7	Del Acceso a Correo Electrónico e Internet	91
2.3.1.3	Políticas de Seguridad para Recursos Computacionales y de Red	92
2.3.1.3.1	Configuración de la Red	92
2.3.1.3.2	De la Administración de Base de Datos y Aplicaciones	92
2.3.1.3.3	De los Respaldos y Recuperación de Archivos	92
2.3.1.4	Políticas de Seguridad para la Adquisición, Registro, Almacenamiento y Manejo de Software Comercial	92
2.3.1.5	Políticas de Seguridad para el Desarrollo y Mantenimiento de Software Institucional	93
2.3.1.6	Políticas de Seguridad para Combatir el Crimen Cibernético	93
2.3.1.6.1	De los Ataques Internos, Externos y Virus	93
2.3.1.7	Políticas de Seguridad para Contingencias ante Desastres	93
2.3.1.8	Políticas de Seguridad para la Capacitación del Personal Técnico	93
2.3.1.9	Políticas de Seguridad de los Sistemas de Protección (UPS)	93
2.3.2	NORMAS DE SEGURIDAD	94
2.3.2.1	Normas para la Instalación del Equipo de Computo	94
2.3.2.2	Normas para el Mantenimiento del Equipo de Computo	94
2.3.2.3	Normas de la Seguridad Física del Equipo de Computo	94
2.3.2.4	Normas del Acceso Físico a las Áreas Críticas	95

2.3.2.5	Normas de Control de Acceso a la Red.....	95
2.3.2.6	Normas del Control de Software y Acceso al Sistema Operativo	95
2.3.2.7	Normas de Creación, Identificación y Autenticación de Usuarios.....	95
2.3.2.8	Normas de Acceso a Documentos y Archivos	96
2.3.2.9	Normas del Control de Acceso Remoto	96
2.3.2.10	Normas del Acceso a Correo Electrónico e Internet.....	96
2.3.2.11	Normas de Configuración de la Red	96
2.3.2.12	Normas de la Administración de Base de Datos y Aplicaciones.....	97
2.3.2.13	Normas de los Respaldos y Recuperación de Archivos de Información	97
2.3.2.14	Normas para Adquirir, Registrar, Almacenar y Administrar Software Corporativo	98
2.3.2.15	Norma para el Desarrollo del Software Institucional	99
2.3.2.16	Normas de los Ataques Internos, Externos y Virus.....	99
2.3.2.17	Normas para Contingencia ante Desastres	99
2.3.2.18	Normas para la Capacitación Técnica del Personal.....	99
2.3.2.19	Normas de los Sistemas de Protección.....	100
2.3.2.20	Normas Generales y Sanciones	100
CAPITULO 3.....		102
PROPUESTA TÉCNICA ECONÓMICA DEL ESQUEMA DE SEGURIDAD		102
3.1	ESPECIFICACIONES TÉCNICAS.....	102
3.1.1	DE LA SEGURIDAD FÍSICA.....	102
3.1.2	DE LOS EQUIPOS ACTIVOS.....	106
3.1.2.1	Equipos Activos - Diseño Completo	107
3.1.2.2	Equipos Activos - Diseño Básico.....	115
3.1.3	DEL SOFTWARE	120
3.1.4	GENERALES.....	121
3.2	PRESUPUESTO REFERENCIAL.....	122
3.2.1	DETALLE DE LAS EMPRESAS.....	122
3.2.2	DETALLE DEL COSTO PROMEDIO REFERENCIAL.....	123
3.2.2.1	Detalle del Costo - Seguridad Física	123
3.2.2.2	Detalle del Costo - Diseño Completo.....	124
3.2.2.3	Detalle del Costo - Diseño Básico.....	125
3.2.3	PROPUESTA PARA LA IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD	126
3.2.3.1	Propuesta - Diseño Completo.....	126
3.2.3.2	Propuesta - Diseño Básico.....	127
CAPITULO 4.....		128
CONCLUSIONES Y RECOMENDACIONES		128
4.1	CONCLUSIONES.....	128
4.2	RECOMENDACIONES	130
BIBLIOGRAFÍA.....		132
ANEXOS		CD
ANEXO 1. METODOLOGÍA PARA UN TEST DE INTRUSIÓN.....		CD
ANEXO 2. HERRAMIENTAS DE ESCANEADO Y VULNERABILIDADES.....		CD
ANEXO 3. NSLOOKUP AL SERVIDOR DE NOMBRES		CD
ANEXO 4. CONTENIDO DEL SITIO WEB		CD
ANEXO 5. TIPOS DE ESCANEADO - DESCRIPCIÓN		CD
ANEXO 6. ESCANEADO SIGILOSO DE PUERTOS		CD
ANEXO 7. IDENTIFICACIÓN DE SERVICIOS Y APLICACIONES.....		CD
ANEXO 8. IDENTIFICACIÓN REMOTA DE SISTEMAS OPERATIVOS		CD
ANEXO 9. IDENTIFICACIÓN DEL BANNER		CD
ANEXO 10. ESCANEADO DIRECTO DEL FIREWALL.....		CD
ANEXO 11. ESCANEADO DE VULNERABILIDADES		CD
ANEXO 12. ESCANEADO DE VULNERABILIDADES – INTERFAZ WEB		CD
ANEXO 13. CALCULO DE LA POTENCIA – UPS Y GENERADOR ELÉCTRICO		CD
ANEXO 14. MODELO “SAFE” DE CISCO.....		CD
ANEXO 15. ESPECIFICACIONES TÉCNICAS - EQUIPOS EXISTENTES		CD
ANEXO 16. PROFORMAS.....		CD

ÍNDICE DE TABLAS

TABLA 1.1 INFORMACIÓN GENERAL DE LA EMPRESA	1
TABLA 1.2 DISTRIBUCIÓN DE LOS EQUIPOS DE COMPUTACIÓN	8
TABLA 1.3 CARACTERÍSTICAS DE LOS SERVIDORES	9
TABLA 1.4 LISTADO DE SOFTWARE.....	10
TABLA 1.5 EQUIPOS DE INTERCONEXIÓN DE LA RED DE DATOS.....	11
TABLA 1.6 SERVICIOS EN LA RED LAN.....	14
TABLA 1.7 MÓDULOS DE RECONOCIMIENTO.....	30
TABLA 1.8 MÓDULOS PARA INTENTOS ACTIVOS DE INTRUSIÓN.....	31
TABLA 1.9 TEST DE INTRUSIÓN SELECCIONADO	34
TABLA 1.10 WHOIS DEL DOMINIO “CARLINK.COM.EC”	37
TABLA 1.11 NSLOOKUP – DOMINIO “CARLINK.COM.EC”	38
TABLA 1.12 ESCANEOS SIGILOSOS DE PUERTOS	43
TABLA 1.13 IDENTIFICACIÓN DE APLICACIONES	44
TABLA 1.14 IDENTIFICACIÓN DE SISTEMAS.....	46
TABLA 1.15 IDENTIFICACIÓN DEL BANNER.....	47
TABLA 1.16 ANÁLISIS DE RUTAS - ROUTER	48
TABLA 1.17 ESCANEOS DIRECTOS DEL FIREWALL.....	49
TABLA 1.18 ESCANEOS DE VULNERABILIDADES.....	52
TABLA 1.19 ESCANEOS DE VULNERABILIDADES – INTERFAZ WEB.....	57
TABLA 2.1 EQUIPOS REQUERIDOS – DISEÑO COMPLETO.....	82
TABLA 2.2 EQUIPOS REQUERIDOS – DISEÑO BÁSICO	84
TABLA 2.3 POLÍTICAS Y NORMAS DE SEGURIDAD.....	101
TABLA 3.1 ESPECIFICACIONES DE LOS EQUIPOS REQUERIDOS - SEGURIDAD FÍSICA	102
TABLA 3.2 ESPECIFICACIONES DE LOS EQUIPOS REQUERIDOS - DISEÑO COMPLETO.....	107
TABLA 3.3 ESPECIFICACIONES DE LOS EQUIPOS REQUERIDOS - DISEÑO BÁSICO	115
TABLA 3.4 SOFTWARE REQUERIDO - DISEÑO COMPLETO	120
TABLA 3.5 SOFTWARE REQUERIDO - DISEÑO BÁSICO.....	120
TABLA 3.6 COSTO DE LOS EQUIPOS - SEGURIDAD FÍSICA.....	123
TABLA 3.7 COSTO DE LA INFRAESTRUCTURA - SEGURIDAD FÍSICA.....	123
TABLA 3.8 COSTO TOTAL REFERENCIAL DE LA IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD FÍSICA.....	123
TABLA 3.9 COSTO DE LOS EQUIPOS DE NETWORKING - DISEÑO COMPLETO	124
TABLA 3.10 COSTO DE LOS ACCESORIOS PARA LOS EQUIPOS DE NETWORKING - DISEÑO COMPLETO	125
TABLA 3.11 COSTO DE LOS EQUIPOS DE NETWORKING – DISEÑO BÁSICO	125
TABLA 3.12 COSTO DE LOS ACCESORIOS PARA LOS EQUIPOS DE NETWORKING – DISEÑO BÁSICO.....	126
TABLA 3.13 COSTO TOTAL REFERENCIAL DE LA IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD – DISEÑO COMPLETO.....	126
TABLA 3.14 COSTO TOTAL REFERENCIAL DE LA IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD – DISEÑO BÁSICO	127

ÍNDICE DE FIGURAS

FIGURA 1.1 ORGÁNICO FUNCIONAL DE LA EMPRESA	3
FIGURA 1.2 DISEÑO LÓGICO DE LA RED.....	11
FIGURA 1.3 ANÁLISIS DE TRÁFICO POR PROTOCOLO.....	13
FIGURA 1.4 MEDICIÓN DEL ANCHO DE BANDA	15
FIGURA 1.5 SISTEMA DE FACTURACIÓN	20
FIGURA 1.6 SISTEMA SKYBASE III	21
FIGURA 1.7 SISTEMA CARLINK	21
FIGURA 1.8 SISTEMA UNITDATA.....	22
FIGURA 1.9 GPRS-SISTEMA.....	22
FIGURA 1.10 PÁGINA WEB DE LA EMPRESA	23
FIGURA 1.11 CLASIFICACIÓN GENERAL DE UN TEST DE INTRUSIÓN.....	27
FIGURA 1.12 FASES DEL TEST DE INTRUSIÓN	29
FIGURA 1.13 PRINCIPIO DE EXCLUSIÓN.....	32
FIGURA 1.14 CLASIFICACIÓN SEGÚN EL TIPO DE ESCANEO DE PUERTOS	42
FIGURA 1.15 INTERFAZ DE INGRESO, APLICACIÓN WEB	45
FIGURA 1.16 ANÁLISIS DE RUTAS - ROUTER	48
FIGURA 2.1 MÓDULO COMPUESTO DE LA EMPRESA.....	68
FIGURA 2.2 DIAGRAMA DE BLOQUES DE “SAFE”	68
FIGURA 2.3 DISEÑO DEL MÓDULO CENTRAL	71
FIGURA 2.4 DISEÑO DEL MÓDULO DE EDIFICIOS.....	72
FIGURA 2.5 DISEÑO DEL MÓDULO DE SERVIDORES	73
FIGURA 2.6 DISEÑO DEL MÓDULO DE ADMINISTRACIÓN	75
FIGURA 2.7 DISEÑO DEL PERÍMETRO DE DISTRIBUCIÓN.....	76
FIGURA 2.8 DISEÑO DEL MÓDULO DE COMERCIO ELECTRÓNICO.....	77
FIGURA 2.9 DISEÑO DEL MÓDULO DE INTERNET.....	79
FIGURA 2.10 DISEÑO DEL MÓDULO VPN Y ACCESO REMOTO.....	80
FIGURA 2.11 DISEÑO DEL MÓDULO WAN	80
FIGURA 2.12 DISEÑO COMPLETO DE SEGURIDAD PARA LA RED DE TRANSMISIÓN DE DATOS.....	83
FIGURA 2.13 DISEÑO BÁSICO DE SEGURIDAD PARA LA RED DE TRANSMISIÓN DE DATOS	85

PRESENTACIÓN

La masiva utilización de las computadoras y redes como medios para transferir, procesar y almacenar información en los últimos años se ha incrementado, transformando la información en todas sus formas y estados en un activo de altísimo valor, el cual se debe proteger y asegurar para garantizar su integridad, disponibilidad y confidencialidad.

El presente proyecto nace de la necesidad de proteger a través de un nuevo esquema de seguridad la red de transmisión de datos de la empresa CARLINK, ofreciendo a la unidad informática (Jefe de Sistemas, asistentes y operarios de monitoreo) una red administrable, flexible y escalable; y a los usuarios y clientes una red segura y confiable.

RESUMEN

El presente proyecto tiene como objetivo realizar el análisis, el diseño y la 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, con la finalidad de garantizar la disponibilidad, integridad y confiabilidad de la red de datos frente a las amenazas internas y externas a las que está expuesta.

El proyecto parte del análisis de la situación actual de la empresa, donde se ha sintetizando el ambiente para el cual se va a desarrollar el esquema de seguridad, lo que permite diseñar un esquema que se ajuste a las necesidades de la empresa y a su presupuesto. Todo el análisis ha sido agrupado en dos puntos generales: Infraestructura, Servicios, Protocolos y Aplicaciones; y Diagnóstico de Vulnerabilidades y Amenazas de la red de transmisión de datos.

El diagnóstico de las Vulnerabilidades y Amenazas de la red de transmisión de datos, fue desarrollado en base al “Penetration Testing Methodology” usado por “la Oficina Federal para la Seguridad de la Información – BSI”, que provee el servicio de seguridad en tecnologías de la información para el Gobierno Alemán. Esta metodología esta dividida en 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, el alcance, el “Test de Intrusión” seleccionado y los riesgos asociados con su ejecución. La fase de “Reconocimiento” se inicia con el análisis de datos publicados, la identificación y el escaneo de puertos, aplicaciones, sistemas y equipos; incluyendo la investigación de vulnerabilidades y defectos conocidos de seguridad. En la fase de “Análisis de Información y Riesgos” se definen prioridades, se establece los riesgos asociados y se limitan sistemas y módulos. La fase de “Intentos Activos de Intrusión” conlleva el mayor riesgo de seguridad en la ejecución del test, ya que se invaden activamente los sistemas y módulos seleccionados en la fase anterior, la ejecución de esta fase se debe considerar cuidadosamente por el tester, ya que es posible afectar el normal desempeño de la empresa.

En la última fase llamada “Análisis Final”, se concluyen las amenazas y vulnerabilidades determinadas durante la aplicación del “Test de Intrusión”.

El diseño del esquema de seguridad para la red de transmisión de datos se estableció en base a los requerimientos obtenidos del análisis de la situación actual de la empresa y del diagnóstico de las vulnerabilidades y amenazas. Para su elaboración se utilizó el Modelo de Seguridad “SAFE” de Cisco para redes empresariales, el cual divide a la red en dos áreas funcionales: el Campus Empresarial y el Perímetro Empresarial, a su vez estas áreas se dividen en módulos: Central, Distribución de Edificios, Edificios (Usuarios), Servidores, Perímetro de Distribución, Administración, Comercio Electrónico, Internet y VPN/Acceso Remoto, en los cuales se detallan las distintas amenazas y las soluciones para combatir cada de una de ellas. Todo esto complementado con las políticas y normas de seguridad, conforman un esquema de seguridad que involucra además de los sistemas y equipos, a los usuarios de la red.

En lo concerniente a la propuesta técnica económica del esquema de seguridad, inicialmente se detalla 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 el costo promedio referencial de la implementación del esquema de seguridad.

CAPITULO 1.

DESCRIPCIÓN DE LA SITUACIÓN ACTUAL DE LA EMPRESA


1.1 INFRAESTRUCTURA, SERVICIOS, PROTOCOLOS Y APLICACIONES DE LA RED DE TRANSMISIÓN DE DATOS.

Antes de describir la infraestructura, servicios, protocolos y aplicaciones presentes en la empresa Carlink, se dará a conocer información acerca de la historia, organización, funcionamiento y actividades, para así entender de mejor manera el entorno para el cual se va a desarrollar el presente proyecto de titulación.

1.1.1 CARACTERIZACIÓN DE LA EMPRESA

1.1.1.1 Información General

Tabla 1.1 Información General de la Empresa

	
Nombre de la empresa:	AUDIOAUTO S.A.
Nombre comercial:	CARLINK
Gerente general:	Sr. Robert Wright Enz
Dirección:	Av. Gaspar de Villarroel E9-39 y Av. de los Shyris
Teléfono:	(593-2) 2439-920
Dirección Web:	http://www.carlink.com.ec

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.1.2 Descripción Histórica

Audioauto S.A. se constituye legalmente el 02 de Julio de 1997, contando con un gerente general, un gerente comercial, una secretaria y dos técnicos instaladores, todos ellos dedicados a la venta de alarmas y radios únicamente, posteriormente incursionan en el mercado de distribuidores y concesionarios, a quienes realizaban ventas relativamente grandes.

En 1998 se estudia el proyecto de lanzamiento del Carlink (paralizador vehicular), haciéndolo efectivo en el mes de octubre de ese mismo año. En 1999 ingresa al mercado de las ensambladoras (Aymesa y Aekia), se crea la sucursal de Guayaquil e inicia operaciones el 13 de septiembre, dedicándose especialmente a la venta de dispositivos Carlink. En el año 2000 la empresa atraviesa el proceso de dolarización, con lo cual se reactivan los negocios tanto en aseguradoras como en concesionarios iniciando una etapa de estabilidad y crecimiento a nivel nacional, de tal manera que se abre en el año 2001 una nueva sucursal en Cuenca. Las ventas en el año 2002 aumentan notablemente, en ese mismo año se abre un nuevo local en la ciudad de Quito con la finalidad de ampliar las áreas de instalación, administración y monitoreo.

Se realizan adecuaciones en el local inicial de Carlink y se destina esta área para el show room y el área comercial, todo esto con el objetivo de realizar el lanzamiento de Tracklink, el mismo que se realiza en octubre del 2002. En ese mismo año se abre una nueva sucursal en Ambato. En el año 2003 se abre una nueva sucursal en Manta y Machala.

1.1.1.3 Actividad Principal

La empresa ofrece el servicio de seguridad y control vehicular, que permite a los clientes conocer en cualquier momento la localización, el estado y situación del vehículo a nivel nacional para en caso de robo, detenerlo y facilitar la recuperación del mismo.

1.1.1.4 Plan Estratégico

1.1.1.4.1 Misión

“Lograr que los clientes se sientan seguros y en control de su modo de transporte y que la seguridad pase a ser un factor secundario dentro de sus mentes”¹.

1.1.1.4.2 Visión

“Ser los mejores asesores de compras de equipos de seguridad y control vehicular del mundo”¹.

1.1.1.4.3 Objetivo

- Ser ejemplo de calidad en nuestro trabajo, productos y servicios
- Trabajar con pasión, lealtad y unidad
- Innovación, Tecnología y Seguridad

1.1.1.5 Orgánico Funcional.

La empresa se encuentra estructurada de acuerdo a la siguiente jerarquía, ver Figura 1.1.

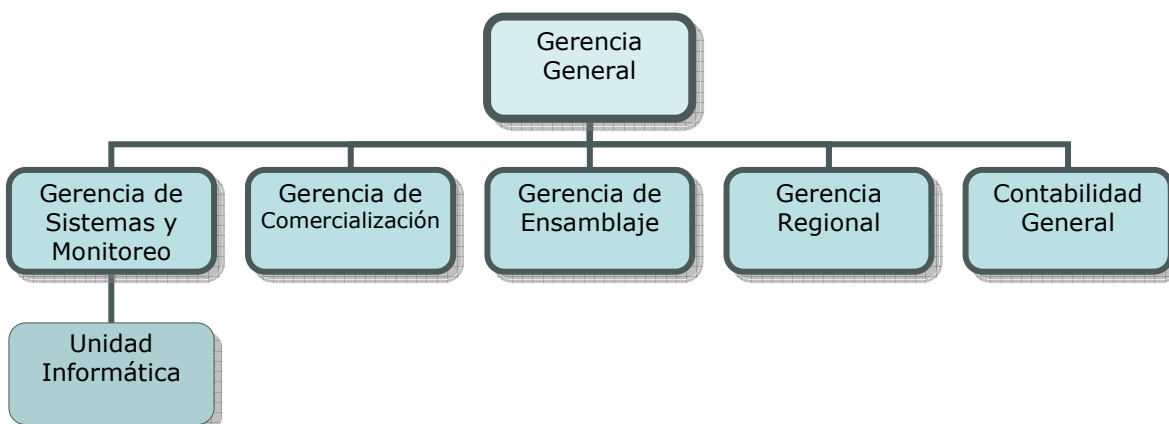


Figura 1.1 Orgánico Funcional de la Empresa

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

¹ <http://200.24.213.164/Carlink/html/ideologia.htm>

1.1.1.6 Servicios

La empresa Carlink presta los siguientes servicios para la satisfacción de los clientes actuales y futuros.

1.1.1.6.1 Seguridad Vehicular

Permiten la localización y paralización instantánea de un vehículo para, en caso de robo posteriormente detenerlo y facilitar la recuperación del mismo. Adicionalmente, cada sistema de seguridad vehicular se encuentra integrado a un dispositivo que permite al usuario conocer, en cualquier momento, la localización del vehículo.

Los sistemas de seguridad vehicular disponibles son:

- **TRACKLINK**

Combina el sistema de satélites GPS, con la tecnología SMS de las operadoras celulares. El uso de ambas tecnologías brinda los beneficios de una localización exacta, amplia cobertura y velocidad en la recepción y envío de información, lo que sumado al acceso al sistema vía Internet, hacen de "Tracklink" el más completo y efectivo sistema de seguridad y control vehicular.

Sus características principales son:

- Localización del vehículo en tiempo real – vía Web
- Apertura remota de puertas – vía Web
- Paralización controlada del vehículo en caso de asalto

- **ROADLINK**

Combina el sistema de satélites GPS con la tecnología SMS de las operadoras celulares. En caso de robo, el usuario del sistema contacta a la central de monitoreo desde donde se envía la señal de localización. Una vez obtenidas las coordenadas del GPS y situadas dentro de los mapas digitales del país, se procede a enviar la señal de paralización.

Sus características principales son:

- Localización del vehículo en tiempo real
- Apertura remota de puertas
- Paralización controlada del vehículo en caso de asalto

- **CARLINK**

Utiliza la tecnología de los sistemas SkyTel para el envío de señales codificadas al vehículo. En caso de robo, el usuario del sistema contacta a la central de monitoreo desde donde se envía la señal de bloqueo preventivo o paralización. Una vez recibida la señal, Carlink interactúa con el sistema eléctrico del vehículo haciendo imposible su movilización.

Sus características principales son:

- Paralización controlada del vehículo en caso de asalto
- Cobertura en las principales ciudades del país: Quito, Guayaquil, Cuenca, Manta, Machala, Babahoyo, Ambato, Latacunga, Ibarra, Riobamba, La Península (Ballenita, Salinas, Santa Elena, Libertad, Ancón, Anconcito, Punta Carnero) y Portoviejo.

1.1.1.6.2 Control Vehicular

Para este fin, únicamente se utiliza el sistema de control vehicular "Transtrack".

- **TRANSTRACK**

Sistema de control y seguridad vehicular que permite al usuario estar conectado constantemente con su vehículo, la interacción del usuario con el sistema a través de la página Web le permite conocer, en cualquier momento, el estado y situación del vehículo.

Combina el sistema de satélites GPS con la tecnología GPRS² de las operadoras celulares. El uso de ambas tecnologías brindan al sistema "Transtrack" los beneficios de una localización exacta, comunicación constante y en tiempo real con el administrador de la flota, amplia cobertura y velocidad en la recepción y envío de información.

² General Packet Radio Service

Desde la página Web el usuario puede:

- Localizar el vehículo en tiempo real
- Generar reportes del recorrido realizado
- Verificar el número y tiempo de las paradas realizadas
- Comprobar si han existido excesos de velocidad
- Confirmar la violación de las cercas virtuales
- Determinar la distancia recorrida
- Recibir alertas de pánico emitidas desde el vehículo
- Visualizar la información en mapas digitalizados

1.1.1.7 Análisis de la Unidad Informática

1.1.1.7.1 Objetivos de la UI

La Unidad Informática en la empresa básicamente cumple con los siguientes objetivos:

- Administrar, dar mantenimiento y soporte a la red de computación
- Desarrollar, implementar y actualizar las aplicaciones de la empresa de acuerdo a las necesidades actuales, para brindar un mejor servicio a los usuarios de la red.
- Incrementar la productividad y aumentar la satisfacción de los usuarios internos y externos, a través del servicio "Help Desk".
- Proveer una disponibilidad 24/7 de los recurso y servicios informáticos a cada uno de los departamentos que forman parte de la empresa.
- Incorporar nuevas tecnologías en beneficio del mejoramiento continuo de la empresa.

1.1.1.7.2 Funciones de los Miembros de la UI

Las funciones del **Jefe de Sistemas** son las siguientes:

- Administrar la red de cómputo
- Administrar los servidores
- Administrar los respaldos
- Administrar las cuentas de correo
- Asesorar en la compra de equipos y contratación de servicios informáticos
- Establecer políticas y normas de seguridad
- Controlar el cumplimiento de políticas y normas
- Implantar nuevas tecnologías en beneficio de la empresa
- Gestionar y administrar el Departamento de Sistemas

Las funciones del **Asistente de Sistemas** son las siguientes:

- Proveer el servicio de “Help Desk”
- Soporte de la red de computo
- Respalda datos de los servidores
- Desarrollar nuevas aplicaciones
- Capacitar a los usuarios de la empresa en nuevas tecnologías

Las funciones del **Operario de Monitoreo** son las siguientes:

- Instalar y probar las aplicaciones del sistema de monitoreo
- Reportar alertas en el sistema de monitoreo a un asistente de sistemas
- Coordinar la recuperación de autos robados

1.1.2 ESTADO ACTUAL DE LA RED DE TRANSMISIÓN DE DATOS

1.1.2.1 Hardware

1.1.2.1.1 Equipos de Computación y su Distribución

Dentro de la empresa existe un total de 7 portátiles, 66 equipos de computación y 17 impresoras, todos estos se encuentran distribuidos dentro de 13 departamentos. A continuación se muestra la distribución de los equipos de computación en cada departamento, ver Tabla 1.2.

Tabla 1.2 Distribución de los Equipos de Computación

Departamento	Equipos de Computación	Portátiles	Impresoras
Sistemas	15	0	0
Ventas	9	0	6
Comercial	7	2	1
Cobranzas	7	0	0
Renovación	6	0	3
Contratos	5	0	0
Monitoreo	4	1	1
Contabilidad	3	1	2
Ensamblaje	2	2	1
Recursos Humanos	2	1	0
Bodega	2	0	2
Importaciones	2	0	1
Laboratorio	2	0	0
Total	66	7	17

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.2.1.2 Servidores

La empresa cuenta con un total de 11 servidores, de los cuales 8 poseen arquitectura de servidor y 3 poseen arquitectura de Workstation. Entre los servidores que pueden ser accedidos desde el Internet tenemos: IIS y Administración, cada uno cumple la función de servidor Web y de Correo respectivamente.

Las principales características de hardware de los servidores se indican a continuación, ver Tabla 1.3.

Tabla 1.3 Características de los Servidores

Nombre del Equipo	Marca	Procesador	RAM	Disco	Sistema Operativo
ADMINISTRACIÓN	Compaq Proliant ML350 G2	Intel Pentium III 1,26 GHz	1024 MB	90 GB	Windows 2000 SP4
CLUSTER1	Compaq Proliant ML350 G2	Intel Pentium III 1,26 GHz	512 MB	16,9 GB	Windows 2000 AS SP4
IIS	Compaq Proliant ML350 G2	Intel Pentium III 1,26 GHz	1024 MB	36 GB	Windows 2000 SP4
Server-Carlink (Workstation)	Gateway E-3200	Intel Pentium III 1,2 GHz	128 MB	20 GB	Windows 2000 Professional
Sincronización (Workstation)	HP xw4400	Intel Core 2 Duo 2,4 GHz	2048 MB	160 GB	Windows 2000 SP4
Skycontrol (Workstation)	Compaq Evo W6000	Intel Xeon 1,4 GHz	512 MB	16,9 GB	Windows 2000 SP4
SPYRALBDD	HP ProLiant DL385 G2	AMD Opteron Dual core 2,80 GHz	2048 MB	110 GB	Windows 2003 SP1
SQL-UIO-01	HP ProLiant DL380 G5	Intel Xeon Quad Core 2,33 GHz	4864 MB	252 GB	Windows 2003 SP2
SRVPORTA	HP ProLiant ML350 G3	Intel Xeon 3,06 GHz	1536 MB	72 GB	Windows 2000 AS
SRVWEB	HP ProLiant DL380 G5	Intel Xeon Quad Core 2,33 GHz	3072 MB	144 GB	Windows 2003 SP2
WRSQL	HP ProLiant DL380 G5	Intel Xeon Quad Core 2,33 GHz	3328 MB	252 GB	Windows 2003 SP2

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.2.2 Software

Hasta septiembre del 2007, la empresa mantiene instalado el siguiente listado de software, ver Tabla 1.4; con sus respectivas licencias en los equipos de la red.

Tabla 1.4 Listado de Software

Sistemas Operativos	Nro. Licencias
Microsoft Windows 98	3
Microsoft Windows 2000	11
Microsoft Windows Me	1
Microsoft Windows XP	38
Motores de Base de Datos	Nro. Licencias
Cliente/Microsoft SQL Server 2000	41
MySQL 5.0	2
Monitoreo y Control	Nro. Licencias
GFI LANguard Network Security 7.0	64
Sniffer Pro 4.7	1
Oficina	Nro. Licencias
Open Office 2.0	28
Microsoft Office 97	14
Microsoft Office 2000	2
Microsoft Office 2003	4
Microsoft Office XP	9
Utilitarios	Nro. Licencias
Symantec Norton Antivirus EE 2006	50
Lotus Notes 5.0.9	45
Adobe Acrobat Reader 6.0	35
Spy Sweeper 5.2	11
Lotus Domino 6.0	1
PcAnywhere 12.1	1
Auto CAD 2004	1
Institucional	Nro. Licencias
Spyral	39
Skybase III	5
Carlink	3
Control de Asistencia	1
UnitData	1
Sincronizador-BDD	1
SMS-Sistema	1
GPRS-Sistema	1
Control de Llamadas	1
Sitio Web	1

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.2.3 Redes y Comunicaciones

1.1.2.3.1 Equipos Activos de la Red

Los equipos de interconexión en la red de datos se presentan a continuación, ver Tabla 1.5.

Tabla 1.5 Equipos de Interconexión de la Red de Datos

Cantidad	Equipos Activos	Fabricante	Modelo
1	Switch	Hewlett Packard	Procurve 2524
2	Switch	3Com	Baseline 2024
1	Firewall	Check Point	VPN-1 UTM Edge
1	Router	Cisco	805
1	Router	Cisco	1601 R

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.2.3.2 Diseño Lógico de la Red

El diseño lógico de la red de datos se presenta a continuación, ver Figura 1.2.

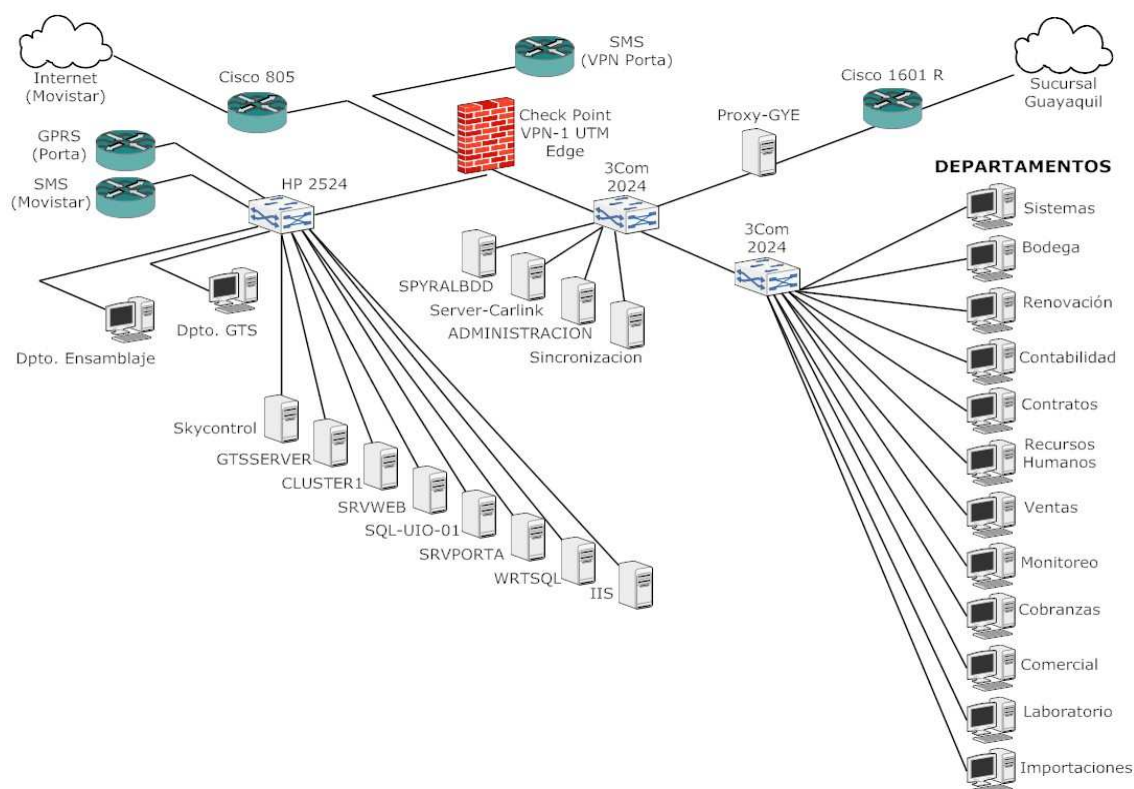


Figura 1.2 Diseño Lógico de la Red

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.2.3.3 Análisis de la Red LAN

La red LAN Ethernet presenta una topología de estrella extendida, ya que los equipos de cada departamento están conectados a un equipo activo de la red, y estos a su vez se conectan a un nodo central (Firewall).

Se utiliza cable de par trenzado no blindado (UTP nivel 5e) para conectar los servidores, los equipos de computación y los equipos activos de la red. Lo que permite una velocidad de transmisión de hasta 1 Gbps, sin embargo los switches solamente soportan 100 Mbps de velocidad de transmisión.

La asignación de direcciones IP para cualquier equipo de la red se realiza manualmente, ya que la administración de permisos de acceso a los servidores, a los servicios y a los recursos de la red se basa en la dirección IP.

Las horas de mayor tráfico en la red son en la mañana de 8:30 a 10:00 y en la tarde de 15:00 a 17:30, para determinar los protocolos más utilizados en este horario se utilizó la herramienta "Wireshark Network Protocol Analyzer v0.9"³, que registra todos los paquetes que circulan por la red, y genera un reporte con el porcentaje de paquetes recibidos según el protocolo, ver Figura 1.3.

³ <http://ftp.uni-kl.de/pub/wireshark/win32/wireshark-setup-0.99.6a.exe>

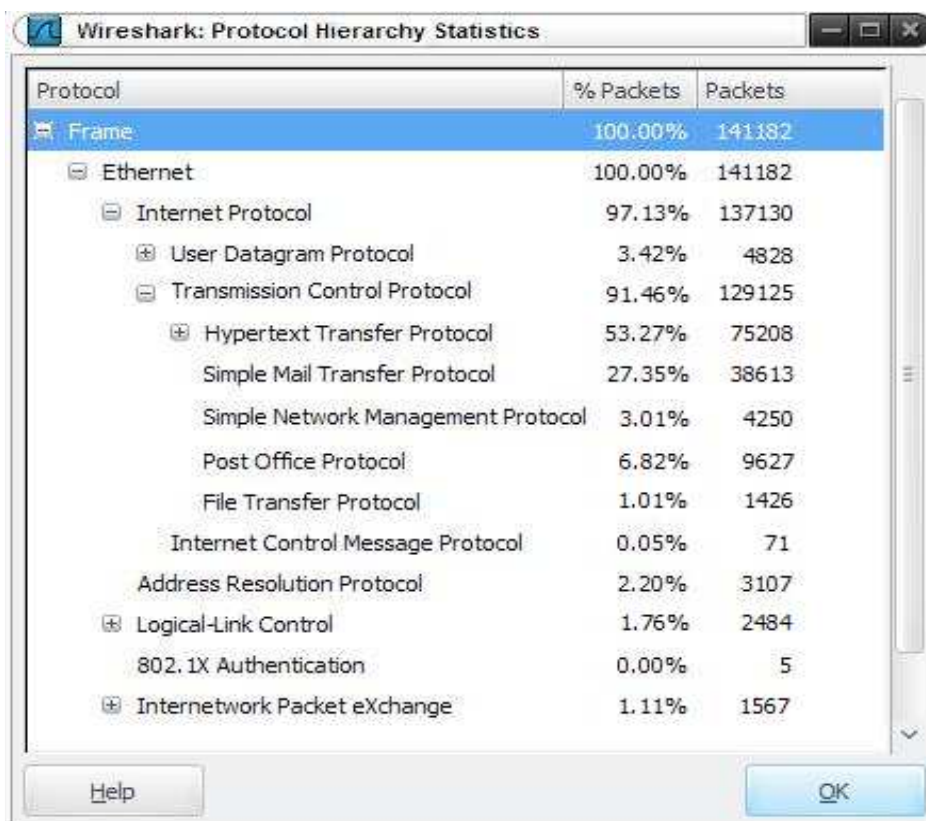


Figura 1.3 Análisis de Tráfico por Protocolo

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

El protocolo más utilizado es el HTTP, esto se debe a que los usuarios manejan aplicaciones y servicios Web, por lo que es necesario conocer las páginas Web mas visitadas por los usuarios, para así determinar el uso que le dan a la red de datos, sin embargo la empresa no dispone de ningún software para este objetivo.

1.1.3 SERVICIOS, PROTOCOLOS Y APLICACIONES

1.1.3.1 Servicios

Los servicios configurados en la empresa son: acceso al Internet, correo electrónico, antivirus, DNS, Proxy, directorio activo, base de datos, servidor Web, servidor de archivos, servidor de aplicaciones y servidor de respaldos.

Los servicios se encuentran distribuidos en los servidores de la siguiente manera, ver Tabla 1.6.

Tabla 1.6 Servicios en la Red LAN

Servidor	Aplicaciones	Servicios
SPYRALBDD	MSSQL 2000	Base de Datos
Server-Carlink	Microsoft Access 2003	
Skycontrol	SMS-Sistema	Servidor de Aplicaciones
Sincronización	Sincronizador-BDD Control de Llamadas	
ADMINISTRACION	-----	DNS
	-----	Directorio Activo
	Symantec Norton 2006 E.E.	Servidor de Antivirus
	Lotus Domino 5.6.0.1	Servidor de Correo
	-----	Servidor de Archivos
WRTSQL SQL-UIO-01 (Respaldo)	MSSQL 2000	Base de Datos
SRVWEB IIS (Respaldo)	Sitio Web	Servidor WEB
SRVPORTA	Symantec Norton 2006 E.E.	Servidor de Antivirus
	-----	Servidor de Respaldos
	MySQL 5.0	Base de Datos
	UnitData SMS-Sistema GPRS-Sistema	Servidor de Aplicaciones
CLUSTER1	-----	DNS
	-----	Directorio Activo
	-----	Servidor de Archivos
Proxy-GYE	Squid 2.5	Servidor Proxy

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.3.1.1 Acceso al Internet

El proveedor del servicio de Internet es la telefónica Movistar. La velocidad de transferencia de la conexión de Internet es de 512 Kbps. Únicamente el Departamento de Sistemas y Monitoreo, el jefe de cada departamento y la gerencia disponen de este servicio, cada uno tiene acceso ilimitado al canal.

El acceso al Internet también es compartido con la sucursal de Guayaquil, esto es debido a un enlace de datos directo de fibra óptica que existe entre las dos sucursales, adicionalmente se tiene un servidor Proxy para mejorar el tiempo de respuesta y no saturar el ancho de banda.

Sin embargo, para garantizar el uso eficiente del ancho de banda es necesario instalar un Inspector de Contenidos para el filtrado de páginas Web. A continuación se presenta la utilización del servicio de Internet en la empresa durante el mes de Septiembre/2007, ver Figura 1.4; donde el promedio de consumo es de 320 Kbps, lo que representa el 62,5% del total de ancho de banda contratado.

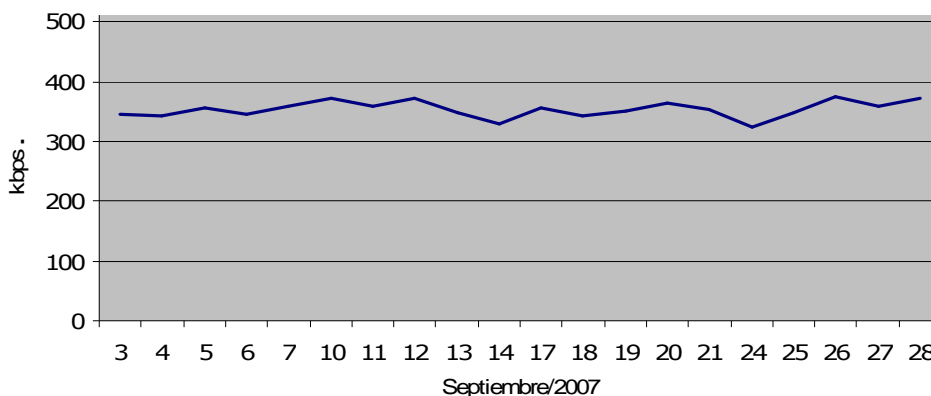


Figura 1.4 Medición del Ancho de Banda

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.1.3.1.2 Correo Electrónico

Es un servicio de la red, permite a los usuarios acceder a una cuenta de correo para el envío y recepción de mensajes de texto o documentos adjuntos, para la

implementación del servicio se utilizó “Lotus Domino 5.6.0.1” como servidor y “Lotus Notes 5.0.9” como cliente.

Las políticas y normas para la utilización de este servicio han sido establecidas y se encuentran en ejecución. En cuanto a la configuración, todos los usuarios tienen la posibilidad de enviar y recibir correo utilizando certificados digitales, esto garantiza la integridad del contenido, evita la suplantación de identidad y permite cifrar el correo, pese a esto es una práctica que se utiliza esporádicamente dentro de la empresa. Los respaldos de la configuración se obtienen cada semana y son realizados por el Jefe de Sistemas.

Existen normas para la creación, actualización y caducidad de las cuentas de usuario, cada cuenta tiene asignado una cuota en el servidor según el perfil de usuario, y un límite (5 MB) en el tamaño de los archivos que pueden ser adjuntados.

No se ha podido implantar un filtro contra el correo basura (SPAM) lo que causa que los buzones de correo se llenen prematuramente con información irrelevante. Este servicio reside en el servidor “ADMINISTRACIÓN”.

1.1.3.1.3 Antivirus

La empresa utiliza el antivirus “Norton Enterprise Edition 2006”, que permite bloquear la entrada o salida de virus provenientes del Internet, correo electrónico, y dispositivos de almacenamiento portátiles. Las actualizaciones inicialmente se descargan en un servidor principal, para después de forma automática actualizar a todos los equipos que tienen instalado la versión cliente del antivirus.

Los equipos están programados para actualizar y ejecutar un escaneo de su sistema antes de la hora de entrada de los usuarios, todos los días a tempranas horas de la mañana. Este servicio reside en el servidor “ADMINISTRACION” para la subred de administración y en el servidor “SRVPORTA” para la subred de monitoreo.

1.1.3.1.4 DNS

Existen 2 servidores de nombres, el primer servidor es “ADMINISTRACIÓN”, que se encuentra bajo el sistema operativo Microsoft Windows 2000 y resuelve los nombres para la subred administrativa, el segundo servidor es “CLUSTER1”, que se encuentra bajo el sistema operativo Microsoft Windows 2000 Advanced Server y resuelve los nombres para la subred de monitoreo.

1.1.3.1.5 Directorio Activo

La empresa ha implementado el servicio de directorio activo, el cual almacena información acerca de los recursos de la red y permite el acceso de los usuarios y las aplicaciones a dichos recursos, de forma que se convierte en un medio para organizar, controlar y administrar centralizadamente el acceso a los recursos de la red. Una de las ventajas fundamentales del directorio activo es que separa la estructura lógica (dominios) de la estructura física (topología de red) de la empresa.

El servicio de directorio activo reside en los servidores “ADMINISTRACIÓN” y “CLUSTER1” y establecen los dominios: *carlink.com* para la red administrativa y *wrtavl.local* para la red de monitoreo respectivamente.

1.1.3.1.6 Base de Datos

La empresa utiliza los siguientes motores de base de datos: MSSQL Server, MySQL y MSAccess, y se utilizan para las aplicaciones institucionales: Spyrall, SMS-Sistema, GPRS-Sistema y Control de Asistencia. La administración de cada uno de los motores de base de datos esta a cargo del Jefe de Sistemas.

La base de datos principal de la empresa reside en el servidor “SQL-UIO-01” donde se guarda la información de los dispositivos instalados en los vehículos, debido a la importancia de esta información se mantiene siempre disponible un servidor de base de datos de respaldo llamado “WRTSQL”.

Los servidores donde se encuentran instaladas las base de datos son: “SPYRALBDD”, “Server-Carlink”, “WRTSQL”, “SQL-UIO-01” y “SRVPORTA”.

1.1.3.1.7 Servidor Web

Aloja a la página Web principal de la empresa y permite a los clientes acceder a los servicios de seguridad y control vehicular. La empresa posee dos servidores, el “SRVWEB” es el principal, mientras el “IIS” se lo mantiene como respaldo.

1.1.3.1.8 Servidor de Archivos

Permite centralizar la gestión de la información y los recursos de las redes, se realiza desde los servidores “ADMINISTRACIÓN” y “CLUSTER1” para la red Administrativa y de Monitoreo respectivamente. Frecuentemente se utiliza para mantener software utilitario y demás herramientas utilizadas por el Departamento de Sistemas en la red, comparte su espacio con el directorio activo.

1.1.3.1.9 Servidor Proxy

Únicamente se tiene instalado un servidor Proxy (Proxy-GYE) para la conexión con la sucursal de Guayaquil, ya que esta comparte el acceso al Internet con la sucursal en Quito. Estos equipos los provee la empresa “Telconet”.

1.1.3.1.10 Servidor de Aplicaciones

Existen 3 servidores de aplicaciones: “SRVPORTA”, “Skycontrol” y “Sincronización”, que mantienen los sistemas: UnitData, SMS-Sistema, GPRS-Sistema, Control de llamadas y Sincronizador-BDD disponibles para la red.

1.1.3.1.11 Servidor de Respaldos

Se almacenan los respaldos de la red de monitoreo de forma temporal, aproximadamente por un mes, hasta que se genera el respaldo en un disco de almacenamiento óptico. Este servicio reside en el servidor “SRVPORTA”.

1.1.3.2 Protocolos

Los protocolos más utilizados en la red de la empresa de acuerdo al escaneo realizado, ver Figura 1.3 y al Modelo de Referencia TCP/IP son:

- Nivel de red:
 - **IP (Internet Protocol)**.- Usado para la comunicación entre equipos (origen y destino) a través de la red interna y externa de la empresa.
 - **ICMP (Internet Control Message Protocol)**.- Usado principalmente por los routers (Cisco 805 y 1601 R) para el envío de mensajes de error y de control hacia otros routers y al servidor Administración.
- Nivel de transporte:
 - **TCP (Transmission Control Protocol)**.- Permite a los usuarios internos transferir ficheros entre los equipos de la red, además es utilizado para la descarga y subida de archivos a la Internet.
 - **UDP (User Datagram Protocol)**.- Usado principalmente por las aplicaciones, ver sección 1.1.3.3 para transmitir mensajes sobre la red hacia un host que necesita identificar su destino.
- Nivel de aplicación:
 - **HTTP (HyperText Transfer Protocol)**.- Utilizado para la transferencia de hipertexto entre dos dispositivos de la red.
 - **SMTP (Simple Mail Transfer Protocol)**.- Utilizado en el servicio de Correo Electrónico, ver sección 1.1.3.1.2; para el intercambio de mensajes escritos (E-mail).
 - **SNMP (Simple Network Management Protocol)**.- Facilita el intercambio de información entre los equipos de la red y permite al administrador supervisar el desempeño de la misma.
 - **POP3 (Post Office Protocol)**.- Utilizado en los clientes locales para obtener los mensajes de correo electrónico almacenados en el servidor Administración.
 - **FTP (File Transfer Protocol)**.- Permite la transferencia de archivos entre los equipos de la red desde un lugar “local” a uno “remoto” o viceversa.

1.1.3.3 Aplicaciones

A continuación se describen las aplicaciones implementadas por el personal interno para la automatización de la empresa, a excepción del sistema de facturación que fue desarrollado por consultores externos.

1.1.3.3.1 *Spyral*

Sistema utilizado para las tareas de facturación dentro de la empresa, ver Figura 1.5. La información recolectada se guarda en el equipo “SPYRALBDD”, que utiliza como base de datos MSSQL.



Figura 1.5 Sistema de Facturación

Fuente: CARLINK. Unidad Informática. Quito. Septiembre/2007.

1.1.3.3.2 *Skybase III*

Sistema utilizado por el personal interno para los servicios: Roadlink, Tracklink y Transtrack, ver Figura 1.6. Permite la localización y paralización de los vehículos, despliega su ubicación en mapas virtuales, facilita la apertura remota de puertas y genera reportes de recorrido.

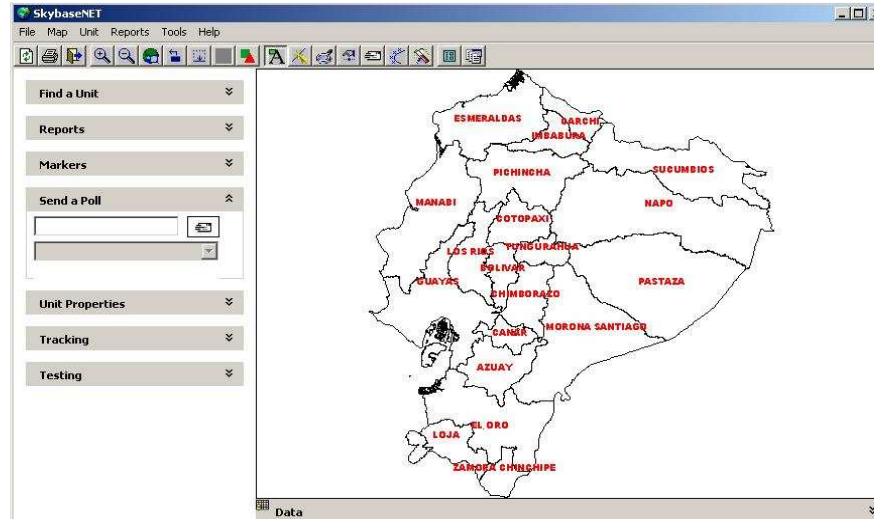


Figura 1.6 Sistema Skybase III

Fuente: CARLINK. Unidad Informática. Quito. Septiembre/2007.

1.1.3.3.3 Sincronizador-BDD

Utilizado para sincronizar las BDD de Quito y Guayaquil. El servidor de base de datos que se sincroniza en la sucursal de Quito es el "SPYRALBDD" que mantiene la información de los clientes.

1.1.3.3.4 Carlink

Sistema utilizado por los operarios de monitoreo para el servicio de seguridad vehicular "Carlink", ver Figura 1.7. Diseñado con el propósito de paralizar el vehículo y permitir la apertura remota de puertas.

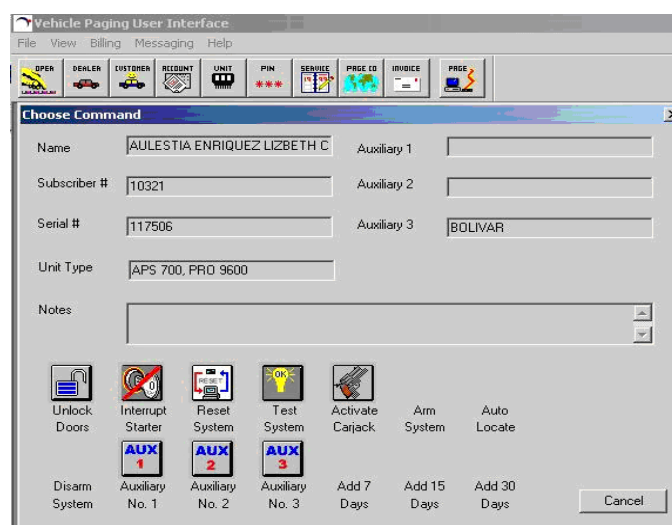


Figura 1.7 Sistema Carlink

Fuente: CARLINK. Unidad Informática. Quito. Septiembre/2007.

1.1.3.3.5 UnitData

Sistema utilizado para generar reportes de la ubicación de los vehículos, ver Figura 1.8. Se encuentra en el equipo “SRVPORTA” y utiliza la información recolectada en la base de datos MySQL.

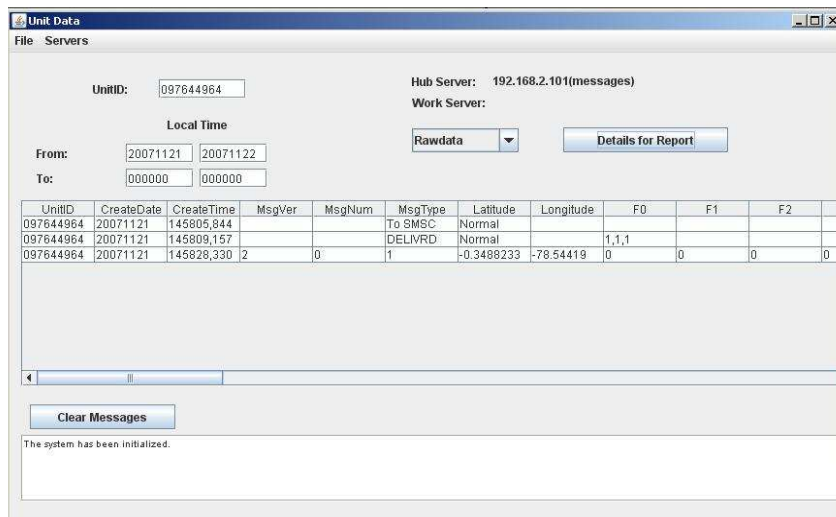


Figura 1.8 Sistema UnitData

Fuente: CARLINK. Unidad Informática. Quito. Septiembre/2007.

1.1.3.3.6 SMS-Sistema, GPRS-Sistema

Sistemas utilizados para posicionar a los vehículos en mapas digitales, mediante la interpretación de las señales enviadas por los dispositivos a través de las operadoras celulares, ver Figura 1.9. Se encuentran instaladas en los equipos “Skycontrol” y “SRVPORTA” para Movistar y Porta, respectivamente.

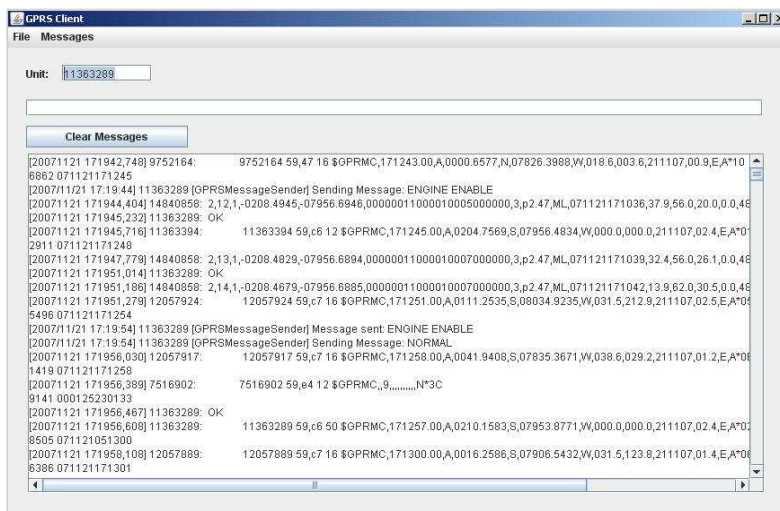


Figura 1.9 GPRS-Sistema

Fuente: CARLINK. Unidad Informática. Quito. Septiembre/2007.

1.1.3.3.7 Sitio Web

Mantiene la imagen corporativa de la empresa y permite el acceso a los servicios “Tracklink” y “Transtrack”, ver Figura 1.10. Se mantiene instalado en el equipo “SRVWEB”.



Figura 1.10 Página Web de la Empresa

Fuente: CARLINK. <http://www.carlink.com.ec>. Septiembre/2007.

1.1.3.3.8 Control de llamadas

Sistema centralizado de llamadas, desarrollado por el personal interno de la empresa. Se encuentra instalado en el equipo “Sincronización”.

1.1.3.3.9 Control de Asistencia

Sistema que registra la entrada y salida de los empleados, permite generar reportes de asistencia, horas de entrada y salida, total de horas trabajadas y el cálculo de las multas. Se encuentra instalado en un equipo en el Departamento de Recursos Humanos.

1.1.4 ADMINISTRACIÓN DE LA RED

1.1.4.1 Gestión de Hardware

Todos los equipos de computación se someten a un mantenimiento preventivo cada 4 meses, con el fin de conservar un rendimiento óptimo para el desarrollo de las actividades dentro de la empresa. El mantenimiento correctivo de los equipos de computación, UPS's, además de todo lo referente al cableado es realizado inicialmente por los asistentes de sistemas, sin embargo si el daño no puede ser reparado se contacta con los proveedores o se envía el equipo a reparaciones.

Los servidores se encuentran a cargo exclusivo de la empresa "Compuequip DOS" la cual mantiene una alianza estratégica con "Hewlett Packard", para el asesoramiento y soporte técnico requerido.

1.1.4.2 Gestión de Software

El desarrollo y manejo de versiones del software institucional es realizado por los asistentes de sistemas. La instalación del software se realiza utilizando CD's, DVD's o distribuyendo los instaladores a través del servidor de archivos.

Para mantener un inventario detallado del hardware y software instalado en los equipos de computación se utiliza el software "Belarc Advisor 7.2".

1.1.4.3 Gestión de Usuarios

Todas las cuentas de usuario utilizadas para la inicialización y autenticación de sesiones en los equipos de computación son administradas con Active Directory en la plataforma Windows Server 2000, esto permite que el Jefe de Sistemas sea el único responsable de crear, modificar, deshabilitar y eliminar una cuenta de usuario en el sistema.

Las características principales de las cuentas de usuario son:

- El login de la cuenta esta formada por la primera letra del nombre seguido del apellido del usuario, por ejemplo *epazminio*.
- Al crear una cuenta la contraseña inicial es *invitadoa*, cuando el usuario abre su correo por primera vez tiene un mensaje indicándole que debe cambiar la contraseña por su seguridad.
- Cada usuario debe cambiar obligatoriamente la contraseña cada 3 meses, sino lo recuerda el computador despliega un mensaje de cambio de contraseña.
- Existen políticas y normas acerca de la estructura de las contraseñas

1.1.4.4 Plan de Respaldos

Se contemplan los siguientes criterios:

- La información crítica de la red de monitoreo es respaldada todos los días, mientras en la red administrativa se lo realiza pasando un día.
- Toda esta información es almacenada al final del mes en DVD's (2 copias) y en el servidor de respaldos, cada respaldo es verificado y etiquetado para garantizar su disponibilidad para futuras contingencias.
- La persona encargada de la administración de los respaldos, es el Jefe de Sistemas, sin embargo quienes generan y verifican los respaldos son los asistentes de sistemas.

1.1.4.5 Políticas de seguridad

- La empresa mantiene un documento de "Políticas de Seguridad" que no se encuentra basado en un estándar; donde se detallan únicamente normas de seguridad, las cuales han sido difundidas a todo el personal involucrado para su aplicación.

1.2 DIAGNÓSTICO DE VULNERABILIDADES Y AMENAZAS DE LA RED DE TRANSMISIÓN DE DATOS.

1.2.1 METODOLOGÍA PARA UN TEST DE INTRUSIÓN

Para una correcta determinación de vulnerabilidades y amenazas de la red de transmisión de datos, se ha tomado como base la metodología llamada “Penetration Testing Methodology”⁴, que establece un procedimiento estructurado que actúa como base para realizar y ejecutar un test de intrusión específico.

Fue desarrollado por “la Oficina Federal para la Seguridad de la Información” (“Bundesamt für Sicherheit in der Informationstechnik“- BSI), que se encarga de proveer el servicio de seguridad en tecnologías de la información para el gobierno Alemán. Fue Publicada el 21 de septiembre del 2005, y servirá como base para el desarrollo del presente proyecto de titulación. La descripción completa de la metodología se detalla en el Anexo 1.

1.2.1.1 Objetivos y Clasificación

1.2.1.1.1 Objetivos

Para un test de intrusión acertado que resuelva las expectativas de la empresa, una definición clara de los objetivos es absolutamente esencial. Los objetivos que pueden ser logrados ejecutando el test de intrusión, se pueden agrupar en 4 categorías:

- Mejorar la seguridad de los sistemas
- Identificar las vulnerabilidades
- Alcanzar una seguridad confirmada por terceras personas
- Mejorar la seguridad del personal y de la infraestructura de la empresa

⁴ <http://www.bsi.de/english/publications/studies/penetration.pdf>

1.2.1.1.2 Clasificación

La caracterización de un test de intrusión nos permite satisfacer los objetivos de la empresa, asegurar la eficiencia y la eficacia manteniendo un riesgo calculado.

A continuación se muestra la clasificación de un test de intrusión, ver Figura 1.11; a la izquierda se encuentran seis criterios para definir el test y a la derecha tenemos los valores para cada criterio.

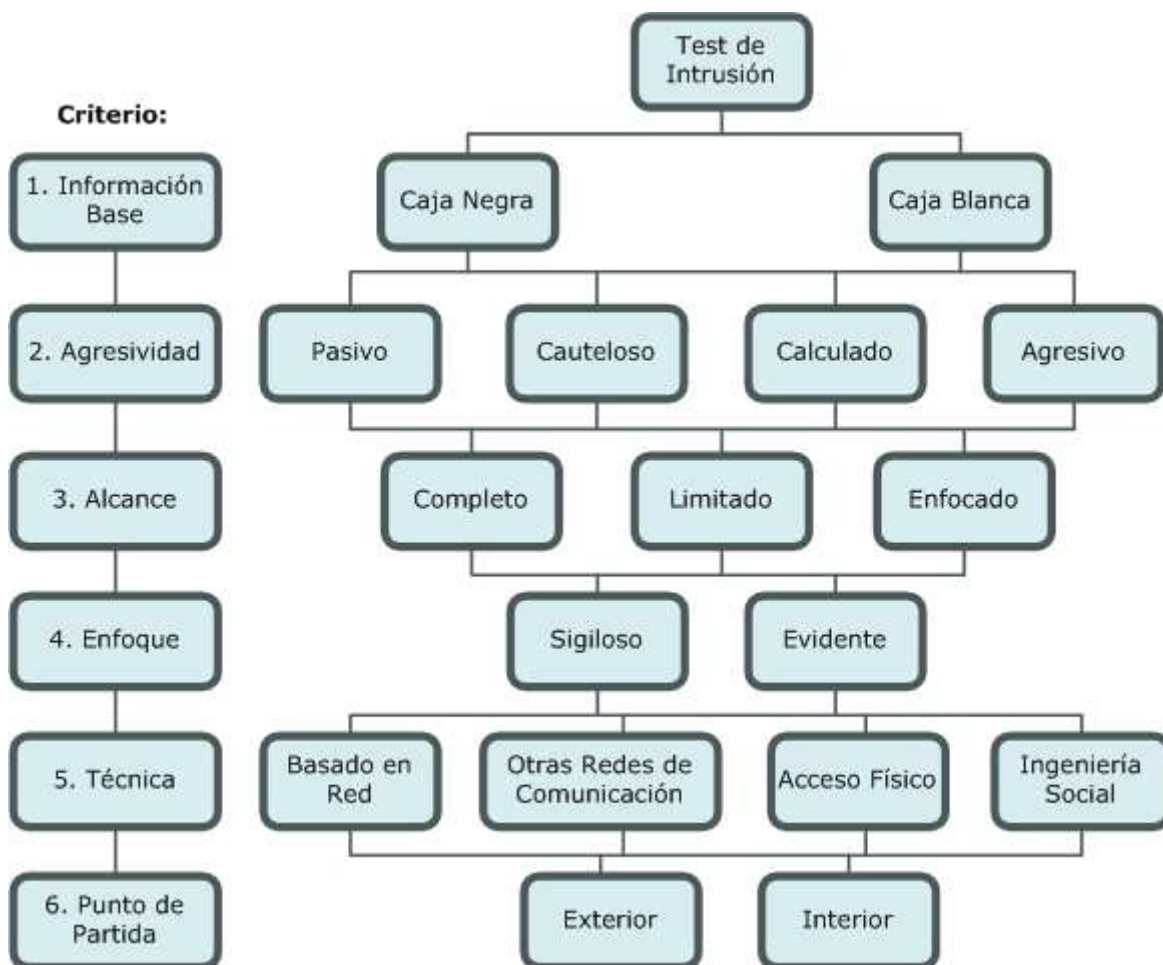


Figura 1.11 Clasificación General de un Test de Intrusión

Fuente: Penetration Testing Methodology.
<http://www.bsi.de/english/publications/studies/penetration.pdf>. Septiembre/2005.

Se debe notar que no todas las combinaciones posibles son pruebas útiles, por ejemplo un test agresivo se identifica generalmente muy rápido y no es ideal en combinación con un enfoque sigiloso.

Los 6 criterios con sus respectivos valores se describen en el Anexo 1.

1.2.1.2 Fases

A continuación se describen las 5 fases del test de intrusión.

1.2.1.2.1 Fase 1: Preparación

Al inicio del test de intrusión los objetivos y el alcance deben ser aclarados y definidos con la empresa. El tester debe por lo tanto asegurarse de que los riesgos asociados a las técnicas utilizadas hayan sido discutidos y/o documentados.

1.2.1.2.2 Fase 2: Reconocimiento

El tester inicia la recopilación de información acerca del objetivo. Esta fase también se conoce como test de intrusión pasivo. Esta dirigido a obtener una descripción 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 (router y firewall) e investigación de vulnerabilidades, incluyendo áreas abiertas a un ataque o defectos conocidos en la seguridad. Dependiendo del número de equipos o del tamaño de la red que se examine, el ejecutar cada paso del test puede ser extremadamente demoroso, por lo que el tiempo requerido para ello debe ser considerado en el planeamiento.

1.2.1.2.3 Fase 3: Análisis de Información y Riesgos

El análisis debe incluir la definición de prioridades, evaluación de los riesgos potenciales para el sistema y el tiempo estimado requerido para evaluar los defectos potenciales de seguridad para los posteriores intentos activos de intrusión. Los objetivos de la fase 4 serán seleccionados en base a este análisis. De la lista de los sistemas identificados el tester puede, por ejemplo, elegir probar solamente servicios sobre los cuales el tester está particularmente bien informado.

1.2.1.2.4 Fase 4: Intentos Activos de Intrusión

Finalmente, los sistemas seleccionados son invadidos activamente. Esta fase conlleva el riesgo más alto dentro de un test de intrusión y se debe realizar con el debido cuidado.

Para los sistemas con requerimientos de alta disponibilidad o de integridad, los efectos potenciales podrían ser devastadores por lo que existe la posibilidad de excluir esta fase del test seleccionado.

1.2.1.2.5 Fase 5: Análisis Final

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

1.2.1.3 Enfoque

El planeamiento a realizarse en cada una de las fases del test de intrusión se describe a continuación, ver Figura 1.12.

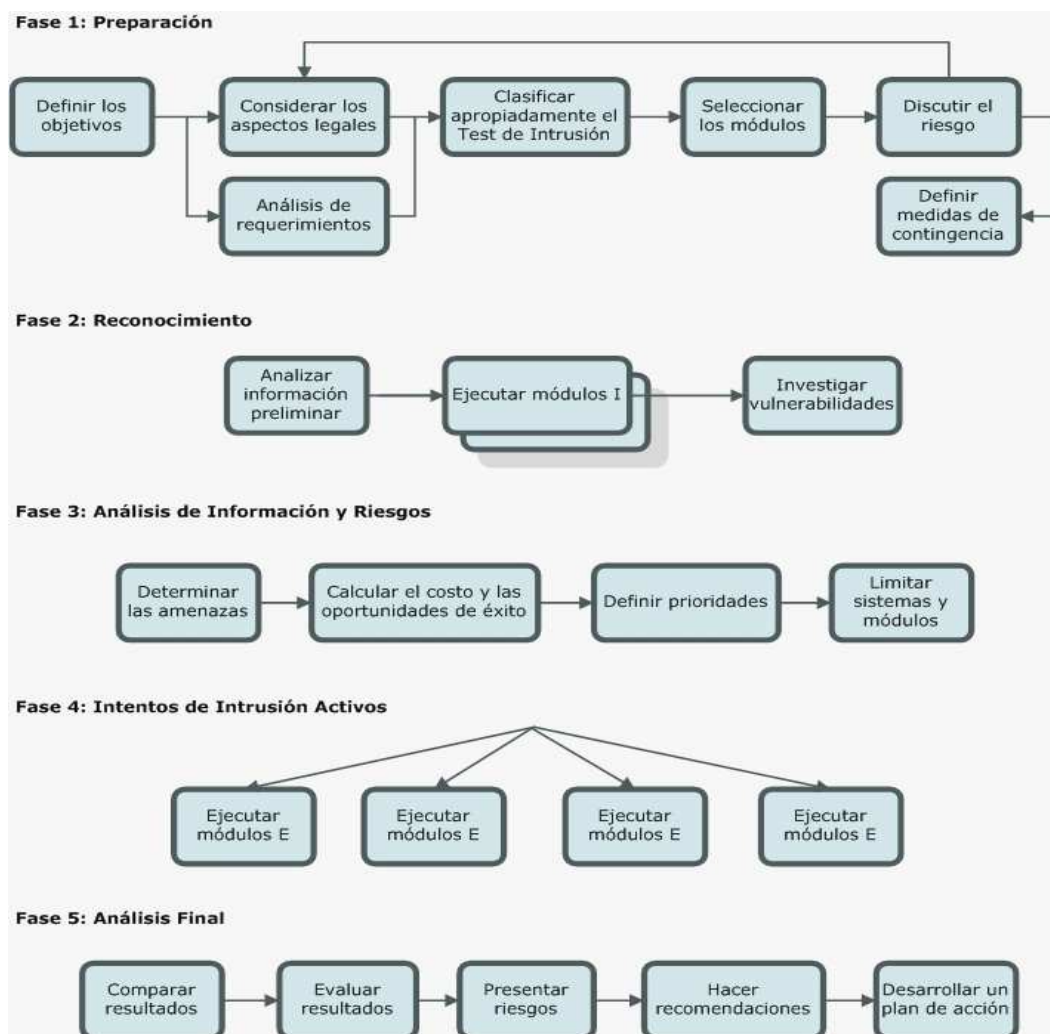


Figura 1.12 Fases del Test de Intrusión

Fuente: Penetration Testing Methodology.
<http://www.bsi.de/english/publications/studies/penetration.pdf>. Septiembre/2005.

1.2.1.4 Módulos

El enfoque mencionado anteriormente no contiene métodos de prueba explícitos, únicamente menciona la ejecución de los módulos I y E. En base al OSSTMM⁵ los diferentes métodos de prueba han sido agrupados en módulos, los cuales se han dividido en dos clases: módulos I para “Reconocimiento” y módulos E para “Intentos Activos de Intrusión”.

1.2.1.4.1 Módulos de Reconocimiento

La Tabla 1.7 contiene la lista de los módulos del I 1 al I 22 para reconocimiento.

Tabla 1.7 Módulos de Reconocimiento

Nro.	Módulos.
I 1	Análisis de Datos Publicados
I 2	Consulta Sigilosa de Información Básica de la Red
I 3	Consulta Evidente de Información Básica de la Red
I 4	Escaneo Sigiloso de Puertos
I 5	Escaneo Evidente de Puertos
I 6	Identificación de Aplicaciones
I 7	Identificación de Sistemas
I 8	Identificación Sigilosa del Router
I 9	Identificación Evidente del Router
I 10	Identificación Sigilosa del Firewall
I 11	Identificación Evidente del Firewall
I 12	Investigación de Vulnerabilidades
I 13	Identificación de Vulnerabilidades en las Interfaces de Aplicación
I 14	Recolección de Información para Ingeniería Social
I 15	Recolección de Información basada en Informática para Ingeniería Social
I 16	Recolección de Información personal para Ingeniería Social
I 17	Pruebas de Comunicación Inalámbrica
I 18	Pruebas del Sistema Telefónico
I 19	Pruebas del Sistema de Correo de Voz
I 20	Pruebas del Sistema de Fax
I 21	Análisis del Entorno Físico
I 22	Identificación del Control de Acceso

Fuente: Penetration Testing Methodology.
<http://www.bsi.de/english/publications/studies/penetration.pdf>. Septiembre/2005.

⁵ <http://www.isecom.info/mirror/osstmm.en.2.2.pdf>

1.2.1.4.2 Módulos de Intentos Activos de Intrusión

La Tabla 1.8 contiene la lista de los módulos del E 1 al E 23 para intentos activos de intrusión.

Tabla 1.8 Módulos para Intentos Activos de Intrusión

Nro.	Módulos.
E 1	Verificación Sigilosa de Vulnerabilidades Actuales
E 2	Verificación Evidente de Vulnerabilidades Actuales
E 3	Verificación de las Vulnerabilidades Actuales en las Interfaces de Aplicación
E 4	Prueba Sigilosa del Router
E 5	Prueba Evidente del Router
E 6	Prueba de Sistemas Confiados
E 7	Prueba Sigilosa de Firewall desde el Exterior
E 8	Prueba Evidente de Firewall desde el Exterior
E 9	Prueba de Firewall desde Ambos Lados
E 10	Prueba del Sistema de Detección de Intrusos
E 11	Intercepción de Contraseñas
E 12	Descifrado de Contraseñas
E 13	Pruebas de sensibilidad para ataques DoS (Denial of Service)
E 14	Ingeniería Social basado en Informática
E 15	Ingeniería Social directa al Personal con Acceso Físico
E 16	Ingeniería Social indirecta al Personal sin Acceso Físico
E 17	Pruebas de Comunicación Inalámbrica
E 18	Pruebas de Acceso Administrativo al Sistema Telefónico
E 19	Pruebas del Sistema de Correo de Voz
E 20	Pruebas de Puntos de Acceso Administrativo al Sistema de Fax
E 21	Pruebas del MODEM
E 22	Pruebas del Control de Acceso
E 23	Procedimientos para Pruebas de Contención

Fuente: Penetration Testing Methodology.
<http://www.bsi.de/english/publications/studies/penetration.pdf>. Septiembre/2005.

1.2.1.4.3 Principio de Exclusión

De acuerdo con la clasificación seleccionada, los módulos que no pueden ser realizados debido al enfoque elegido se excluyen del test. Si un módulo no se excluye, los pasos de la prueba contenidos en él deben ser realizados, esto ayuda a asegurar un test de intrusión comprensivo.

A continuación se muestra dentro de los paréntesis los módulos que serán excluidos para cada uno de los criterios, ver Figura 1.13.

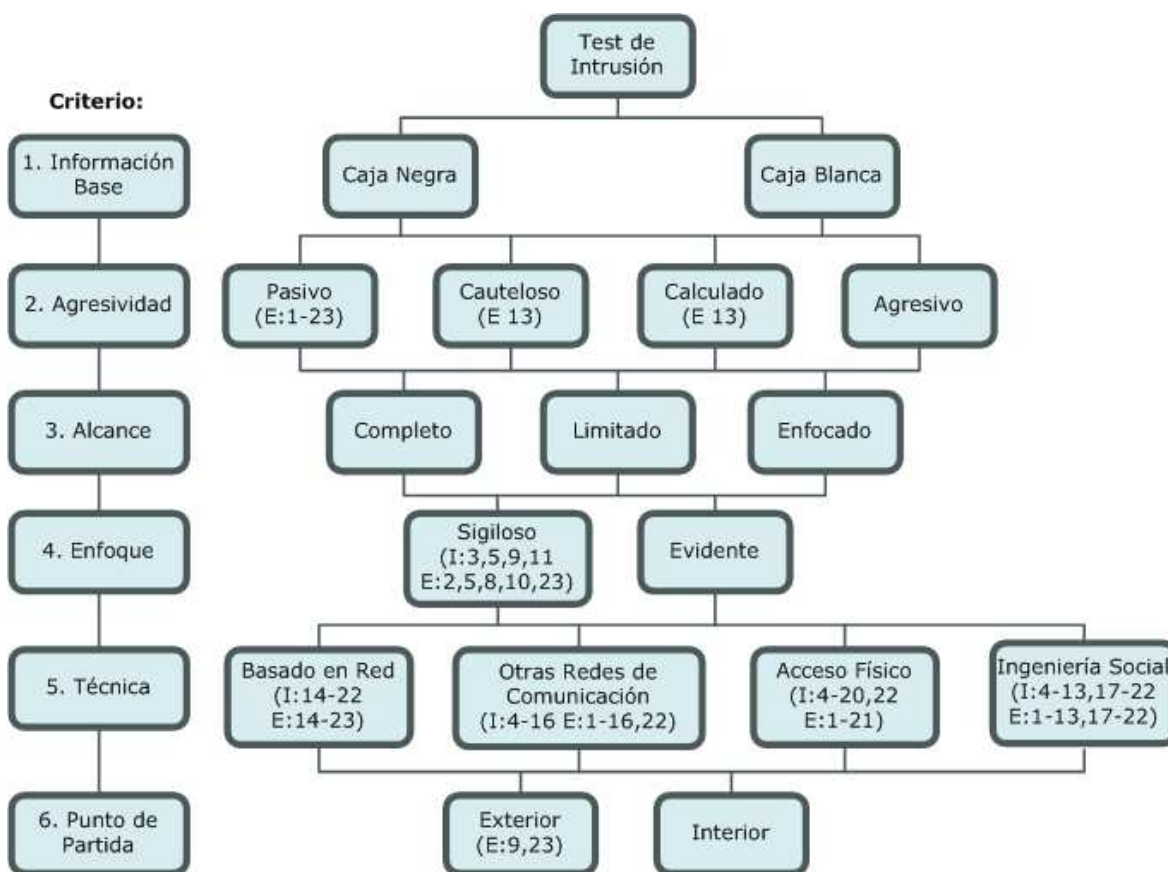


Figura 1.13 Principio de Exclusión

Fuente: Penetration Testing Methodology.
<http://www.bsi.de/english/publications/studies/penetration.pdf>. Septiembre/2005.

1.2.2 EJECUCIÓN DEL TEST DE INTRUSIÓN

En esta sección se ejecutara el test de intrusión presentado anteriormente, por lo cual se realiza una selección de las herramientas de escaneo ha utilizar de acuerdo a los siguientes criterios:

- Instalación y Configuración
- Tipo de distribución
- Facilidad de generar reportes
- Plataforma
- Flexibilidad de la herramienta
- Experiencia en la herramienta
- Adecuada documentación (Ayuda)

Después del análisis entre las herramientas más conocidas y usadas en la ejecución de un Test de Intrusión (escaneo de puertos, banners, identificación de servicios y aplicaciones), ver Anexo 2; se ha seleccionado las siguientes herramientas:

- BackTrack 2.0
- Nmap 4.2
- UnicornScan 0.4.6e
- Amap 5.2
- Xprobe2
- Scaline 1.01
- Ping-Probe 1.1.3

1.2.2.1 Fase 1: Preparación

Los objetivos principales para ejecutar el test de intrusión son:

- Mejorar la seguridad de los servicios Web
- Identificar las vulnerabilidades de los equipos activos de la red
- Alcanzar una seguridad confirmada por terceras personas

Según la clasificación presentada, ver Figura 1.11; apoyados en el principio de exclusión, ver Figura 1.13; y en base a los requerimientos presentados por el Jefe de Sistemas, se ha seleccionado la siguiente propuesta, ver Tabla 1.9; que cubre en su totalidad con los objetivos presentados.

Tabla 1.9 Test de Intrusión Seleccionado

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

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

La posibilidad de que el sistema sea interrumpido o su rendimiento afectado es el principal riesgo asociado con la ejecución del test, por lo cual, se ha considerado ejecutar inicialmente un test "Pasivo", que será confirmado o descartado en la fase 3.

Para la fase de reconocimiento, las medidas de contingencia que se tomaran son:

- El análisis de las vulnerabilidades será realizado durante un tiempo y horario definido, por el tester y el Jefe de Sistemas.
- Las herramientas utilizadas en el test serán ejecutadas inicialmente en una LAN de pruebas, para conocer sus requerimientos y resultados.
- Las vulnerabilidades detectadas y catalogadas como críticas, serán informadas inmediatamente al Jefe de Sistemas.

Para finalizar la fase 1, se detallara los servicios, equipos activos y servidores seleccionados para la aplicación del test de intrusión:

- Sitio Web
- Firewall y Router externo
- Servidor Web y de correo

1.2.2.2 Fase 2: Reconocimiento

Definidos los objetivos, el alcance y discutidos los riesgos asociados con el test, se procederá a ejecutar los módulos I sin un orden definido, sin embargo antes de ejecutar el módulo I 12, todos los anteriores deben estar completos.

1.2.2.2.1 I 1. Análisis de Datos Publicados

El tester trata de obtener tanta información como sea posible. La información que se busca es acerca de la empresa, sus empleados y la tecnología usada.

Resultados Esperados:	Perfil de la empresa
------------------------------	----------------------

Pasos de Prueba:

- Buscar información en la página inicial de la empresa

La dirección Web de la página inicial de la empresa es <http://www.carlink.com.ec>, la información presentada esta relacionada con los servicios brindados tanto para seguridad vehicular como para control vehicular, cada uno de estos servicios ha sido detallado en la sección 1.1.1.6, adicionalmente existe un sistema de autenticación que permite a los clientes acceder a estos servicios vía Web.

- Investigar información relevante en los grupos de noticias

No existe información relacionada con la empresa en los diferentes grupos de noticias, tales como:

- <http://www.elcomercio.com/>
- <http://www.hoy.com.ec>
- <http://www.eluniverso.com/>

- Investigar en bases de datos públicas

La información disponible respecto a los socios de la empresa, en bases de datos públicas tales como <http://www.google.com.ec> y <http://www.yahoo.com>, es:

“**Black Box Ecuador**”⁶.- organización dedicada al desarrollo de contenidos multimediales para Internet y sitios Web. Se encargo del diseño de la interfaz del sistema de ubicación vehicular GPS, y del rediseño del sitio Web corporativo.

“**Aurora Soluciones Integrales**”⁷.- empresa especializada en el desarrollo de productos para sincronización de datos y transacciones móviles. Realizo la sincronización e integración de sucursales Carlink con “i-Connector Suite”.

1.2.2.2.2 I2. Consulta Sigilosa de Información Básica de la Red

Resultados Esperados:	Nombres de dominio Nombres de host Direcciones IP Descripción de los servidores Información del ISP Contacto administrativo (admin.-c)
------------------------------	---

Requerimientos

- Direcciones IP/Rango IP o dominios/Nombres del servidor

La consulta se inicia a partir del dominio “carlink.com.ec”.

Pasos de Prueba:

- Consultar en bases de datos Whois

Inicialmente las consultas se realizaran a través de las distintas páginas Web que prestan este servicio:

- <http://samspade.org/whois/carlink.com.ec>
 carlink.com.ec = [200.24.213.174]
 WEB: No compatible whois server exists for this domain.
 Please try http://www.nic.ec/consulta/whois.asp
 for more information.
 See also http://www.IANA.org/root-whois/ec.htm
- <http://www.dnsstuff.com/tools/whois.ch?ip=carlink.com.ec>
 Generated by www.DNSstuff.com
 Sorry, Ecuador doesn't have a WHOIS server.
 Try [Clicking](#) here, or wait for me to redirect you...

Las consultas muestran que la única página que nos puede dar información es <http://www.nic.ec>, el resultado se presenta a continuación, ver Tabla 1.10.

⁶ <http://www.blackbox.ec/bbe/>

⁷ <http://www.aurorasi.com>

Tabla 1.10 Whois del Dominio “carlink.com.ec”

Registrante:	
Audio Auto S.A.	
Alvaro Samper Quevedo	carlink@interactive.net.ec
Telf:59322-439945	
Fax:59322-439920	
Paris 200 y Gaspar de Villaroel	
Quito, Pichincha,	
Ecuador	
Nombre de Dominio: carlink.com.ec	
Contacto Administrativo, Contacto Técnico y Contacto de Facturación	
Otecel S.A. - Movistar	
Yomar Mera	nsadm@telefonica.com.ec
Telf: 5932-2227700	
Fax: 5932-2227597	
Av. República y Pradera Esquina, Edf. Movistar	
Quito, Pichincha, 1717792	
Ecuador	
Fecha de expiración del dominio:	17-Junio-2008
Fecha de creación del dominio:	17-Junio-2002
Fecha de última modificación del registro:	18-Junio-2007
Nombres de dominios DNS listados en orden:	
dns1uio.cyberweb.net.ec	200.24.208.2
dns2gye.cyberweb.net.ec	200.24.194.83
dns2uio.cyberweb.net.ec	200.24.208.1

Fuente: Consulta Whois.
<http://www.nic.ec/reg/whois.asp?dominio=carlink.com.ec>. Septiembre/2007.

- Consultar al servidor de nombres

El comando “nslookup” permite realizar consultas directamente contra el servidor de nombres (DNS), para ejecutar este comando se utiliza la consola de Windows, el detalle completo de la consulta a cada DNS se encuentra en el Anexo 3. Entre la información destacada tenemos, ver Tabla 1.11.

Tabla 1.11 Nslookup – Dominio “carlink.com.ec”

<i>Tipo</i>	<i>Datos</i>
Nombre del servidor DNS primario para la zona	uio.carlink.com.ec
Dirección de correo del responsable de la zona	nsadm@bellsouth.com.ec
DNS con “autoridad” sobre el dominio especificado	dns1uio.cyberweb.net.ec - 200.24.208.2 dns2gye.cyberweb.net.ec - 200.24.194.83
Servidor de correo	carlink.com.ec
Registro de direcciones	carlink.com.ec - 200.24.213.174
	www - 200.24.208.181

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

- Examinar las cabeceras de los correos electrónicos

Las cabeceras de correo son líneas de texto insertadas automáticamente por el software que envía el correo y por cada uno de los servidores de correo por los que va pasando hasta llegar al buzón destino. Si no han sido manipuladas, únicamente nos muestra la lista de los equipos por los que el mensaje ha pasado.

A continuación analizaremos dos tipos de correo, el primero enviado desde la cuenta epazmino@carlink.com.ec, a través del cliente de correo interno:

```
X-Apparently-To: sandra_maigua@yahoo.com via 206.190.49.175; Tue, 06 Feb
2007 10:54:57 -0800
X-YahooFilteredBulk: 200.24.213.174
X-Originating-IP: [200.24.213.174]
Authentication-Results: mta164.mail.re3.yahoo.com from=carlink.com.ec;
domainkeys=neutral (no sig)
Received: from 200.24.213.174 (EHLO administracion.carlink.com.ec)
(200.24.213.174)
  by mta164.mail.re3.yahoo.com with SMTP; Tue, 06 Feb 2007 10:54:57 -0800
Subject: URGENTE
To: sandra maigua <sandra_maigua@yahoo.com>
X-Mailer: Lotus Notes Release 5.0.9a January 7, 2002
Message-ID: <OF96CF9FB5.6CC6B5EA-ON0525727A.0067AEC6-
0525727A.0067BF9A@carlink.com.ec>
From: epazmino@carlink.com.ec
Date: Tue, 6 Feb 2007 13:53:12 -0500
X-MIMETrack: Serialize by Router on administracion/Carlink(Release 5.0.9
|November 16, 2001) at 06/02/2007 13:53:14
```

El segundo, enviado desde la cuenta esthela_pazmar@hotmail.com, a través del servicio de correo que presta Hotmail.

```
X-Apparently-To: jackbriel@yahoo.com.mx via 209.191.85.53; Mon, 12 Mar
2007 11:03:43 -0700
X-Originating-IP: [65.54.246.168]
Authentication-Results: mta360.mail.re4.yahoo.com from=hotmail.com;
domainkeys=neutral (no sig)
```

Received: from 65.54.246.168 (EHLO bay0-omc2-s32.bay0.hotmail.com) (65.54.246.168)
 by mta360.mail.re4.yahoo.com with SMTP; Mon, 12 Mar 2007 11:03:42 -0700
 Received: from hotmail.com ([65.55.154.111]) by bay0-omc2-s32.bay0.hotmail.com with Microsoft SMTPSVC(6.0.3790.2668);
 Mon, 12 Mar 2007 10:59:05 -0700
 Received: from mail pickup service by hotmail.com with Microsoft SMTPSVC;
 Mon, 12 Mar 2007 10:59:05 -0700
 Message-ID: <BAY143-F31F97ACBA9DEE6AB2B0F74E77D0@phx.gbl>
 Received: from 65.55.154.123 by by143fd.bay143.hotmail.msn.com with HTTP;
 Mon, 12 Mar 2007 17:59:04 GMT
X-Originating-IP: [200.24.213.171]
 X-Originating-Email: [esthela_pazmar@hotmail.com]
 X-Sender: esthela_pazmar@hotmail.com
 From: =?iso-8859-1?B?RXN0aGVsYSBQYXptaFV?=<esthela_pazmar@hotmail.com>
 To: sandra_maigua@yahoo.com
 Cc: jackbriel@yahoo.com.mx
 Bcc:
 Subject: URGENTE
 Date: Mon, 12 Mar 2007 17:59:04 +0000
 X-OriginalArrivalTime: 12 Mar 2007 17:59:05.0152 (UTC)
 FILETIME=[1FB8AC00:01C764D0]
 X-Antivirus: AVG for E-mail 7.5.476 [269.11.19/953]
 Mime-Version: 1.0

Al examinar la cabecera de los correos recibidos, en particular los campos "X-Originating-IP", "X-Mailer", y el "Received" inicial concluimos que: la dirección IP real del servidor de correo es 200.24.213.174 y el equipo se llama "administración.carlink.com.ec", el cliente de correo utilizado es "Lotus Notes 5.0.9a" y la dirección IP real del firewall es 200.24.213.171.

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

A continuación se presenta el código fuente de <http://www.carlink.com.ec>:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-
8859-1">
<title>Carlink - Sistema de Control Vehicular</title>
<script language="JavaScript" type="text/JavaScript">
<!--
function MM_goToURL() { //v3.0
var i, args=MM_goToURL.arguments; document.MM_returnValue = false;
for (i=0; i<(args.length-1);
i+=2) eval(args[i]+".location='"+args[i+1]+'");
}
//-->
</script>
</head>
```

```

    <body
onLoad="MM_goToURL('parent','http://200.24.213.164/Carlink/sistema/tracklink/cv
tracklink.aspx');return document.MM_returnValue">
    </body>
</html>

```

En la página principal existe un script que tiene la función de redireccionar el acceso hacia el servidor Web de la empresa (IP: 200.24.213.164). En el browser la dirección que se muestra es la siguiente:

<http://200.24.213.164/Carlink/carlinkmain.aspx?ReturnUrl=%2fCarlink%2fsistema%2ftracklink%2fcvtracklink.aspx>.

Para analizar la nueva dirección se utiliza el software “Trellian SiteMapper 2.0”, que examina el contenido del sitio Web, creando una lista detallada de todos los recursos, validando links y enlaces externos. Entre la información destacada tenemos que el directorio en el servidor Web es <http://200.24.213.164/Carlink>, la página inicial es “carlinkmain.aspx”, no existen comentarios y el único enlace externo es a <http://www.carlink.com.ec>, más información se detalla en el Anexo 4.

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

No existen ofertas de puestos de trabajo en tecnologías de la información relacionadas con la empresa. Se buscó esta información en las siguientes páginas Web:

- <http://www.multitabajos.com>
- <http://www.porfinempleo.com>
- <http://www.computrabajo.com.ec>
- <http://www.miquiacomercial.com>

1.2.2.2.3 I 4. Escaneo Sigiloso de Puertos

Se ejecuta un escaneo sigiloso de puertos en todos los dispositivos identificados para conocer los servicios que ofrecen.

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 o imposible de detectar, Ej. fijando parámetros apropiados cuando se usa las herramientas de escaneo o haciendo consultas con intervalos prolongados.

El escaneo de puertos es el proceso de analizar por medio de software el estado de los puertos de un equipo conectado a una red de comunicación, con el fin de identificar el sistema operativo y las aplicaciones del sistema. Se utiliza principalmente los protocolos TCP, UDP e ICMP y la manipulación de las banderas de la cabecera TCP.

El estado de un puerto se puede definir como:

Abierto.- acepta conexiones, hay una aplicación escuchando en este puerto. Esto no quiere decir que se tenga acceso, sino que existe la posibilidad de conectarse.

Cerrado.- se rechaza la conexión. Probablemente no hay una aplicación escuchando en este puerto, o no se permite el acceso por alguna circunstancia.

Filtrado.- no hay respuesta, normalmente este comportamiento se debe a la existencia de un firewall.

A continuación se muestra la clasificación según el tipo de escaneo de puertos, ver Figura 1.14.

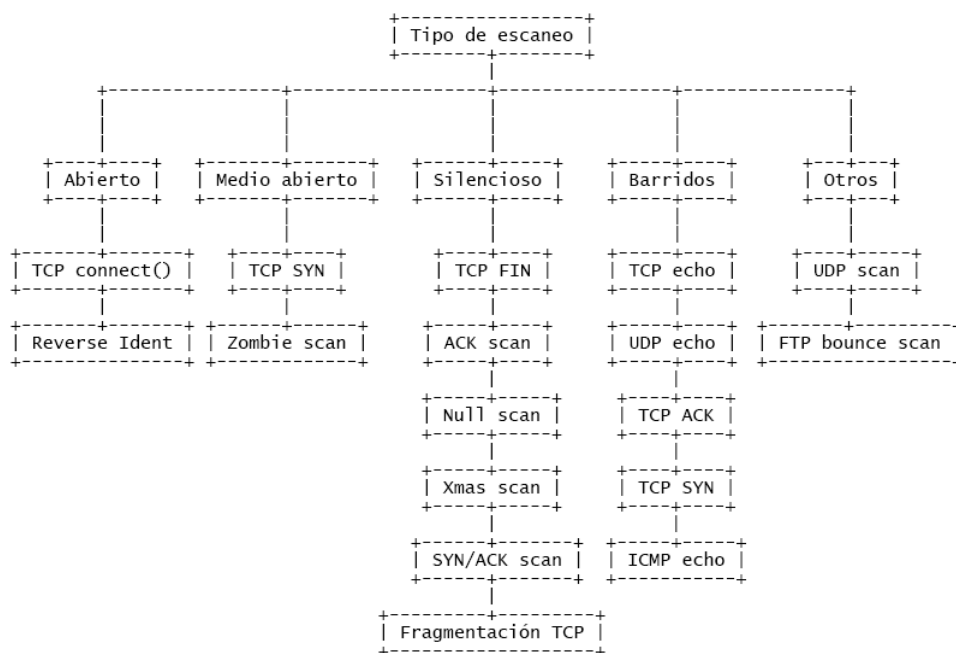


Figura 1.14 Clasificación Según el Tipo de Escaneo de Puertos

Fuente: El escaneo de puertos.

<http://www.telefonica.net/web2/thedeathmaster/articulos/sabuesos/Sabuesos.pdf>, pág. 12. Septiembre/2007.

En el Anexo 5 se describen los tipos de escaneo considerados: abierto, medio abierto y silencioso/sigiloso.

Conocidos los distintos tipos de escaneo, el proceso de análisis de puertos se establece de la siguiente manera: inicialmente se ejecuta el escaneo del tipo medio abierto (TCP SYN), seguido del escaneo del tipo silencioso (TCP FIN, ACK, Null, Xmas), y finalmente se realiza el escaneo UDP.

Para ejecutar el escaneo se utilizara las herramientas “Nmap 4.2”⁸ y “UnicornScan 0.4.6e”⁹, se escanearán la totalidad de puertos existentes (65536) para TCP y UDP.

A continuación se muestra la información destacada de cada uno de los objetivos, ver Tabla 1.12; los puertos no mencionados, así como los tipos de escaneo ACK, Null y Xmas han sido filtrados para todos los casos.

El resultado completo del escaneo se muestra en el Anexo 6.

⁸ <http://download.insecure.org/nmap/dist/nmap-4.20-setup.exe>

⁹ <http://www.unicornscan.org/releases/unicornscan-0.4.6e.tar.gz>

Tabla 1.12 Escaneo Sigiloso de Puertos

Servidor Web					
Protocolo	Puerto	Servicio	TCP SYN	TCP FIN	UDP
TCP	80	http	abierto	cerrado	---
	443	https	cerrado	cerrado	---
	1863	msoap	abierto	filtrado	---
	5190	aol	abierto	filtrado	---
UDP	53	dominio	---	---	cerrado

Servidor de Correo					
Protocolo	Puerto	Servicio	TCP SYN	TCP FIN	UDP
TCP	25	smtp	abierto	cerrado	---
	110	pop3	abierto	cerrado	---
	1863	msoap	abierto	filtrado	---
	5190	aol	abierto	filtrado	---
UDP	53	domain	---	---	abierto

Router (Movistar)					
Protocolo	Puerto	Servicio	TCP SYN	TCP FIN	UDP
TCP	23	telnet	abierto	filtrado	---
	79	finger	abierto	filtrado	---
	1863	msoap	abierto	filtrado	---
	5190	aol	abierto	filtrado	---
UDP	161	snmp	---	---	abierto

Firewall					
Protocolo	Puerto	Servicio	TCP SYN	TCP FIN	UDP
TCP	25	smtp	abierto	cerrado	---
	80	http	abierto	cerrado	---
	110	pop3	abierto	cerrado	---
	264	bgmp	abierto	filtrado	---
	443	https	cerrado	cerrado	---
	1863	msoap	abierto	filtrado	---
	5190	aol	abierto	filtrado	---
UDP	500	isakmp	---	---	abierto

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.2.2.2.4 I6. Identificación de Aplicaciones

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

Resultados Esperados:	Identificación de servicios ofrecidos Identificación de las aplicaciones ofrecidas
------------------------------	---

Requerimientos

- Resultados del escaneo previo de puertos

Pasos de Prueba:

- Identificación de servicios disponibles por el servidor

Determinados los puertos relevantes en los distintos servidores y equipos activos, utilizamos las herramientas “Nmap 4.20” y “Amap 5.2” para identificar los servicios y aplicaciones que están escuchando en un puerto dado.

A continuación se muestra la información destacada de cada uno de los objetivos, ver Tabla 1.13. El resultado completo del escaneo se muestra en el Anexo 7.

Tabla 1.13 Identificación de Aplicaciones

Servidor Web			
Protocolo	Puerto	Servicio	Aplicación
TCP	80	http	Microsoft IIS webserver 5.0 webmin
	1863	msnp	---
	5190	aol	---

Servidor de Correo			
Protocolo	Puerto	Servicio	Aplicación
TCP	25	smtp	Lotus Domino smtpd 6.0
	110	pop3	Lotus Domino POP3 server X2.0 (CN=administracion;Org=Carlink)
	1863	msnp	---
	5190	aol	---
UDP	53	domain	Microsoft DNS (djb)

Firewall			
Protocolo	Puerto	Servicio	Aplicación
TCP	25	smtp	---
	80	http	Microsoft IIS webserver 5.0 webmin
	110	pop3	Lotus Domino POP3 server X2.0 (CN=administracion;Org=Carlink)
	264	fw1-topology	Checkpoint FW1 Topology mysql
	1863	msnp	---
	5190	aol	---
UDP	500	isakmp	---

Router (Movistar)			
Protocolo	Puerto	Servicio	Aplicación
TCP	23	telnet	Cisco router telnet-t-rex-proxy
	79	finger	Cisco fingerd
	1863	tcpwrapped	---
	5190	tcpwrapped	---
UDP	161	snmp	SNMPv1 server (public)

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

- Identificar aplicaciones de Internet disponibles públicamente

Los servicios de seguridad “tracklink” y “transtrack” se encuentran disponibles vía Internet, ver Figura 1.15; para ingresar es necesario un ID (cédula o RUC) y una contraseña que son proporcionadas por la empresa al momento de la firma del contrato.



Figura 1.15 Interfaz de Ingreso, Aplicación Web

Fuente: CARLINK. <http://www.carlink.com.ec>. Septiembre/2007.

1.2.2.2.5 I 7. Identificación de Sistemas

El tester intenta obtener información acerca del sistema operativo, el estado del nivel de parcheo y del hardware del sistema.

Resultados Esperados:	Información acerca del sistema operativo Información acerca del nivel de parcheo
------------------------------	---

Pasos de Prueba:

- Ejecutar un escaneo de puertos con identificación de sistemas

La identificación de sistemas operativos en base a la comprobación de huellas TCP/IP, también conocida como “OS Fingerprinting”, es la técnica que usan la mayoría de los analizadores de puertos avanzados para determinar el sistema operativo de un equipo remoto. Esta identificación se basa en las particularidades de los distintos sistemas a la hora de manejar la pila de protocolos TCP/IP.

A continuación se muestra la información destacada de cada uno de los objetivos, ver Tabla 1.14. Las herramientas utilizadas son “Nmap 4.2” y “Xprobe2”. El resultado completo del escaneo, así como la descripción de las técnicas de identificación activa y pasiva se muestra en el Anexo 8.

Tabla 1.14 Identificación de Sistemas

Equipo	Sistema Operativo
Servidor Web	Microsoft Windows 2000 SP4
Servidor de Correo	Microsoft Windows 2000 SP4
Router (Movistar)	Cisco 805, Version 12.1(3)XG4
Firewall	F5 Labs kernel 4.2PTF-05a (x86)

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

- Analizar la información del banner

Las técnicas habituales para la identificación de sistemas mediante la captura del banner, en servicios como TELNET, FTP, etc. que proporcionan información acerca del sistema operativo son limitadas y obsoletas, debido a la facilidad con la que pueden ser modificadas, por lo tanto la información obtenida usando esta técnica no es fiable.

A continuación se muestra la información destacada de cada uno de los objetivos, ver Tabla 1.15. Las herramientas utilizadas son “Amap 5.2” y “Scaline 1.01”. El resultado completo de la identificación del banner se muestra en el Anexo 9.

Tabla 1.15 Identificación del Banner

Equipo	Puerto	Banner
Servidor Web	TCP:80	[HTTP/1.1 403 Access Forbidden Server: Microsoft-IIS/5.0 Date: Tue, 06 Nov 2007 15:29:20 GMT Content-Type: text/html Content-Length: 172 <html><head><title>Di]
Servidor de Correo	TCP:25	[220 administracion.carlink.com.ec ESMTP Service (Lotus Domino Release 6.0) read y at Tue, 6 Nov 2007 09:17:17 -0500]
	TCP:53	y\r\r CKAAAAAAAAAAAAA AAAAAAAAAAAAAAAAAAAA!@b\froot- serversnet2@c?2@d?2@e?2@f?2@g?2@h?2@i?2@j?2@k?2@l?2@m?2@a?=@O]@!\fm@\nZ}@\n@p\$@?5@\$@@@S*@\f!\r@)
	TCP:110	[+OK Lotus Notes POP3 server version X2.0 ready <004F6538.0525738B.00000C28.0000 000B@administracion/Carlink> on administracion/Carlink.]
Router (Movistar)	TCP:23	[User Access Verification Password:]
	TCP:79	[Line User Host(s) Idle Location 2 vty 0 idle 00:00:00]
	UDP:161	02public%L3V00+\taudioauto
Firewall	TCP:264	Q

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.2.2.2.6 I 8. Identificación Sigilosa del Router

El tester intenta identificar el router usado por la empresa, 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 del router
------------------------------	--

Requerimientos

- Información básica de la red e identificación de sistemas

El IP asignado al router es: 200.24.213.161, su funcionalidad dentro de la empresa es conectar al servicio de Internet y permitir el acceso de los usuarios externos a los servicios en línea. La marca y modelo es “Cisco 805” y el sistema operativo que utiliza es el “IOS 12.1(3)XG4”.

Pasos de Prueba:

- Seguir cautelosamente las rutas con el comando “tracert”

Se utilizara la aplicación “Ping-Probe 1.1.3”¹⁰ para seguir las rutas, ver Tabla 1.16.

Tabla 1.16 Análisis de Rutas - Router

Servidor Web	Servidor de Correo	Router	Firewall
1 - 192.168.1.1	1 - 192.168.1.1	1 - 192.168.1.1	1 - 192.168.1.1
2 - 190.152.27.1	2 - 190.152.27.1	2 - 190.152.27.1	2 - 190.152.27.1
3 - 200.107.34.217	3 - 200.107.34.217	3 - 200.107.34.217	3 - 200.107.34.217
4 - 190.11.18.17	4 - 190.11.18.17	4 - 190.11.18.17	4 - 190.11.18.17
5 - 190.11.18.65	5 - 190.11.18.65	5 - 190.11.18.65	5 - 190.11.18.65
6 - 190.11.18.82	6 - 190.11.18.82	6 - 190.11.18.82	6 - 190.11.18.82
7 - 200.1.6.7	7 - 200.1.6.7	7 - 200.1.6.7	7 - 200.1.6.7
8 - 200.24.222.165	8 - 200.24.222.165	8 - 200.24.222.165	8 - 200.24.222.165
9 - 10.116.253.49	9 - 10.116.253.49	9 - 10.116.253.49	9 - 10.116.253.49
10 - 10.116.253.65	10 - 10.116.253.65	10 - 10.116.253.65	10 - 10.116.253.65
11 - 172.22.1.93	11 - 172.22.1.93	11 - 172.22.1.93	11 - 172.22.1.93
12 - 172.22.1.94	12 - 172.22.1.94	12 - 200.24.213.161	12 - 172.22.1.94
13 - 200.24.213.164	13 - 200.24.213.174		13 - * * * *
14 - 200.24.213.164	14 - 200.24.213.174		

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

Analizando los resultados, concluimos que las rutas se mantienen iguales para todos hasta el salto 11, sin embargo al comparar la ruta entre el router y el firewall en el salto 12 se puede apreciar las 2 direcciones IP asignadas al router.

- Analizar las rutas de los paquetes IP

El router “Cisco 805” tiene asignado 2 IP’s, el primero es: 200.24.213.161 que se utiliza para conectarlo con el firewall, mientras el segundo es: 172.22.1.94 que se conecta a un router que pertenece a la red WAN, ver Figura 1.16.

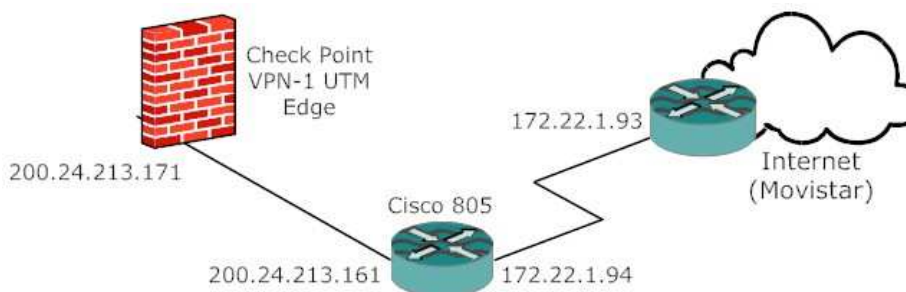


Figura 1.16 Análisis de Rutas - Router

¹⁰ <http://www.ping-probe.com/Ping-Probe/Download/Index.html>

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.2.2.2.7 I 10. Identificación Sigilosa del Firewall

El tester intenta identificar el firewall, el tipo/forma (paquetes filtrados), modelo (fabricante, versión), y la configuración (puertos abiertos y protocolos).

Resultados Esperados:	Direcciones IP Sistema operativo del Firewall Modelo y nivel de parcheo del software del firewall
------------------------------	---

Requerimientos

- Resultados del escaneo previo de puertos

La información recolectada desde el exterior nos indica que se trata de un firewall de marca "Check Point".

Pasos de Prueba:

- Escaneo directo a los puertos del firewall desde el interior

A continuación se muestra la información destacada, ver Tabla 1.17; los puertos no mencionados así como los tipos de escaneo TCP FIN, ACK, Null, Xmas y UDP han sido filtrados para todos los casos. El resultado completo del escaneo se encuentra en el Anexo 10.

Tabla 1.17 Escaneo Directo del Firewall

Firewall				
Protocolo	Puerto	Servicio	TCP SYN	Servicios
TCP	22	ssh	abierto	Mocanada embedded SSH (protocol 2.0)
	25	smtp	abierto	Lotus Domino smtpd 6.0
	53	domain	abierto	ISC Bind BIND 8.2.2-P5
	80	http	abierto	Microsoft IIS webserver 5.0
	110	pop3	abierto	Lotus Domino POP3 server X2.0 (CN=administracion;Org=Carlink)
	264	bgmp	abierto	Checkpoint FW1 Topology
	981	unknown	abierto	OpenSSL

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

- Ejecutar la identificación del sistema

El firewall usado por la empresa es un Check Point VPN-1 UTM Edge, que utiliza el kernel 4.2PTF-05a (x86) y fue desarrollado por la empresa “F5 Labs”.

1.2.2.2.8 I 12. Investigación de Vulnerabilidades

La información obtenida (puertos abiertos, aplicaciones, sistemas operativos) es analizada por vulnerabilidades, utilizando un conjunto de herramientas.

Resultados Esperados:

Lista de vulnerabilidades potenciales

Requerimientos

- Conocimiento a fondo sobre puertos abiertos, servicios ofrecidos, aplicaciones y sistemas operativos usados.

Pasos de Prueba:

- Usar los mejores escaners de vulnerabilidades

Entre las herramientas de escaneo de vulnerabilidades, ver Anexo 2; se han seleccionado las siguientes herramientas:

- “NESSUS”¹¹.- es el mejor escáner de vulnerabilidades de red no comercial, constantemente actualiza su registro de vulnerabilidades a través de plug-in(s). Los resultados del escaneo se presentan en un informe donde, se detallan las vulnerabilidades, el riesgo y las posibles soluciones.
- “RETINA NETWORK SECURITY SCANNER”¹².- escáner comercial para la evaluación de vulnerabilidades. Al igual que NESSUS, la función de RETINA es escanear todos los equipos en una red y reportar cualquier vulnerabilidad encontrada. Es producido por la empresa eEye.

¹¹ <http://www.nessus.org/nessus/>

¹² <http://www.eeye.com/html/Products/Retina/index.html>

- “SAINT”¹³.- es una herramienta usada para la evaluación de vulnerabilidades de red, esta basada en SATAN, se ejecuta únicamente sobre sistemas Linux y presenta una interfaz Web de fácil manejo. Entre sus características tenemos la capacidad de escaneo a través de un Firewall y la actualización de sus pruebas de seguridad basados en boletines emitidos por la CIAC¹⁴.

¹³ <http://www.saintcorporation.com/download.html>

¹⁴ <http://www.ciac.org>

A continuación se presenta la información destacada, ver Tabla 1.18; esto incluye: el equipo, el protocolo y puerto, las vulnerabilidades y los correspondientes identificadores “CVE”¹⁵; Estos permiten definir de una forma común las vulnerabilidades/exploits entre los distintos productos de seguridad. El resultado completo del escaneo de vulnerabilidades se detalla en el Anexo 11.

Tabla 1.18 Escaneo de Vulnerabilidades

Servidor Web			
Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP:80	Alto	Microsoft IIS versiones 4 y 5 son vulnerables a un ataque de denegación de servicio (DoS), debido a una vulnerabilidad en las extensiones del servidor frontpage. Un atacante puede enviar solicitudes de sumisión especialmente diseñadas al servidor Web, causando que falle.	CVE-2001-0096
	Alto	OmniHTTPd contiene un defecto que permite a un atacante remoto ejecutar código arbitrario en un servidor vulnerable.	CVE-1999-0951
	Medio	El script htmimage.exe incluido en las extensiones del servidor FrontPage contiene ciertas vulnerabilidades, que permiten a un atacante remoto determinar la existencia de archivos arbitrarios y de carpetas en el directorio Web raíz.	CVE-2000-0122

Servidor de Correo			
Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP:25	Alto	Un desbordamiento de buffer en el servicio ESMTP del servidor Lotus Dominio 5.0.1 permite a un atacante remoto provocar una denegación de servicio (DoS), mediante el uso del comando “MAIL FROM” con un parámetro extenso.	CVE-2000-0452
	Alto	Múltiples vulnerabilidades permiten a un atacante causar una denegación de servicio (DoS) por consumo de CPU, esto sucede al enviar solicitudes de reunión VCAL deformadas usando SMTP.	CVE-2006-0119
	Alto	Un desbordamiento de búfer en el servicio tunekrnl en IBM Lotus Domino 6.x, permiten a los usuarios locales obtener privilegios y ejecutar código arbitrario.	CVE-2006-5818

¹⁵ Common Vulnerabilities and Exposures

TCP:25	Alto	Múltiples vulnerabilidades no especificadas en IBM Lotus Notes y Domino en versiones anteriores a la 6.5.5, permiten a un atacante provocar una denegación de servicio (DoS).	CVE-2006-0120
	Medio	El número de secuencia TCP es predecible y permite "spoofing"	CVE-1999-0077
UDP:53	Medio	Es posible consultar al servidor remoto de nombres por nombres de terceros, esto permite realizar un ataque de envenenamiento de cache contra el servidor.	CVE-1999-0024
	Medio	El servidor DNS remoto responde las consultas de dominio de terceros que no tienen el bit de recursión activo, que permite a un atacante remoto realizar un "Cache Snooping Attack".	-----

Router			
Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
UDP:161	Alto ¹⁶	Cisco IOS permite a un atacante remoto causar una denegación de servicio (DoS) por bloqueo de tráfico, mediante el envío de una secuencia particular de paquetes IPv4 a una interfaz en el equipo, causando que la cola de entrada en la interfaz sea marcada como llena.	CVE-2003-0567
	Alto*	Múltiples vulnerabilidades en la implementación del protocolo H.323 para Cisco IOS, permiten a un atacante remoto causar desde denegación de servicio (DoS) hasta una posible ejecución arbitraria de código.	CVE-2004-0054
	Alto*	Mediante el envío de un paquete de control (NTP) diseñado, es posible provocar un desbordamiento de buffer en el demonio NTP, esta vulnerabilidad puede ser explotada remotamente.	CVE-2001-0414
	Alto*	El IOS contiene un defecto que podría permitir un ataque de denegación de servicio (DoS), causado por un atacante cuando envía paquetes ARP que explotan el manejo de direcciones MAC incorrectas.	CVE-2001-0895

¹⁶ Vulnerabilidad basada en el banner del equipo remoto (*)

UDP:161	Alto ¹⁷	Un atacante remoto al intentar explotar la vulnerabilidad "SSH CRC32", puede causar que el módulo SSH en los equipos Cisco llegue a consumir todos los recursos disponibles del CPU.	CVE-2002-1024
	Alto*	El problema sucede cuando un atacante provoca numerosos login equivocados en el equipo utilizando autenticación SSH con TACACS, lo que conlleva a una fuga de memoria	CVE-2005-1021
	Alto*	SSH2 en un dispositivo Cisco permite a un atacante remoto causar una denegación de servicio (DoS) por reinicio del equipo, sucede al ingresar un nombre de usuario que contiene un nombre de dominio en el servidor TACACS+ usado para autenticación.	CVE-2005-1020
	Alto*	Una fuga de memoria en el TCP listener permite a un atacante remoto causar una denegación de servicio (DoS). Sucede al enviar tráfico TCP diseñado a una dirección IPv4 en el equipo.	CVE-2007-0479
	Alto*	Cisco IOS 12.1(3)T permite a un atacante remoto causar una denegación de servicio (DoS) por reinicio del dispositivo, mediante una conexión TCP a un rango específico de puertos: 3100-3999, 5100-5999, 7100-7999 y 10100-10999.	CVE-2001-0750
	Alto*	Cisco IOS con MPLS instalado pero deshabilitado, permite a un atacante remoto causar una denegación de servicio (DoS) por reinicio del dispositivo, sucede al enviar paquetes diseñados a las interfaces deshabilitadas.	CVE-2005-0197
	Alto*	Cisco IOS permiten a un atacante remoto causar una denegación de servicio o ejecutar código arbitrario, sucede al modificar las opciones IP en la cabecera de los paquetes ICMP, PIMv2, PGM o URD.	CVE-2007-0480
	Alto	Las vulnerabilidades en el manejo de solicitudes SNMPv1 de un gran número de implementaciones SNMP, permiten a un atacante remoto causar una denegación de servicio.	CVE-2002-0013
	Medio	Existe una vulnerabilidad existe en la opción DLSw en el Cisco IOS, donde un valor invalido en un mensaje DLSw puede provocar el reinicio del equipo.	CVE-2007-0199

¹⁷ Vulnerabilidad basada en el banner del equipo remoto (*)

UDP:161	Medio	Cisco IOS mantiene números predecibles de secuencia inicial, que permite a un atacante remoto ejecutar un "spoof" o "hijack" de las conexiones TCP.	CVE-2001-0288
	Medio	El "SNMP community name" mantiene su valor por defecto	CVE-1999-0517
	Medio	Múltiples vulnerabilidades no especificadas en IBM Lotus Notes y Domino Server en versiones menores al 6.5.5, permite a un atacante provocar una denegación de servicio (DoS).	CVE-2004-1776
TCP:79	Medio	Una versión de finger esta ejecutándose, lo que expone información valida de un usuario a cualquier entidad en la red.	CVE-1999-0612
TCP:23	Medio	Existe un error en el Cisco IOS que permite a través de sesiones telnet especialmente diseñadas causar un fallo en todos los accesos administrativos al equipo.	CVE-2004-1464

Firewall			
Protocolo: Puerto	Riesgo	Vulnerabilidad	CVE
TCP:General	Alto	Es posible bloquear al host remoto enviando un paquete IP especialmente diseñado con una longitud nula para la opción IP #0xE4.	CVE-2005-2577
TCP:80	Alto	OmniHTTPd contiene un defecto que permite a un atacante remoto ejecutar código arbitrario en un servidor vulnerable.	CVE-1999-0951
UDP:500	Medio	Es posible causar un desbordamiento de buffer al iniciar una negociación IKE, y a continuación enviar un paquete IKE con datos ASN.1 deformados.	CVE-2004-0699
	Información	El servicio ISAKMP esta corriendo sobre el host explorado, este proporciona información sobre lo que esta activo dentro de la red.	-----

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

- Consultar bases de datos de vulnerabilidades

Entre los recursos utilizados para la consulta de vulnerabilidades tenemos:

- <http://www.securityspace.com/smysecure/search.html>
- <http://www.securityfocus.com/vulnerabilities>
- <http://osvdb.org:80/>
- <http://nvd.nist.gov/>
- <http://secunia.com/>

1.2.2.2.9 I 13. Identificación de las Interfaces de Aplicación

El objetivo de este módulo es identificar las interfaces que pueden ser accedidas desde el Internet, en particular aquellas que han sido desarrolladas por el Departamento de Sistemas, para proceder a examinarlas en búsqueda de 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 empresa, en búsqueda de vulnerabilidades potenciales.

Para llevar acabo el escaneo de vulnerabilidades de la página principal de la empresa, se utilizara el escaner CGI conocido como "Watchfire Appscan 7.0"¹⁸, esta herramienta permite generar reportes que contienen el listado de problemas de seguridad encontrados, una descripción para cada uno de ellos, además de los riesgo asociados y las recomendaciones para corregirlos.

A continuación se presenta la información destacada, ver Tabla 1.19. El resultado completo del escaneo se muestra en el Anexo 12.

¹⁸ <http://download.watchfire.com>

Tabla 1.19 Escaneo de Vulnerabilidades – Interfaz Web

Interfaz Web	
Riesgo	Vulnerabilidad
Alto	Enumeración de credenciales en mensajes de error de login. Las excepciones y mensajes de error presentadas a los usuarios podrían contener información sensible.
Alto	Existe la posibilidad de ejecutar "SQL Injection" en la página de login, debido a que el saneamiento de caracteres peligrosos no ha sido realizado correctamente en las entradas de usuario.
Medio	Credenciales de logeo predecibles, debido a la programación o configuración defectuosa de la aplicación Web.
Medio	Solicitud de login no encriptada. Campos de datos de entradas sensibles tales como nombres de usuarios o contraseñas se transmiten sin encriptar.

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

1.2.2.3 Fase 3: Análisis de Información y Riesgos

En la fase de análisis de información y riesgos el objetivo es determinar si los módulos pertenecientes a la fase 4 del test serán ejecutados, esto conlleva definir las prioridades, establecer los riesgos asociados y si fuera el caso, limitar los sistemas y módulos.

1.2.2.3.1 Definición de Prioridades

La prioridad para ejecutar la fase 4 (Intentos Activos de Intrusión) es garantizar la seguridad y disponibilidad 24/7 de los servicios y aplicaciones que presta la empresa a través del Internet. Sin embargo, debido a la naturaleza de estas pruebas los servicios y aplicaciones podrían llegar a comprometerse, lo que sería perjudicial para el buen nombre y confianza ganada por la empresa durante años.

1.2.2.3.2 Riesgos Asociados

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

- Denegación de servicio (DoS) y desbordamiento de buffer del servidor Web, causando que los servicios que mantiene la empresa en el Internet no estén disponibles.

- Denegación de servicio y desbordamiento de buffer del servidor de correo, causando que los usuarios de la red LAN no tengan disponible el servicio de correo electrónico además de bloquear el acceso a los equipos de la red administrativa.
- Denegación de servicio y desbordamiento de buffer del router, causando que la empresa no tenga acceso al Internet y que los servicios que mantiene la empresa en el Internet no estén disponibles.
- Desbordamiento de buffer del firewall, causando que la red de la empresa quede aislada del Internet y que los servicios que mantiene la empresa en el Internet no estén disponibles.

1.2.2.3.3 Limitación de Sistemas y Módulos

Basados en las prioridades y los riesgos asociados, se confirma que se va a realizar únicamente un test “Pasivo”, donde los módulos pertenecientes a la fase 4 no van a ser ejecutados.

1.2.2.4 Fase 5: Análisis Final

Esta sección describe las amenazas y vulnerabilidades detectadas en la empresa.

1.2.2.4.1 Determinación de Amenazas

Considerando que las amenazas a la red son eventos que pueden desencadenar un incidente en la empresa, produciendo daños materiales o pérdidas inmateriales, tenemos:

- Amenazas Físicas
 - Acceso no autorizado a datos
 - Robo de información a través de dispositivos de almacenamiento portátiles
 - Alta rotación del personal
 - Técnicas de Ingeniería social - phishing
 - Riesgos asociados con el personal de limpieza o externo
 - Daño inadvertido de cables
 - Robo, destrucción o mal funcionamiento de un componente o equipo
 - Cortes de luz, UPS descargados o variaciones de voltaje
 - Factores ambientales
 - Error Humano

- Amenazas Lógicas
 - Programas maliciosos - Virus, Worm, Troyano y similares
 - Mensajes no solicitados – SPAM
 - Botnets y Zombies
 - Pharming
 - Spoofing y Sniffing
 - Redes sociales y video online
 - SQL Inyection
 - Desbordamiento de Buffer
 - Denegación de Servicio (DoS)

1.2.2.4.2 Determinación de Vulnerabilidades

Las vulnerabilidades se establecen en base a las condiciones que favorecen la ocurrencia de una amenaza. A continuación se describen las vulnerabilidades encontradas en la red de datos:

- Vulnerabilidades Físicas
 - Cuarto de Telecomunicaciones sin ventilación
 - Cableado estructurado no certificado
 - Inexistencia de una fuente de energía emergente
 - Almacenamiento inseguro de respaldos
 - Firewall subdimensionado
 - Documentación inexistente
 - Falta de difusión de las políticas de seguridad entre el personal
- Vulnerabilidades Lógicas
 - No esta implementada una zona desmilitarizada (DMZ)
 - No existe un software para el filtrado de correo basura
 - No existe un software para el filtrado de páginas Web y asignación de perfiles de uso.
 - No existe un sistema de detección de intrusos
 - Configuración inapropiada de servicios
 - Técnicas inadecuadas de programación
 - Software desactualizado

CAPITULO 2.

ANÁLISIS Y DISEÑO DE UN ESQUEMA DE SEGURIDAD PARA LA RED DE TRANSMISIÓN DE DATOS

2.1 REQUERIMIENTOS DE SEGURIDAD DE LA EMPRESA

Las diferentes fuentes de consulta de las cuales se obtuvo la información para determinar los requerimientos de seguridad son:

- Jefe de Sistemas
- Asistentes y Operarios del Departamento de Sistemas y Monitoreo
- Usuarios de la red
- Descripción de la situación actual de la empresa, Capítulo 1

Los requerimientos de seguridad identificados en la empresa se detallan a continuación.

2.1.1 REQUERIMIENTOS FÍSICOS

2.1.1.1 Control de Acceso Físico y de Seguridad

- Remodelar el cuarto de telecomunicaciones con el objetivo de ubicar dentro de este todos los equipos activos de la red, tales como: servidores, switches, routers, UPS's, Firewall's y modem's.
- Controlar el acceso físico a las áreas críticas, mediante el uso de tarjetas magnéticas o claves, permitiendo únicamente el ingreso al personal autorizado.
- Establecer revisiones periódicas de los controles de acceso físico a cada área, durante el horario de trabajo y fuera de este.

2.1.1.2 Estructura del Cableado

- Integrar el sistema de cableado en la estructura del edificio, para así evitar el posible seccionamiento del cableado de la red.
- Disponer de la documentación de señalización e identificación de terminales en la estructura de la empresa.
- Aplicar estándares de referencia como el EIA/TIA-568A, EIA/TIA-569, EIA/TIA-606, EIA/TIA-607, que permiten administrar el cableado dependiendo de los requerimientos y de la evolución tecnológica en la empresa, ya que el edificio no cuenta con cableado estructurado certificado.

2.1.1.3 Sistema Emergente de Energía

- Para evitar pérdidas y daños físicos de los equipos de cómputo es necesario revisar periódicamente las instalaciones eléctricas de la empresa.
- Utilizar fuentes redundantes y dispositivos UPS (Uninterruptible Power Supply) en el Departamento de Sistemas, ya que permiten mantener operativos los sistemas ante repentinas caídas del servicio de electricidad.
- Adquirir una planta de energía eléctrica auxiliar para todas las instalaciones de la empresa.

2.1.1.4 Planes de Contingencia

2.1.1.4.1 Desastres Naturales

- Probar y actualizar periódicamente el plan de contingencia para el Departamento de Sistemas, donde se incluyen: aplicaciones críticas, sistemas de cómputo y de comunicación. Con el objetivo de minimizar los daños frente a desastres de grandes proporciones tales como: erupciones volcánicas, terremotos, inundaciones, etc.

- Emitir planes de contingencia que correspondan a las actividades críticas que realiza cada uno de los departamentos, los cuales deben ser difundidos a todo el personal ante desastres naturales.

2.1.1.4.2 Desastres del Entorno

- Instalar detectores de humo, para prevenir incendios que puedan comprometer los equipos, la información y pongan en peligro la vida de los empleados de la empresa.
- Regular las condiciones ambientales de temperatura y humedad dentro del el cuarto de telecomunicaciones, a través de ventiladores o un equipo de aire acondicionado.

2.1.2 REQUERIMIENTOS LÓGICOS

2.1.2.1 Control de Acceso lógico y de Seguridad

- Implementar controles de acceso para el sistema operativo, las bases de datos, software institucional y archivos compartidos, con la intención de que estos no puedan ser utilizados, modificados o eliminados sin autorización y se asegure la integridad de la información.
- Monitorear constantemente el acceso a los sistemas operativos, los servidores y las aplicaciones dentro y fuera de la red de datos.

2.1.2.1.1 Identificación y Autentificación

- Definir perfiles de acceso a los diferentes recursos de la red (configuraciones, aplicaciones, documentos, etc.), dependiendo de la función que cumple cada usuario dentro de la empresa.

2.1.2.1.2 Control de Acceso Interno

- Utilizar contraseñas fuertes para proteger los datos, aplicaciones y equipos de computación.
- Mantener actualizada la lista de registro de usuarios (grupos de usuarios, equipos de computación y servicios), a quienes se les ha proporcionado acceso para el ingreso a los recursos del sistema.

2.1.2.1.3 Control de Acceso Externo

- Monitorear constantemente el firewall, con el fin de evitar accesos no autorizados hacia la red LAN.
- Monitorear el router que conecta al servicio de Internet, para evitar posibles ataques DoS, desbordamiento de buffer o reinicio inesperado del dispositivo, lo que impide un desempeño normal de los usuarios.

2.1.2.2 Protección de Datos

2.1.2.2.1 Respaldos

- Instalar un sistema centralizado de respaldos alojado en un rack o armario seguro con su respectivo monitoreo.
- Tomar medidas necesarias para proteger físicamente los medios donde se van a obtener los respaldos, sean estos CD's, DVD's o cartuchos de cinta magnética, con el objetivo de evitar: altas temperaturas, humedad, rayones, rupturas y campos magnéticos, entre otros.
- Salvaguardar la integridad y disponibilidad de los respaldos, es decir, mantenerlos en un lugar seguro.
- Gestionar un cronograma mensual de verificación de respaldos, que garantice la integridad de estos.

2.1.2.3 Seguridad en los Servicios

- Chequeos permanentemente con el fin de detectar modificaciones en los sistemas operativos, grupo de trabajo, usuarios, etc. que pueden afectar la seguridad de los usuarios o de la red.

2.1.2.3.1 Acceso al Internet

- Adquirir un software o equipo para filtrado Web, con el objetivo de evitar el ingreso a páginas Web recreativas o ilegales.
- Establecer perfiles para el uso del servicio de Internet.

2.1.2.3.2 *Correo Electrónico*

- Instalar y configurar software o equipo para filtrado de correo basura (SPAM), con el objetivo de evitar que las cuentas de correo se llenen prematuramente o que el servidor de correo se sature.

2.1.2.3.3 *Antivirus*

- Mantener un software antivirus de reconocido prestigio permanentemente actualizado.

2.1.3 REQUERIMIENTOS DE RED Y COMUNICACIÓN

2.1.3.1 Infraestructura de la Red

- Implementar en la red de la empresa una Zona Desmilitarizada o “DMZ”
- Instalar un sistema de detección de intrusos en la red de la empresa, para el monitoreo contra: escaneos, OS fingerprint, exploits, DoS, tráfico no deseado e intentos de intrusión.
- Impedir que los datos que circulan por el canal de comunicación sean escuchados mediante el uso de programas tipo sniffer, evitando un ataque interno a la red de datos.
- Adquirir un nuevo y moderno firewall con mejores características, debido al aumento de usuarios, servicios y aplicaciones dentro de la intranet.

2.1.4 REQUERIMIENTOS DE GESTIÓN

2.1.4.1 Gestión de la Seguridad de la Información

- Para complementar el esquema tecnológico de la red de datos, se requiere un conjunto de políticas y normas de seguridad (esquema organizacional) que permita indicar las directrices del manejo interno y externo de la empresa.

2.2 DISEÑO DE ESCENARIOS DE SEGURIDAD

El diseño del escenario de seguridad para la red de transmisión de datos de la empresa Carlink se define a continuación:

2.2.1 ESCENARIO DE LA SEGURIDAD FÍSICA

A continuación se detalla el diseño del escenario de seguridad física para la red de transmisión de datos de la empresa, el cual permite cubrir los requerimientos físicos descritos en la sección 2.1.1.

2.2.1.1 Control de seguridad en el acceso físico.

El cuarto de telecomunicaciones debe ser remodelado mediante la instalación de piso y techo falso, además se debe realizar un rediseño de las instalaciones eléctricas e implementarse una puerta eléctrica. Esta puerta deberá abrirse mediante la utilización de tarjetas magnéticas, tarjetas de aproximación, o claves para el control de acceso en esta área.

Para el acceso al Departamento de Sistemas y Monitoreo también se debe contar con una puerta eléctrica. El acceso a los demás departamentos de la empresa deberá ser controlado por el guardia de seguridad a toda hora.

A toda persona externa a la empresa que ingrese por diferentes motivos, el guardia de seguridad deberá solicitarle algún documento de identificación para poder registrar la siguiente información: nombre, hora de ingreso, departamento al que se dirige, hora de salida.

2.2.1.2 Estructura del Cableado

“Los Sistemas de Cableado Estructurado deberán emplear una Arquitectura de Sistemas Abiertos (OSA) y soportar aplicaciones basadas en estándares internacionales como el EIA/TIA-568A, EIA/TIA-569, EIA/TIA-606, EIA/TIA-607 (Electronic Industries Association/ Telecommunications Industry Association) “. ¹⁹

Las instalaciones de cableado eléctrico deberán ser independiente del cableado de red para evitar interferencias.

2.2.1.3 Sistema Emergente de Energía

El Departamento de Sistemas y Monitoreo debe coordinar revisiones periódica de las instalaciones eléctricas con el personal pertinente.

El Departamento de Sistemas debe adquirir un UPS para asegurar el trabajo continuo de los equipos activos hasta que la planta eléctrica (motogenerador) auxiliar se active.

2.2.1.4 Planes de Contingencia

El Departamento de Sistemas y Monitoreo deberá difundir los planes de contingencia existentes en la empresa ante desastres naturales, emergencias y/o actividades críticas.

Se debe instalar un sistema contra incendios para toda la empresa, esta instalación debe estar bajo la norma N.F.P.A-72 (National Fire Protection Association). Además cada departamento deberá poseer un extintor de CO₂ o espuma para que el personal pueda contener cualquier pequeño incendio.

¹⁹ <http://www.emsetel.com/cableado-estructurado/index.php>

2.2.2 MODELO DE SEGURIDAD “SAFE” DE CISCO

El modelo de seguridad SAFE fue elaborado por Sean Convery y Bernie Trudel en el año 2000, ambos fueron miembros del equipo de marketing técnico de las arquitecturas de VPN y de seguridad de la línea empresarial de negocios de Cisco. La segunda versión fue creada por Greg Abelar y Jason Halpern del equipo de Arquitectura SAFE en el año 2004. Los cambios al documento original están relacionados con la evolución de nuevas tecnologías de seguridad.

El objetivo principal del modelo de seguridad “SAFE” de Cisco es “ofrecer información sobre las mejores prácticas, a las partes interesadas en el diseño e implementación de redes seguras”²⁰.

Este tipo de diseño está orientado en las amenazas que se esperan y en los medios para combatirlas. El resultado de esta estrategia es un enfoque de seguridad por módulos, donde no es probable que el fallo de uno de los sistemas de seguridad ponga en peligro a los demás recursos de la red.

2.2.2.1 Visión General de la Arquitectura

2.2.2.1.1 Fundamentos del Diseño

“SAFE” de Cisco es una arquitectura de seguridad, no es una forma revolucionaria de diseñar redes sino únicamente es un modelo para asegurarlas. La arquitectura también es robusta y escalable, la robustez de las redes está asociada con la redundancia física, es decir, que la protege de fallos de los dispositivos debido a una configuración errónea, o a un ataque a la red.

La implementación varía según las necesidades funcionales de la red.

2.2.2.1.2 Concepto de Módulos

En la Figura 2.1 se muestra la primera capa de modularidad del modelo “SAFE” de Cisco, cada bloque del gráfico representa una área funcional.

²⁰ http://www.solunet.com/wp-upload/safe_wp.pdf

Cabe señalar que el módulo del ISP no lo implementa la empresa, sino que esta incluido hasta el punto de que para combatir ataques sería necesario pedir determinadas características de seguridad en este servicio.

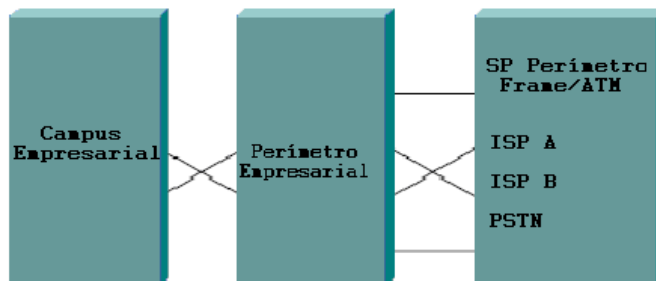


Figura 2.1 Módulo Compuesto de la Empresa

Fuente: The SAFE Blueprint from Cisco Systems.
http://www.solunet.com/wp-upload/safe_wp.pdf, pág. 4. 2004.

La segunda capa de modularidad, ver Figura 2.2; representa una vista de los módulos de cada área funcional. Cada módulo realiza funciones específicas en la red y tienen requisitos de seguridad específicos.

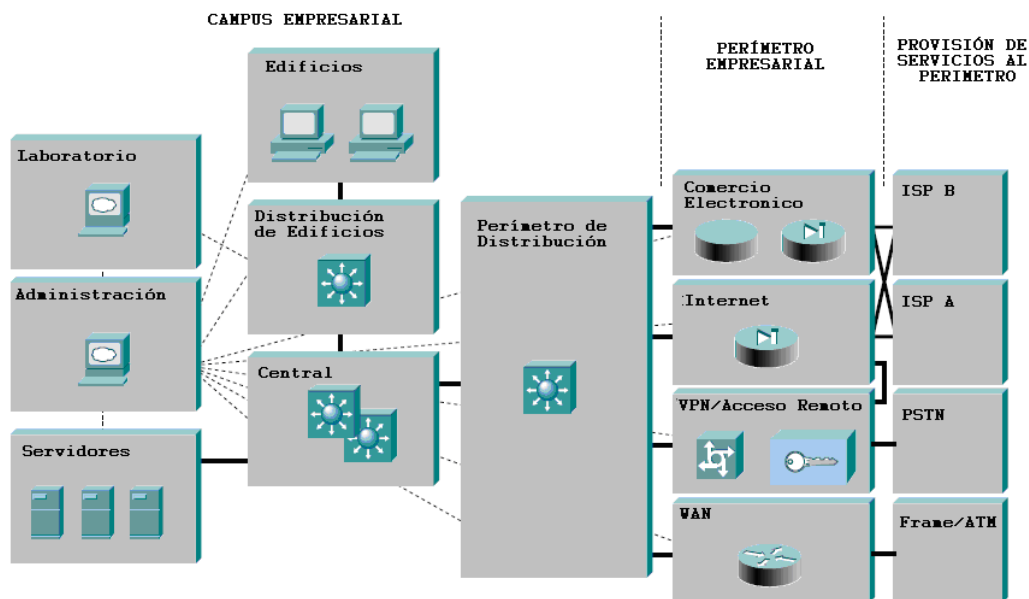


Figura 2.2 Diagrama de Bloques de “SAFE”

Fuente: The SAFE Blueprint from Cisco Systems.
http://www.solunet.com/wp-upload/safe_wp.pdf, pág. 5. 2004.

2.2.2.1.3 Axiomas de “SAFE” de Cisco

“SAFE” de Cisco define 5 axiomas, que deben ser considerados cuando se diseña una red, ya que al ser aplicados disminuyen los puntos vulnerables de la misma.

- **LOS ROUTERS SON EL OBJETIVO.**- son dispositivos críticos en cualquier implementación de seguridad, controlan el acceso de los usuarios internos a los servicios de red de la empresa y a los servicios de Internet, por consiguiente hay que asegurarlos para disminuir la posibilidad de que estén en peligro. Entre las principales consideraciones de seguridad tenemos:
 - Bloquear el servicio de Telnet
 - Bloquear el protocolo SNMP
 - Controlar el acceso a través del uso de TACACS+
 - Desactivar los servicios innecesarios
 - Usar el registro de eventos
 - Autenticar las actualizaciones de enrutamiento

- **LOS SWITCHES SON EL OBJETIVO.**- los switches (capa 2 y 3) permiten el encaminamiento de la información de una red a otra, por consiguiente también hay que asegurarlos para disminuir la posibilidad de que estén en peligro. Adicionalmente a las técnicas de seguridad aplicadas a los routers, los switches tienen las siguientes:
 - Deshabilitar todos los puertos sin uso
 - Desactivar los puertos que no necesitan enlaces troncales
 - Asegurarse que un puerto troncal use un número de VLAN único
 - No utilizar VLAN's como único método para asegurar el acceso entre dos subredes.

- **LOS HOST SON EL OBJETIVO.**- son el objetivo mas probable durante un ataque, ya que son los mas visibles. Presentan el reto más difícil en cuanto a la seguridad debido al número de plataformas de hardware, sistemas operativos y aplicaciones. Entre las principales consideraciones de seguridad tenemos:
 - Mantener los sistemas con los últimos parches y actualizaciones
 - Evaluar toda actualización en una red de prueba antes de implantarla en la red de producción.

- **LAS REDES SON EL OBJETIVO.**- el objetivo de este ataque no es bloquear un equipo, sino que deje de funcionar toda la red. Este tipo de ataques aprovecha las características intrínsecas de la forma en que opera la red. Entre las principales consideraciones de seguridad tenemos:
 - Seguir el RFC 1918 que especifica las redes que están reservadas para uso privado
 - Usar los filtros del RFC 2827 para evitar la falsificación IP (spoofing)
 - Limitar la cantidad de ancho de banda que se permite a un protocolo específico utilizar.

- **LAS APLICACIONES SON EL OBJETIVO.**- la mayor parte de aplicaciones son desarrolladas por seres humanos, y como tales, están sujetas a numerosos errores que podrían ser benignos o malignos. Estos problemas se los puede superar con la utilización de sistemas de detección de intrusos (IDS) de 2 tipos, basados en host (HIDS) y en red (NIDS), “SAFE” de Cisco recomienda la combinación de los dos sistemas para abarcar toda la red.

2.2.2.2 Módulos de la Empresa

El diseño “SAFE” de Cisco divide a una empresa en dos áreas funcionales: el campus empresarial y el perímetro empresarial, estas áreas a su vez se dividen en módulos, los cuales definen detalladamente las distintas funciones de cada área. El detalle de los módulos se puede apreciar en el Anexo 13.

2.2.3 ESCENARIO DE LA SEGURIDAD LÓGICA BASADO EN “SAFE” DE CISCO

A continuación se va a detallar el diseño del esquema de seguridad de la red de transmisión de datos, utilizando el modelo de seguridad “SAFE” de Cisco. El diseño que se va a implementar tiene el objetivo de garantizar la seguridad, resistencia, rendimiento, confiabilidad e integridad de la red de datos de la empresa. Además permitirá cubrir los requerimientos lógicos, de red y comunicación de las secciones 2.1.2 y 2.1.3 anteriormente mencionadas.

2.2.3.1 Campus Empresarial

De acuerdo al modelo “SAFE” de Cisco, el Campus Empresarial se compone de los siguientes módulos: Central, Distribución de Edificios, Edificios, Servidores, Perímetro de Distribución y Administración.

El módulo Central se encarga de optimizar el tráfico central, enrutando y swicheando todos los datos que circula por la red de datos. EL módulo de Distribución de Edificios previene los ataques internos a la red y protege la información de cada departamento. El módulo de Edificios (Usuarios) se encarga de analizar las necesidades del usuario final dando servicios seguros y confiables. El módulo de Servidores garantiza la seguridad y funcionalidad de los mismos, brindando a los usuarios finales los servicios necesarios. El Perímetro de Distribución permite la conectividad entre los equipos activos (internos y externos). El módulo de Administración se encargara de administrar de una forma segura los dispositivos y equipos existentes en la empresa.

2.2.3.1.1 Módulo Central

El módulo central se encarga de rutear y switchear los datos de la red empresarial de una manera rápida y segura de una red a otra. El objetivo de este módulo se logra con la implementación de 2 switches de capa 3, ver figura 2.3; que deberán ser ubicados en el cuarto de servidores de la empresa.

Las amenazas que este modulo previene son:

- Paquetes tipo sniffer que circulen en la red de datos
- Ataque de denegación de servicios distribuido

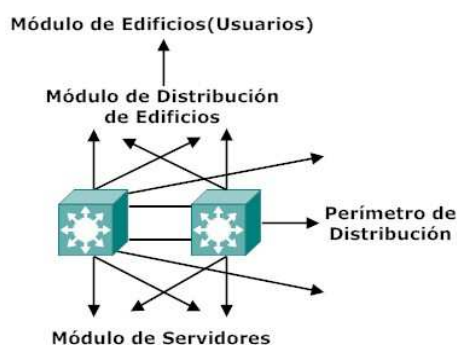


Figura 2.3 Diseño del Módulo Central

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.1.2 Módulo de Distribución de Edificios

El módulo de Distribución de Edificios se encarga de proporcionar los servicios de enrutamiento, control de acceso y calidad de servicio (QoS) al módulo de Edificios. Para la implementación "SAFE" nos permite combinar el módulo Central con el módulo de Distribución de Edificios, para así disminuir el número de dispositivos involucrados.

Entre las amenazas que este módulo previene tenemos:

- Acceso no autorizado a la red LAN de la empresa
- Direcciones IP falsificadas
- Paquetes tipo sniffer que circulen en la red de datos

2.2.3.1.3 Módulo de Edificios (Usuarios)

El módulo de Edificios se encarga de ofrecer un servicio seguro y confiable a los usuarios finales. La mayor parte del control de acceso a nivel de usuario es proporcionado por el módulo de Distribución de Edificios, para esto es necesario contar con 3 switches de capa 2 que conecten las estaciones de trabajo con el módulo Central, ver Figura 2.4.

Las amenazas que este modulo previene son:

- Paquetes tipo sniffer que circulen en la red de datos
- Virus y troyanos en las estaciones de trabajo.

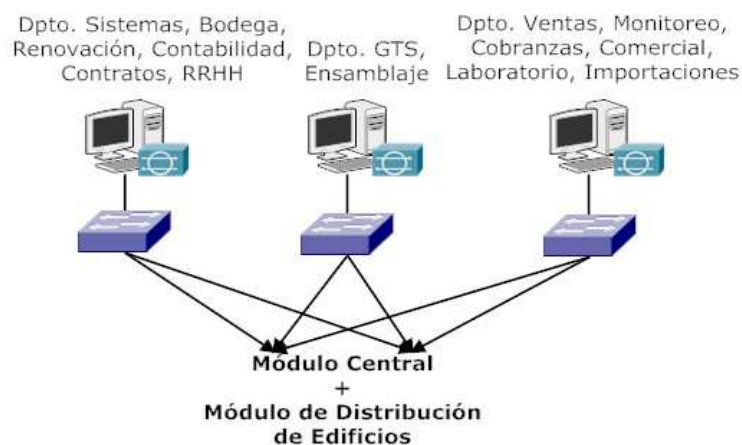


Figura 2.4 Diseño del Módulo de Edificios

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

Para la implementación de este módulo es necesaria la creación de políticas, normas y procedimientos de seguridad para los usuarios finales, los cuales deben estar capacitados para el manejo adecuado de los servicios y recursos informáticos, ateniéndose a las sanciones pertinentes en caso de no cumplirlas.

2.2.3.1.4 Módulo de Servidores

El módulo de servidores garantiza la seguridad y funcionalidad de los mismos, brindando a los usuarios finales servicios, tales como: DNS, impresión, aplicaciones, base de datos, archivos y de respaldo. Para la implementación se utilizara 2 switches de capa 3 que incluyen un módulo IDS, el cual inspecciona el tráfico dirigido a los servidores Departamentales y Corporativos, ver Figura 2.5.

Para el caso de que se realice un diseño básico es posible combinar este módulo con el módulo Central, sin embargo se recomienda mantenerlos separados ya que la empresa depende del rendimiento de los servidores para poder brindar un servicio eficiente.

Las amenazas que este modulo previene son:

- Accesos no autorizados a los servidores Corporativos y Departamentales
- Ataques a las aplicaciones que residen en los servidores
- Direcciones IP falsificadas
- Paquetes tipo sniffer que circulen en la red de datos
- Redireccionamiento de puertos

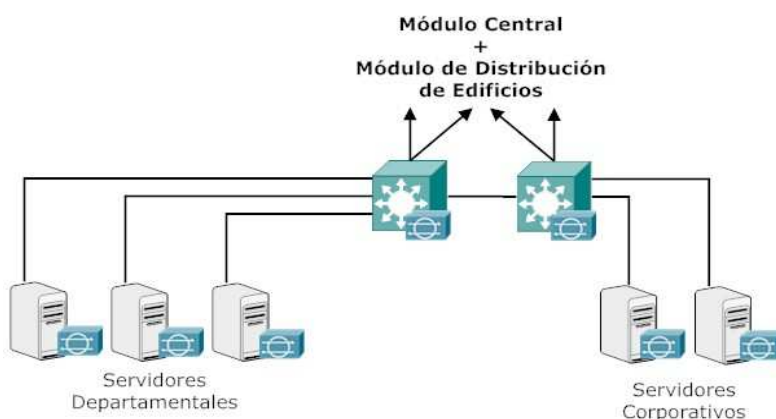


Figura 2.5 Diseño del Módulo de Servidores

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.1.5 *Módulo de Administración*

El módulo de Administración se encarga de gestionar de una forma segura todos los equipos y dispositivos de la empresa, la información de reportes y registros fluye desde los dispositivos hasta los equipos de administración, mientras que el contenido, las configuraciones y el software fluyen viceversa; este módulo mantiene mecanismos de seguridad que exigen que uno o varios equipos sean responsables del control de acceso, monitoreo de red, syslog, administración del sistema e IDS, ver Figura 2.6.

Toda la administración de la red se maneja desde 2 segmentos, el primero llamado “En Banda” que comparte el tráfico de la red de administración con la red de producción, el segundo llamado “Fuera de Banda” que utiliza una red físicamente separada y distinta de la red de producción para administrar los equipos de la red.

Este modulo permitirá cubrir con varios de los requerimientos planteados en las secciones 2.1.2.1, 2.1.2.3 y 2.1.3.1.

- Control de Acceso lógico y de seguridad (sistemas operativos, base de datos, software institucional y archivos compartidos)
- Identificación y Autenticación (definición perfiles de acceso a usuarios)
- Actualización de listas de registros de usuarios
- Monitoreo de equipos activos (firewall, routers)
- Administración de sistema de detección de intrusos (IDS)
- Monitoreo de software tipo sniffer

Los equipos a utilizados en la implementación según las recomendaciones dadas por Cisco son: 2 switches de capa 2, 1 router con características de firewall y 1 router para conectarse a los puertos de consola de los equipos a administrar.

Las actividades que se realizan en este módulo son:

- Generación de reportes estadísticos del uso de los recursos y servicios que presta los diferentes servidores de la empresa.
- Utilización de un sistema de gestión de software
- Monitoreo y detección de intrusos
- Análisis de eventos y reportes
- Control de logs

Las amenazas que este modulo previene son:

- Acceso no autorizado
- Ataques del tipo “Man in the middle”
- Reconocimiento de red
- Ataques a contraseñas
- Direcciones IP falsificadas
- Paquetes sniffer dentro de la red

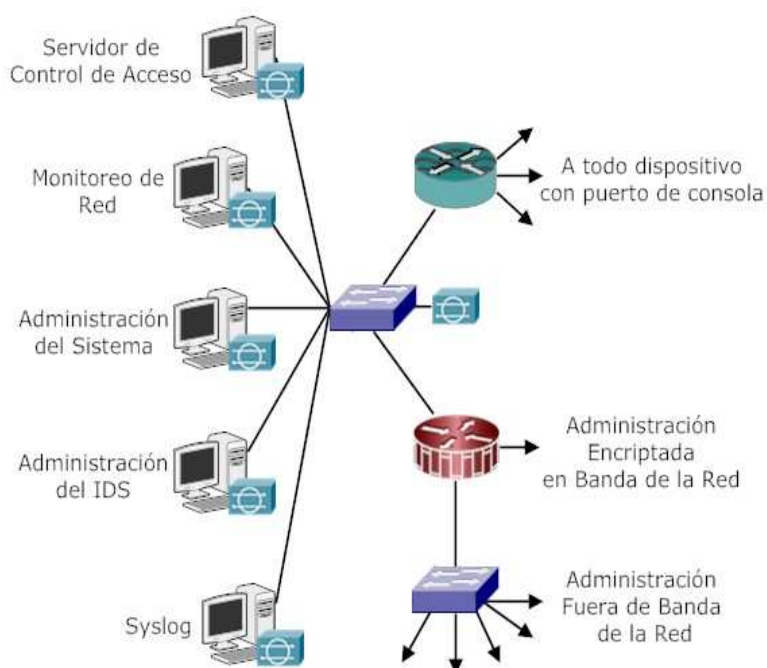


Figura 2.6 Diseño del Módulo de Administración

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.1.6 Perímetro de Distribución

El Perímetro de Distribución se encarga de la conectividad de los elementos que se encuentran en el Perímetro Empresarial con el módulo Central. Para la implementación de este módulo es necesario 2 switches de capa 3, ver Figura 2.7.

Las amenazas que este modulo previene son:

- Accesos no autorizados al Perímetro de Distribución
- Direcciones IP falsificadas
- Reconocimiento de la red
- Paquetes sniffer dentro de la red.

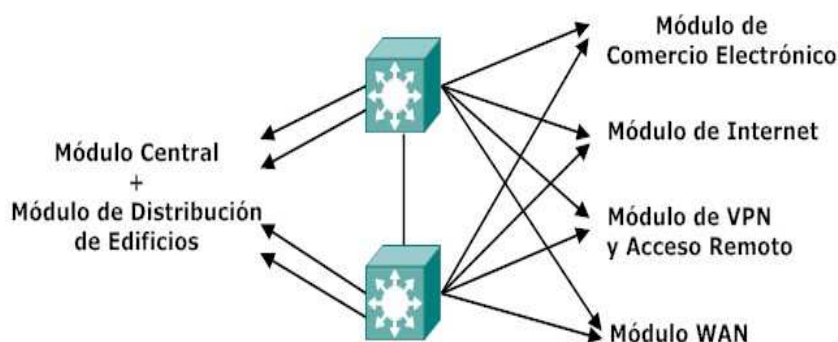


Figura 2.7 Diseño del Perímetro de Distribución

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.2 Perímetro Empresarial

De acuerdo al modelo "SAFE" de Cisco, el Perímetro Empresarial se compone de los siguientes módulos: Comercio Electrónico, VPN y de Acceso Remoto, Internet y WAN.

El módulo de Comercio Electrónico se encarga de ponderar el equilibrio entre el acceso y la seguridad. El módulo de Internet permite la conexión entre los usuarios internos a los servicios de Internet y el acceso de los usuarios externos a la información de los servicios públicos. El módulo de VPN y de Acceso Remoto permite concentrar el tráfico de VPN de los usuarios y sitios remotos.

2.2.3.2.1 Módulo de Comercio Electrónico

El módulo de Comercio Electrónico tiene el objetivo de equilibrar el acceso y la seguridad en los servicios, debido a esto se divide en tres componentes (Web, Aplicaciones y Base de Datos) proporcionando varios niveles de seguridad sin impedir el acceso.

Este modulo permite cumplir con el requerimiento planteado en la sección 2.1.2.3.1 para el Correo Electrónico.

Para este módulo los equipos que van a intervenir son: Servidor Web, Servidor de aplicaciones, Servidor de Base de Datos, 4 switches capa 2, un balanceador de carga, 2 Firewall's, un switch de capa 3 que incluye un módulo IDS, y un router, ver Figura 2.8.

Las amenazas que este modulo previene son:

- Acceso no autorizado a los servidores
- Ataques a la capa de aplicaciones
- Denegación de servicios
- Direcciones IP falsificadas
- Paquetes sniffer dentro de la red
- Reconocimiento de la red
- Redireccionamiento de puertos

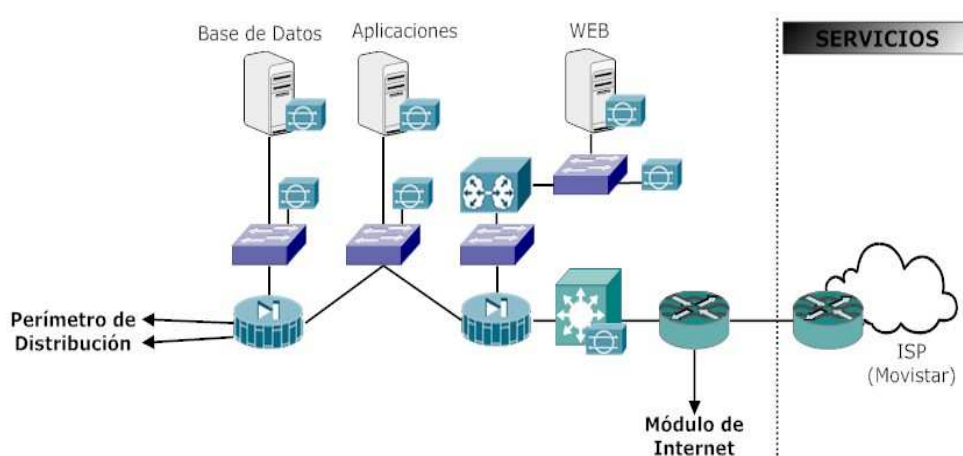


Figura 2.8 Diseño del Módulo de Comercio Electrónico

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.2.2 *Módulo de Internet*

El módulo de Internet permite la conexión entre los usuarios internos a los servicios de Internet y el acceso de los usuarios externos a la información de los servicios públicos. Para la implementación "SAFE" nos permite conectar un switch de capa 2 entre el firewall y el perímetro de distribución.

Este modulo permite cumplir con el requerimiento planteado en la sección 2.1.2.3.1 para el Acceso al Internet.

En este módulo los equipos que van a intervenir son: 3 switches de capa 2, un firewall que permita la implementación de una DMZ (servidor SMTP, servidor DNS y servidor Web/FTP) requerido en la empresa y un Inspector de Contenidos, ver Figura 2.9.

Las amenazas que este modulo previene son:

- Acceso no autorizado
- Ataques a la capa de aplicaciones
- Virus y trojan's
- Ataques a contraseñas
- Denegación de servicios
- Direcciones IP falsificadas
- Paquetes sniffer dentro de la red
- Reconocimiento de la red
- Redireccionamiento de puertos

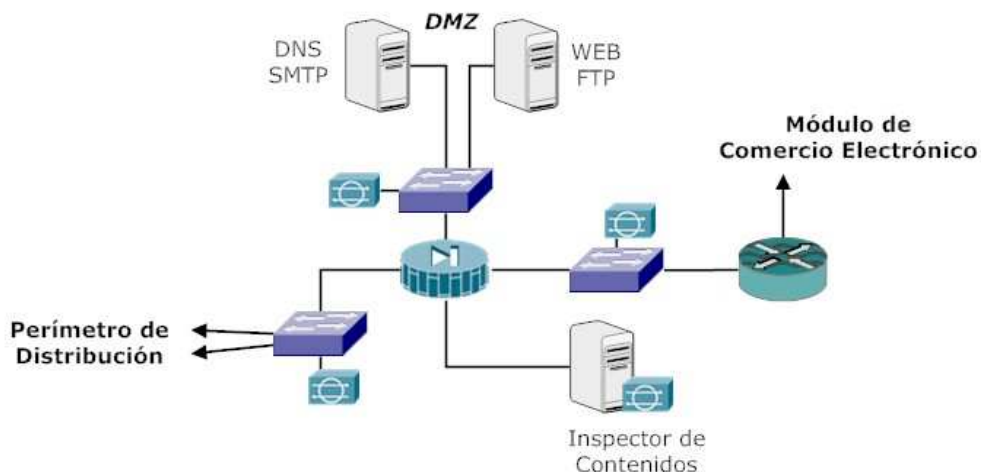


Figura 2.9 Diseño del Módulo de Internet

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.2.3 Módulo VPN y de Acceso Remoto

El módulo de VPN y de Acceso Remoto permite concentrar el tráfico de VPN de los usuarios y sitios remotos, para esto es necesario tener un concentrador de VPN que autentique a los usuarios remotos, un router VPN para la autenticación de los sitios remotos y un firewall para proporcionar seguridad a los servicios de acceso remoto, ver Figura 2.10.

Entre las alternativas disponibles para la implementación de este módulo tenemos:

- Autenticación con tarjeta inteligente y/o biométrica
- Túneles VPN de acceso remoto L2TP y/o PPTP
- Autoridades de certificación (CA)
- Mecanismo de resistencia keep-alive IKE
- VPN con Multiprotocol Label Switching (MPLS)

Las amenazas que este modulo previene son:

- Descubrimiento de la topología de la red de la empresa
- Ataques a contraseñas
- Acceso no autorizado
- Paquetes sniffer dentro de la red

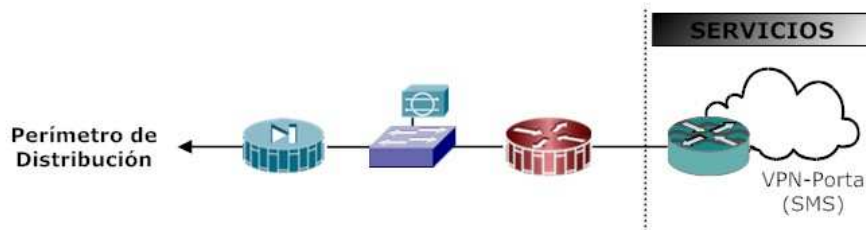


Figura 2.10 Diseño del Módulo VPN y Acceso Remoto

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

La empresa mantiene implementado una “VPN site-to-site” utilizando el protocolo L2TP²¹, que se implementa sobre IPSec y proporciona altos niveles de seguridad. Las conexiones de usuarios remotos están prohibidas por políticas de la empresa.

2.2.3.2.4 Módulo WAN

El módulo WAN permite mostrar la resistencia y la seguridad de las terminaciones WAN's, la resistencia se proporciona con una conexión dual a través de routers desde el proveedor del servicio de mensajería (Porta y Movistar) hacia el Perímetro de Distribución y la seguridad se proporciona utilizando características de seguridad del IOS (Sistema Operativo de Interconexión de Redes), ver Figura 2.11.

Las amenazas que este modulo previene son:

- Direcciones IP falsificadas
- Acceso no autorizado

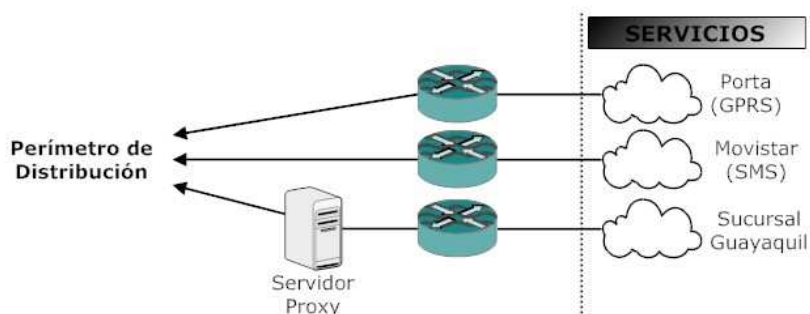


Figura 2.11 Diseño del Módulo WAN

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

²¹ Layer Two Tunneling Protocol

2.2.3.3 Diseño del Esquema de Seguridad para la Red de Datos

Utilizando el modelo de seguridad "SAFE" de Cisco se han elaborado dos diseños, un diseño completo y un diseño básico, que podrían ser implementados en un futuro dependiendo del presupuesto para la red de transmisión de datos que se disponga en la empresa.

Ambos diseños corresponden a una arquitectura modular, la cual permite crecer dependiendo de las necesidades que se presentan en la red de transmisión de datos. Inicialmente se puede implementar el diseño básico e ir creciendo hasta el punto de obtener en el mejor de los casos el diseño completo propuesto en este proyecto.

Todos los equipos requeridos para la implementación del diseño completo y básico, están basados en las recomendaciones dadas por el modelo de seguridad "SAFE" de Cisco.

2.2.3.3.1 Diseño Completo

El diseño completo, ver Figura 2.12, se ha elaborado en base a todas las recomendaciones descritas por el modelo de seguridad "SAFE" de Cisco.

A continuación se describen los módulos y los equipos a utilizados, ver Tabla 2.1.

- El *Campus Empresarial* consta de los siguientes módulos: Central + Distribución de Edificios, Edificios, Servidores, Perímetro de Distribución, Administración.
- El *Perímetro Empresarial* consta de los siguientes módulos: Comercio Electrónico, Internet, VPN y Acceso Remoto, WAN.

Tabla 2.1 Equipos Requeridos – Diseño Completo

Bloque	Módulo "SAFE" de Cisco	Cantidad	Equipos	
Campus Empresarial	Central + Distribución de Edificios	2	Switch de capa 3	
	Edificios	3	Switch de capa 2	
	Servidores	2	Switch de capa 3 con módulo IDS	
	Perímetro de Distribución	2	Switch de capa 3	
	Administración		1	Router
			1	Router con protección firewall
			1	NIDS
			2	Switch de capa 2
Perímetro Empresarial	Comercio Electrónico	1	Switch de capa 3 con módulo IDS	
		1	Router	
		1	Balancedor de Carga	
		2	Firewall	
		3	NIDS	
		4	Switch de capa 2	
	Internet		1	Firewall
			1	Router
			1	Inspector de Contenidos
			3	Switch de capa 2
			3	NIDS
	VPN y Acceso Remoto		1	Switch de capa 2
			1	NIDS
			1	Firewall
			1	Router con protección firewall
	WAN		3	Router

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

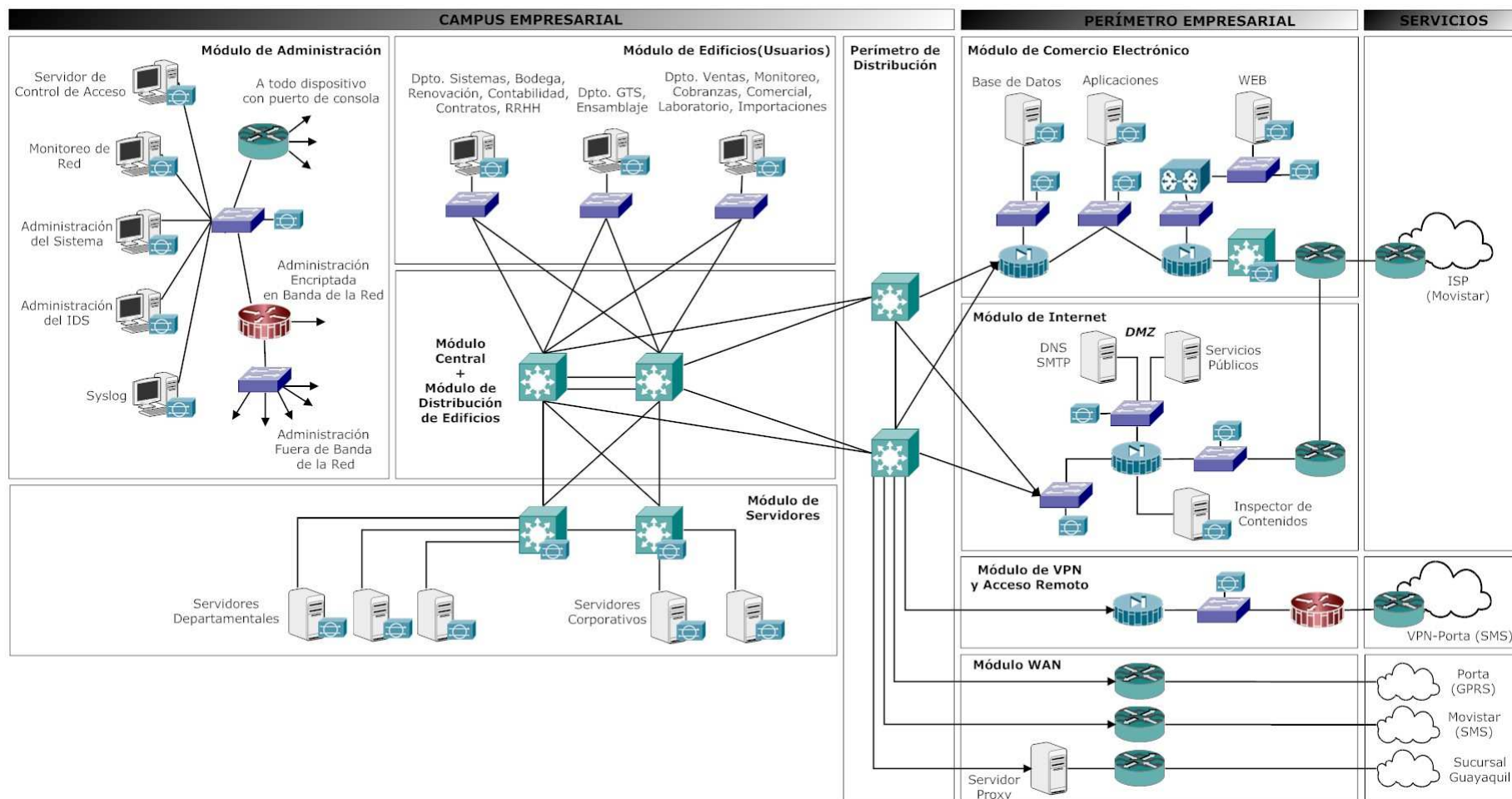


Figura 2.12 Diseño Completo de Seguridad para la Red de Transmisión de Datos

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.3.2 Diseño Básico

El diseño básico, ver Figura 2.13, tiene el objetivo de disminuir la redundancia física, que las protege de los fallos de los dispositivos disminuyendo el número de equipos utilizados en la implementación y que está sustentado en las alternativas propuestas por el modelo de seguridad “SAFE” de Cisco al diseño completo:

- Combinar el módulo Central con el módulo de Distribución de edificios
- Combinar el módulo de Comercio Electrónico con el módulo de Internet
- Utilizar un switch de capa 2 en el módulo de Servidores
- Minimizar la redundancia en la red
- Utilizar únicamente el segmento “En Banda” para el módulo de Administración.
- Reducir el número de equipos utilizados, tales como: switches (capa 2 y 3), firewalls, routers, IDS entre otros.

Los equipos requeridos para la implementación del diseño básico de acuerdo a las recomendaciones de SAFE son, ver Tabla 2.2.

Tabla 2.2 Equipos Requeridos – Diseño Básico

Bloque	Módulo “SAFE” de Cisco	Cantidad	Equipos	
Campus Empresarial	Central + Distribución de Edificios	1	Switch de capa 3	
	Edificios	2	Switch de capa 2	
	Servidores	1	Switch de capa 2	
	Perímetro de Distribución	1	Switch de capa 3	
	Administración		1	NIDS
			1	Router con protección firewall
			1	Switch de capa 2
Perímetro Empresarial	Comercio Electrónico e Internet	1	Router	
		1	Inspector de Contenidos	
		1	Firewall	
		2	Switch de capa 2	
		2	NIDS	
	VPN y Acceso Remoto	1	Router	
	WAN	3	Router	

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

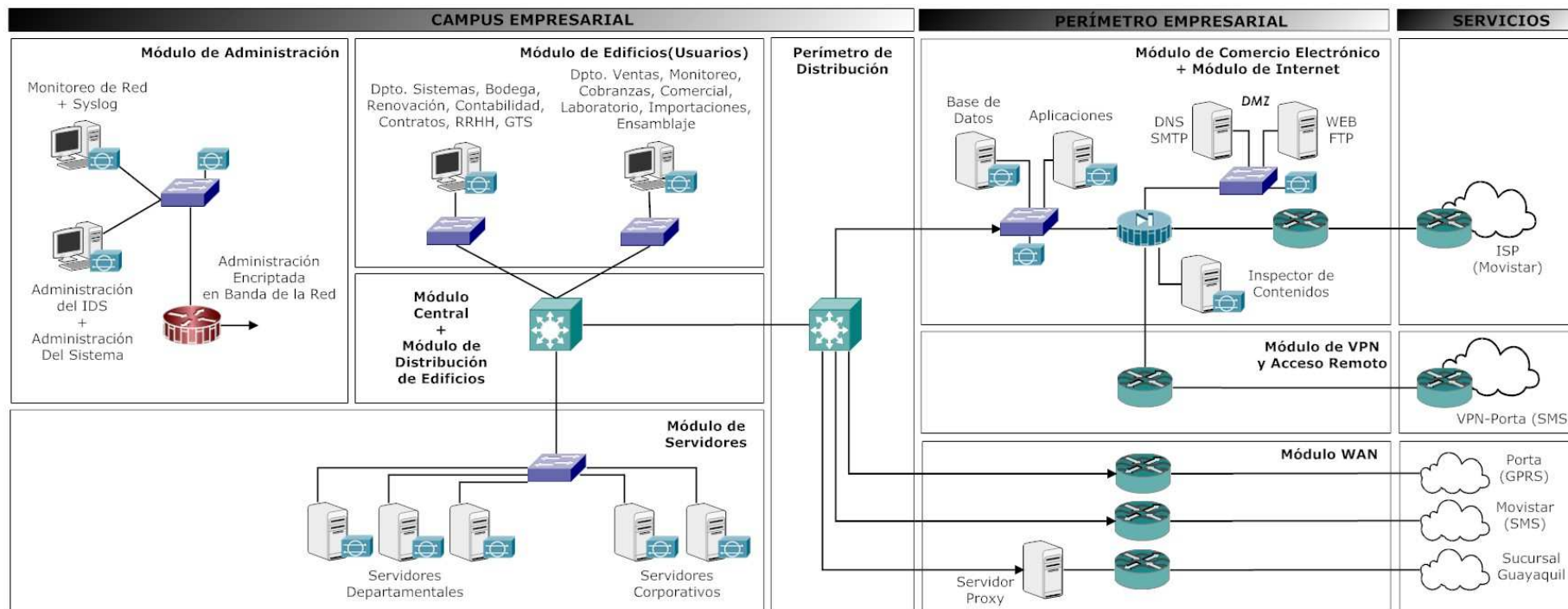


Figura 2.13 Diseño Básico de Seguridad para la Red de Transmisión de Datos

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

2.2.3.3.3 Análisis Comparativo

Para la implementación del diseño completo, es necesario un mayor equipamiento que el utilizado para el diseño básico, esto se debe a que el diseño completo mantiene un control exhaustivo sobre cada módulo y la redundancia de la red esta fuertemente implementada. Por el contrario en el diseño básico se mantiene un buen nivel de rendimiento, brindando seguridad e integridad a la red de datos a un costo menor.

Tomando en cuenta las consideraciones antes mencionadas, la mejor alternativa sería el diseño completo, pero si la empresa lo considera una implementación costosa, se podría optar por implementar el diseño básico.

Para la implantación del diseño básico se elaborara un cronograma de actividades que tendrá una duración de un año y se destinara un porcentaje del presupuesto del Departamento de Sistemas; la ejecución consta de las siguientes etapas:

- Implementación de las seguridades físicas
- Adquisición e implementación de hardware y software del diseño básico
- Aplicación de las políticas y normas de seguridad

2.3 POLÍTICAS Y NORMAS DE SEGURIDAD

Para la elaboración de políticas y normas orientadas a disminuir las amenazas y riesgos existentes en la empresa, se utilizó como guía la norma ISO/IEC 17799; que provee un estándar para realizar la gestión de la seguridad de la información.

Las políticas y normas de seguridad planteadas en esta sección van a permitir cubrir con los requerimientos de seguridad descritos en las secciones 2.1.2.2 y 2.1.3

OBJETIVOS

- Mejorar la seguridad en la red de datos
- Elaborar y retroalimentar las políticas y normas de seguridad que deben seguir los usuarios de la red de datos, para de esta forma obligarlos a proteger y manejar de mejor manera los activos informáticos de la empresa.

JUSTIFICACIÓN

El Gerente de Sistemas y Monitoreo, el Jefe de Sistemas, los asistentes y operarios tienen el compromiso y la responsabilidad de dedicar el tiempo y recursos suficientes para asegurar que los componentes activos y pasivos de la empresa estén adecuadamente protegidos, ante cualquier eventualidad que refleje una debilidad en los sistemas informáticos.

Los equipos y componentes existentes en la red son recursos importantes y vitales, sin ellos la empresa se quedaría rápidamente fuera del negocio, dando como resultado la pérdida económica y su desprestigio. Por tal razón la Junta Directiva tiene el deber de preservarlos, utilizarlos y renovarlos, tomando las acciones apropiadas para asegurar que la información y los sistemas informáticos estén protegidos ante cualquier clase de amenaza o riesgo.

La finalidad principal de las políticas y normas de seguridad es proporcionar instrucciones específicas de cómo mantener segura la red de transmisión de datos, los equipos de computación y la información almacenada en los servidores.

ALCANCE

La creación, elaboración y difusión de las políticas y normas de seguridad a los miembros de la empresa servirán en el futuro para tener un sistema informático confiable y operativo.

RESPONSABLES

Los siguientes funcionarios son los responsables, en distintos grados, de la seguridad en la empresa:

El **Gerente de Sistemas y Monitoreo** es responsable de:

- Dirigir investigaciones de incidentes y problemas relacionados con la seguridad, para poder recomendar las medidas pertinentes.
- Manejar los recursos y presupuestos de la implantación de las políticas y normas de seguridad.
- Verificar la implantación y velar por el cumplimiento de las políticas y normas de seguridad a lo largo de toda la organización, en coordinación con la Junta Directiva.

El **Jefe de Sistemas** es responsable de:

- Adquirir e implantar productos de seguridad informática
- Proporcionar apoyo técnico y administrativo en los asuntos concernientes a la seguridad.
- Establecer controles de acceso apropiados a cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y llevar a cabo tareas de seguridad en los sistemas que administra.
- Diseñar un plan estratégico con plazos y metas para la elaboración, actualización y ejecución de los planes de seguridad informáticos.
- Ser el líder de las actividades de prevención y recuperación en el caso de: fallo del sistema informático, hackers, virus informáticos y desastres naturales.
- Supervisar el avance de los planes de seguridad a implementarse en la empresa.

Los **Asistentes y Operarios** son responsables de:

- Elaborar y ejecutar las políticas y normas de seguridad informática para evitar riesgos que puedan generar problemas en la red de transmisión de datos.
- Diseñar, instalar, mantener e implementar controles para proteger la información que circula por la red de acuerdo a las políticas y normas de seguridad.

El **resto de usuarios** son responsables de:

- Cumplir con todas las políticas y normas de la empresa relativas a la seguridad.
- Conocer y aplicar las políticas y normas de seguridad para el manejo de información y de sistemas informáticos.
- Mantener la lealtad y sinceridad para con la empresa y sus compañeros de trabajo, ya que no servirá de nada tener las políticas y normas de seguridad si un usuario las quebranta.
- Reportar a su jefe inmediato cualquier evento anormal como: virus, intrusos, pérdida de datos u otras actividades poco frecuentes que puedan implicar la seguridad de la empresa o sus recursos informáticos.
- Utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para actividades que estén directamente relacionadas con el trabajo de la empresa.

2.3.1 POLÍTICAS DE SEGURIDAD

2.3.1.1 Políticas de Seguridad en Hardware, Dispositivos Periféricos y otros Equipos

2.3.1.1.1 De la Instalación del Equipo de Computo

- Todos los equipos de computo que estén conectados a la red de transmisión de datos de la empresa, deben sujetarse a las normas y procedimientos de instalación que emite el Departamento de Sistemas y Monitoreo.
- La instalación de los equipos de computo será ejecutado por el Departamento de Sistemas y Monitoreo, previo registro de seriales.

- Los equipos de cómputo requieren estar ubicados en un área que cumpla con los siguientes requerimientos: seguridad física, condiciones ambientales controladas, alimentación eléctrica ininterrumpida (UPS's) y un control de acceso establecido por el Departamento de Sistemas y Monitoreo.

2.3.1.1.2 Del Mantenimiento del Equipo de Cómputo

- Al Departamento de Sistemas y Monitoreo, le corresponde la realización del mantenimiento preventivo y correctivo de los equipos de computo, la conservación de su instalación (actualización de parches), la verificación de la seguridad física de acuerdo a las normas establecidas por ellos.
- Si el manteniendo es contratado a terceros el Departamento de Sistemas y Monitoreo supervisara los trabajos.

2.3.1.1.3 De la Seguridad Física del Equipo de Cómputo

- La protección física de cada uno de los equipos de computo, corresponde al usuario asignado en el momento de la instalación, para el caso de que el equipo sea movido se notificará de inmediato al Departamento de Sistemas y Monitoreo.

2.3.1.2 Políticas de Seguridad para Control de Acceso a los Sistemas e Información

2.3.1.2.1 Del Acceso a las Áreas Críticas

- El acceso a las instalaciones del cuarto de telecomunicaciones u otras áreas que contengan equipos activos de la red, se realizara dependiendo de las normas y procedimientos establecidos por el Departamento de Sistemas y Monitoreo.
- En caso de emergencia, el acceso al cuarto de telecomunicaciones estará sujeto a las disposiciones del Gerente de Sistemas y Monitoreo.

2.3.1.2.2 Del Control de Acceso a la Red

- El acceso a los servicios de red e información, será monitoreado y controlado durante los 365 días del año las 24 horas del día.

- El acceso de los usuarios a los servicios de red e información, será gestionado de acuerdo a las actividades laborales asignadas a cada uno de ellos, sujetándose a las normas y procedimientos emitidos por el Departamento de Sistemas y Monitoreo.

2.3.1.2.3 Del Accesos al Sistema Operativo

- La administración a los sistemas operativos usados en la empresa dependerá de las normas y procedimientos establecidos por el Departamento de Sistemas y Monitoreo.

2.3.1.2.4 De la Creación, Identificación y Autenticación de los Usuarios

- El Departamento de Sistemas y Monitoreo identificara al usuario que utiliza los servicios de red e información, a través de un sistema de identificación y autenticación de usuarios.
- Las contraseñas serán estructuradas y administradas, de acuerdo a las normas y procedimientos establecidas por el Departamento de Sistemas y Monitoreo.

2.3.1.2.5 Del Acceso a Documentos y Archivos

- El acceso a documentos, archivos e información confidencial se manejará de acuerdo a las normas y procedimientos establecidos por el Departamento de Sistemas y Monitoreo, garantizando su integridad.

2.3.1.2.6 Del Acceso Remoto

- El Departamento de Sistemas y Monitoreo es el responsable de bloquear a los usuarios el acceso remoto.

2.3.1.2.7 Del Acceso a Correo Electrónico e Internet

- El Departamento de Sistemas y Monitoreo deberá emitir normas y procedimientos para el acceso a los servicios de correo electrónico e Internet, garantizando de esta forma su disponibilidad.
- El Departamento de Sistemas y Monitoreo implementara técnicas de filtrado para restringir el acceso a información inapropiada existente en el correo electrónico e Internet.

2.3.1.3 Políticas de Seguridad para Recursos Computacionales y de Red

2.3.1.3.1 Configuración de la Red

- La configuración de los equipos de cómputo, deberá garantizar un rendimiento que satisfaga las necesidades de los usuarios de la red, manteniendo controles de acceso, privilegios y restricciones.
- El Jefe de Sistemas deberá garantizar la seguridad, integridad y disponibilidad de los servicios que presta la red.

2.3.1.3.2 De la Administración de Base de Datos y Aplicaciones

- El acceso a los sistemas, módulos, menús, opciones, enlaces y cualquier otro componente de una aplicación, deberá ejecutarse de acuerdo a los perfiles de cada usuario.
- El Departamento de Sistemas y Monitoreo garantizara la integridad, disponibilidad y confiabilidad de los datos almacenados en las bases de datos.

2.3.1.3.3 De los Respaldos y Recuperación de Archivos

- El Departamento de Sistemas y Monitoreo garantizara la integridad, confidencialidad y disponibilidad de la información, la obtención periódica y la restauración de los respaldos en el momento que la empresa lo requiera de acuerdo a las normas y procedimientos vigentes.

2.3.1.4 Políticas de Seguridad para la Adquisición, Registro, Almacenamiento y Manejo de Software Comercial

- Todo software adquirido por la empresa deberá ser previamente planificado, justificado, autorizado, probado, documentado y poseer su respectiva licencia.
- Todo software adquirido por la empresa deberá ser registrado, almacenado y etiquetado de acuerdo a las normas establecidos por el Departamento de Sistemas y Monitoreo.

2.3.1.5 Políticas de Seguridad para el Desarrollo y Mantenimiento de Software Institucional.

- El uso de controles y procedimientos que garanticen la calidad y seguridad en todas las etapas del proceso de desarrollo, estarán bajo la supervisión de los responsables del desarrollo del software institucional.
- En el desarrollo de software institucional, se obligara a seguir procesos formales de desarrollo, de acuerdo a la metodología seleccionada por el Departamento de Sistemas y Monitoreo.

2.3.1.6 Políticas de Seguridad para Combatir el Crimen Cibernético

2.3.1.6.1 De los Ataques Internos, Externos y Virus

- El Departamento de Sistema y Monitoreo deberá establecer normas y procedimientos para disminuir los daños inducidos por ataques internos, externos y de virus.
- El Departamento de Sistemas y Monitoreo proporcionará un software antivirus para minimizar los daños provocados por los virus.

2.3.1.7 Políticas de Seguridad para Contingencias ante Desastres

- El Departamento de Sistemas y Monitoreo deberá contar con un plan de contingencia ante desastres naturales o de entorno, permitiendo de esta manera restaurar los servicios de la red de una forma eficiente, rápida y con una perdida económica e informática mínima.

2.3.1.8 Políticas de Seguridad para la Capacitación del Personal Técnico

- El Departamento de Sistemas y Monitoreo deberá contar con un plan de capacitación para el personal encargado del desarrollo de software, administración y mantenimiento de equipos de cómputo y de red.

2.3.1.9 Políticas de Seguridad de los Sistemas de Protección (UPS)

- Las instalaciones del cuarto de telecomunicaciones y las estaciones de trabajo, deben contar con sistemas de protección que salvaguarden los equipos contra fallas del suministro de energía eléctrica.

2.3.2 NORMAS DE SEGURIDAD

2.3.2.1 Normas para la Instalación del Equipo de Computo

- El personal del Departamento de Sistemas y Monitoreo estará a cargo de la instalación, actualización y/o reemplazo de los equipos de computo y comunicaciones, de acuerdo a los requerimientos del departamento interesado.
- El Departamento de Sistemas y Monitoreo proporcionará instalaciones eléctricas y de red adecuadas para el correcto funcionamiento de los equipos de cómputo.
- El Departamento de Sistemas y Monitoreo encargara a un asistente registrar en un inventario el ingreso de nuevos equipos, su movimiento y el cambio de hardware en los mismos.

2.3.2.2 Normas para el Mantenimiento del Equipo de Computo

- El Jefe de Sistemas será el responsable de elaborar un cronograma semestral y anual para el mantenimiento preventivo de los equipos de cómputo.
- El Jefe de Sistemas encargara a un asistente realizar el mantenimiento preventivo y correctivo de los equipos de cómputo.
- La contratación de terceras persona para el mantenimiento de los equipos se manejará de acuerdo al Reglamento de Contratación firmado.
- El Jefe de Sistemas encargara a un asistente la supervisión del cumplimiento de dichos contratos de mantenimiento.

2.3.2.3 Normas de la Seguridad Física del Equipo de Computo

- La protección física de cada uno de los equipos de computo, corresponde al usuario asignado en el momento de la instalación, para el caso de que existiese algún tipo de daño o cambio se notificará de inmediato al Departamento de Sistemas y Monitoreo.

2.3.2.4 Normas del Acceso Físico a las Áreas Críticas

- El Gerente de Sistemas y Monitoreo será el responsable de la implementación de controles de acceso físico en las áreas críticas, a través de tarjetas magnéticas o claves de acceso.
- El Jefe de Sistemas es responsable de controlar el acceso de proveedores y contratistas al cuarto de telecomunicaciones u otras áreas que contengan equipos activos de la red.

2.3.2.5 Normas de Control de Acceso a la Red

- El Jefe de Sistemas encargara a un asistente la responsabilidad de dar acceso a los servicios de la intranet (configuraciones, aplicaciones, documentos, etc.) a los usuarios finales, siempre y cuando exista la aprobación del jefe del departamento interesado y del Jefe de Sistemas.
- El Jefe de Sistemas o un asistente serán las personas quienes monitoreen, administren y controlen el correcto funcionamiento de los servicios en la red.
- El Jefe de Sistemas debe administrar el acceso lógico a los equipos de cómputo especializados (servidores, routers, bases de datos, switches, etc.) que están conectado a la red de datos.

2.3.2.6 Normas del Control de Software y Acceso al Sistema Operativo

- El Jefe de Sistemas encargara a un asistente la responsabilidad de controlar el software instalado en los equipos de cómputo, incluyendo la elaboración de un acta de entrega-recepción del software instalado.
- El Jefe de Sistemas encargara a un asistente el control de los permisos de acceso de los usuarios al sistema operativo, comandos y configuración de los equipos de cómputo.

2.3.2.7 Normas de Creación, Identificación y Autenticación de Usuarios

- El Jefe de Sistemas será el responsable de crear cuentas de usuario, previa notificación escrita o verbal por parte del Jefe del departamento interesado.

- El Departamento de Sistemas será el encargado de implementar, configurar y controlar el sistema de identificación y autenticación de usuarios.
- El usuario deberá cambiar la contraseña inicial en el primer ingreso a su cuenta, dicha contraseña no debe ser relacionada con datos comunes, tales como apelativos, nombres de familiares, fechas nacionales, etc.
- La fecha de expiración de la contraseña no sobrepasará los 90 días
- La longitud mínima de la contraseña deberá ser de 6 caracteres alfanuméricos (letras, números y símbolos).
- El Jefe de Sistemas podrá habilitar, deshabilitar y borrar una cuenta de usuario previa notificación escrita o verbal por parte del jefe de departamento interesado.

2.3.2.8 Normas de Acceso a Documentos y Archivos

- El Jefe de Sistemas se encargara de proporcionar los respectivos permisos de acceso a documentos y archivos considerados restringidos.

2.3.2.9 Normas del Control de Acceso Remoto

- El Jefe de Sistemas estará encargado de bloquear el acceso remoto de los usuarios a los servicios de Internet, correo electrónico y servidores, por solicitud del Gerente de Sistemas.

2.3.2.10 Normas del Acceso a Correo Electrónico e Internet

- El Jefe de Sistemas deberá difundir a todo el personal los procedimientos de seguridad para el uso adecuado del Internet y correo electrónico.
- Todos los departamentos que se hallen conectados a la red, a través de un proveedor de servicios de Internet distinto al que usa la empresa, deberán acoplarse a las políticas de configuración, seguridad y acceso que dicte el Departamento de Sistemas y Monitoreo.

2.3.2.11 Normas de Configuración de la Red

- El Jefe de Sistemas será el responsable de la configuración de red en los equipos de cómputo y de comunicación.

- El Jefe de Sistemas encargara a un asistente la responsabilidad de realizar la configuración de red en cada una de las estaciones de trabajo.
- El Jefe de Sistemas será el responsable de asignar y administrar las direcciones IP para las estaciones de trabajo, equipos de cómputo y de comunicación.

2.3.2.12 Normas de la Administración de Base de Datos y Aplicaciones

- El Jefe de Sistemas será responsable de definir y asignar los perfiles de usuario, de acuerdo a la función, jerarquía y rol que cumple cada usuario.
- El Jefe de Sistemas encargara a un asistente la responsabilidad de realizar chequeos permanentes de los archivos .log generados, garantizando de esta manera la integridad, disponibilidad y confiabilidad de la información en las bases de datos.

2.3.2.13 Normas de los Respaldos y Recuperación de Archivos de Información

- El Jefe de Sistema es el responsable de elaborar e implementar un método para obtener los respaldos de la información, con este método se llevara a cabo un control de respaldos.
- El Jefe de Sistemas encargara a un asistente la responsabilidad de obtener los respaldos de la información, en periodos diarios, semanales, mensuales y anuales.
- El asistente responsable de la obtención de los respaldos debe saber: que información se va a respaldar, con qué periodicidad, qué medios físico se va a utilizar, en que lugar se lo va a albergar y cómo deberá ser restaurada la información.
- El asistente responsable de los respaldos realizara pruebas de restauración semanales, para comprobar la integridad, disponibilidad y confiabilidad de la información. Luego de esto se generaran 3 copias las cuales deben ser entregadas al Jefe de Sistemas.
- El Jefe de Sistemas deberá guardar físicamente los respaldos de la información en un lugar seguro dentro de la empresa, fuera de la empresa y una copia será entregada al Gerente de Sistemas y Monitoreo.

- Los respaldos de los datos almacenados en las estaciones de trabajo son responsabilidad de los usuarios.

2.3.2.14 Normas para Adquirir, Registrar, Almacenar y Administrar Software Corporativo

- El software adquirido por la empresa (CD's, DVD's originales) deberá estar albergado en una caja de seguridad dentro del Departamento de Sistemas y Monitoreo.
- El Jefe de Sistemas encargara a un asistente la responsabilidad de mantener actualizada la base de datos del inventario de software, incluyendo las licencias adquiridas e instaladas en las estaciones de trabajo y servidores.
- Corresponde al Departamento de Sistemas y Monitoreo emitir los procedimientos de administración básica de software para cualquier equipo dentro de la red.
- Dependiendo de la actividad del usuario se deberá prohibir o no la instalación del software: Explorer, Messenger y Outlook, cuyo principal objetivo es establecer una comunicación hacia el exterior de la empresa.
- Los instaladores tales como: Antivirus, utilitarios, software institucional, etc., deberán ubicarse en carpetas compartidas en el servidor de archivos.
- Para evitar el deterioro de los CD's y DVD's originales, toda instalación se realizara desde una copia del original.
- Cada usuario es responsable del software instalado en su maquina, si se realiza algún cambio eventual se deberá notificar inmediatamente al Departamento de Sistemas y Monitoreo.
- Queda terminantemente prohibido la instalación de software no autorizado o pirata en las estaciones de trabajo.
- El Jefe de Sistemas encargara a un asistente la responsabilidad de realizar la instalación del nuevo software y/o actualización del software existente, previa autorización.

2.3.2.15 Norma para el Desarrollo del Software Institucional

- Todos los sistemas informáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con los recursos de la empresa se mantendrán como propiedad de la empresa.
- Los desarrolladores del software institucional serán los responsables de generar la metodología para el desarrollo y/o actualización del mismo.
- Todo sistema nuevo o actualizado deberá poseer: manuales de usuario, de administración y de instalación actualizados, de acuerdo a los estándares establecidos por la Departamento de Sistemas y Monitoreo.

2.3.2.16 Normas de los Ataques Internos, Externos y Virus

- El asistente autorizado por el Jefe de Sistemas deberá: instalar herramientas de monitoreo, filtros para el correo electrónico e información derivada de Internet, de esta manera se minimizara los posibles daños por ataques internos, externos y virus.
- El asistente autorizado por el Jefe de Sistemas instalara sistemas antivirus y de detección de intrusos, minimizando de esta forma los daños ocasionados por ataques internos, externos y virus.

2.3.2.17 Normas para Contingencia ante Desastres

- El Jefe de Sistemas y sus asistentes deberán emitirán un plan de contingencias ante desastres naturales y de entorno.
- El Jefe de Sistemas encargara a un asistente la responsabilidad de difundir a todo el personal el plan de contingencia ante desastres naturales y de entorno, para que en un lapso muy corto de tiempo, la empresa regrese a sus actividades normales y que las pérdidas económicas sean mínimas.

2.3.2.18 Normas para la Capacitación Técnica del Personal

- El Jefe de Sistemas presentara al Jefe de Personal un cronograma anual de los cursos de capacitación requeridos para los asistentes, con el objetivo de mejorar el desempeño en sus funciones.

2.3.2.19 Normas de los Sistemas de Protección

- El Jefe de Sistemas encargara a un asistente la responsabilidad de vigilar y mantener operativo los sistemas de protección UPS (Uninterruptible Power Supply), ya que permiten salvaguarde los equipos del centro de computo contra fallas en el suministro de energía eléctrica.

2.3.2.20 Normas Generales y Sanciones

- Cada Departamento de la empresa tiene la obligación de emitir planes de contingencia relacionados con las actividades críticas que ellos realicen.
- El Departamento de Sistemas y Monitoreo de la empresa, no ejecutara control sobre el contenido de la información que circula por la red de transmisión de datos, quedando bajo la responsabilidad del funcionario que lo utilice. No obstante, el departamento a través del Jefe de Sistemas pondrá en marcha herramientas de control que analicen, monitoreen, detecten y reporten el uso inadecuado de este servicio.
- El departamento de Sistemas y Monitoreo tiene la autoridad para permitir o negar el acceso a la red a cualquier funcionario que viole las políticas y normas de seguridad, o que interfiera con los derechos de otros usuarios.
- El incumplimiento de las políticas establecidas ocasionarán la cancelación temporal de la cuenta de acceso a cualquier servicio dentro de la red de datos; y en algunos casos, la suspensión definitiva del mismo.
- El Departamento de Sistemas y Monitoreo deberá determinar la sanción para cualquier tipo de abuso cometido dentro de la red de datos.

A continuación se presenta un resumen donde se relaciona cada Política de Seguridad con su respectiva Norma de Seguridad; ver Tabla 2.3.

Tabla 2.3 Políticas y Normas de Seguridad

Políticas de Seguridad		Normas de Seguridad
En Hardware, Dispositivos Periféricos y otros Equipos	De la Instalación del Equipo de Computo	Normas para la Instalación del Equipo de Computo
	Del Mantenimiento del Equipo de Cómputo	Normas para el Mantenimiento del Equipo de Computo
	De la Seguridad Física del Equipo de Cómputo	Normas de la Seguridad Física del Equipo de Computo
Para Control de Acceso a los Sistemas e Información	Del Acceso a las Áreas Críticas	Normas del Acceso Físico a las Áreas Críticas
	Del Control de Acceso a la Red	Normas de Control de Acceso a la Red
	Del Accesos al Sistema Operativo	Normas del Control de Software y Acceso al Sistema Operativo
	De la Creación, Identificación y Autenticación de los Usuarios	Normas de Creación, Identificación y Autenticación de Usuarios
	Del Acceso a Documentos y Archivos	Normas de Acceso a Documentos y Archivos
	Del Acceso Remoto	Normas del Control de Acceso Remoto
Para Recursos Computacionales y de Red	Del Acceso a Correo Electrónico e Internet	Normas del Acceso a Correo Electrónico e Internet
	Configuración de la Red	Normas de Configuración de la Red
	De la Administración de Base de Datos y Aplicaciones	Normas de la Administración de Base de Datos y Aplicaciones
Para la Adquisición, Registro, Almacenamiento y Manejo de Software Comercial	De los Respaldos y Recuperación de Archivos	Normas de los Respaldos y Recuperación de Archivos de Información
Para el Desarrollo y Mantenimiento de Software Institucional	-----	Normas para Adquirir, Registrar, Almacenar y Administrar Software Corporativo
Para el Desarrollo y Mantenimiento de Software Institucional	-----	Norma para el Desarrollo del Software Institucional
Para Combatir el Crimen Cibernético	De los Ataques Internos, Externos y Virus	Normas de los Ataques Internos, Externos y Virus
Para la Capacitación del Personal Técnico	-----	Normas para la Capacitación Técnica del Personal
De los Sistemas de Protección (UPS)	-----	Normas de los Sistemas de Protección
-----	-----	Normas Generales y Sanciones

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

CAPITULO 3.

PROPUESTA TÉCNICA ECONÓMICA 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 completo y básico descrito en el capítulo anterior, ver Tabla 2.1 y 2.2; además de la evaluación del costo referencial.

3.1 ESPECIFICACIONES TÉCNICAS

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 FÍSICA

Para la implementación del diseño de la seguridad física la empresa necesita los siguientes equipos, ver Tabla 3.1:

Tabla 3.1 Especificaciones de los Equipos Requeridos - Seguridad Física

Equipos	Equipos Requeridos
UPS	1
Planta Eléctrica	1

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito, 2008.

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

- Cuarto de Telecomunicaciones remodelado
- Puertas Eléctricas
- Sistema de Cableado Estructurado
- Sistema contra Incendios

Los equipos requeridos para la seguridad física deben cumplir con las siguientes especificaciones técnicas mínimas:

a) Cuarto de Telecomunicaciones remodelado

- Dimensiones:
 - 3 mts de ancho y 2.50 mts de profundidad
- Corregir fallas
- Colocar piso y techo falso
- Revisión del sistema eléctrico
- Instalación de entrada para aire acondicionado
- Refuerzo de ventanas con mallas

a) Puerta Eléctrica

- Cantidad: 2
- Dimensiones:
 - 2.10 mts de alto y 1.20 mts de ancho
- Material:
 - Marco de Aluminio
 - Vidrio blindado de 6 mm.
- Lector de Banda Magnética (Lector de ranura)

b) Cableado Estructurado

- Estándares internacionales como el EIA/TIA-568A, EIA/TIA-569, EIA/TIA-606, EIA/TIA-607.
- Puntos: 73
- Cable: UTP categoría 5e

c) UPS

- Cantidad: 1
- Potencia: 8KVA Escalable, ver Anexo 14
- Tecnología: On Line
- Tiempo de respuesta: <4ms
- Tiempo de recarga de batería: < 8 horas
- Duración típica de reserva a media carga: 15 minutos (6.4Kw)
- Duración típica de reserva con carga completa: 5 minutos (3.2Kw)
- Frecuencia: 50/60 Hz. (auto-sensible)
- Entrada de voltaje 110V AC
- Tomas de corriente: mínimo 5
- Gabinete metálico con conexión a tierra
- Puerto para conexión con software para cierre automático y ordenado de aplicaciones y sistema operativo. Monitoreo de tensión de alimentación y salida, consumo total, estado de carga de la batería
- Botón de control para prender, apagar, probar, silenciar alarmas y arrancar en frío.
- Protección de sobrecarga, corto circuito y calentamiento
- Protocolo remoto: SNMP, TELNET, HTTP
- Interfase Ethernet y software de administración para Windows XP/2000/2003 y NT con capacidad para cierre de múltiples servidores y/o múltiples plataformas con una sola UPS.

d) Planta de energía eléctrica (motogenerador)

- Cantidad: 1
- Potencia:
 - 70 KVA (1800 RPM), ver Anexo 14
- Fase: Bifásico
- Papel de control digital
- Tiempo de respuesta: 5.1 min a carga completa
- Sistema de arranque: Eléctrico y manual de enrollado automático
- Tomas: 110/220 VAC-12 VDC

- Frecuencia: 60 Hz
- Combustible: Diesel
- Tanque de combustible: Mínimo 10 galones
- Motor de arranque de 12 V
- Alternador de carga de baterías de 12 V
- Sistema de Enfriamiento: Aire Forzado
- Batería y cables de batería

e) Sistema contra incendios

- Instalación bajo la norma N.F.P.A-72 (National Fire Protection Association)
- Tipo de alarma audibles y o visibles
- Tipo de activación:
 - Manual, mediante pulsador de incendios
 - Automática, mediante disparo de detector de incendios
- 68 detectores de humo fotoeléctricos
- Agente extintor: polvo químico, espuma, dióxido de carbono (CO₂)
- Rango de detección mínimo: 9m lineales
- Sistema independiente, es decir, que cuenta con su fuente propia de energía, transformador y batería.
- Equipos aprobados por: "NFPA" y "UL SmokAlarm-USA"

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 del diseño completo y básico.

La empresa dispone de equipos que serán incluidos ya sea en la implementación del diseño completo o del diseño básico, ver Anexo 15; no obstante para cumplir con los objetivos planteados por cada módulo será necesaria la adquisición de nuevos equipos. Estos equipos deben cumplir con las recomendaciones dadas por "SAFE" de Cisco, el cual sugiere utilizar dispositivos específicos en los diferentes módulos que integran el sistema de seguridad en la red.

3.1.2.1 Equipos Activos - Diseño Completo

A continuación se detallan los equipos requeridos para la implementación del diseño completo, ver Tabla 3.2.

Tabla 3.2 Especificaciones de los Equipos Requeridos - Diseño Completo

Bloque	Módulo "SAFE" de Cisco	Cantidad	Equipos Existentes	Equipos Requeridos	Equipos	
Campus Empresarial	Central + Distribución de Edificios	2	0	2	Switch de capa 3 ^(a)	
	Edificios	3	0	3	Switch de capa 2 ^(b)	
	Servidores	2	0	2	Switch de capa 3 con módulo IDS ^(c)	
	Perímetro de Distribución	2	0	2	Switch de capa 3 ^(a)	
	Administración		1	1	0	Router
			1	0	1	Router con protección firewall ^(d)
			2	1	1	Switch de capa 2 ^(e)
Perímetro Empresarial	Comercio Electrónico	1	0	1	Switch de capa 3 con módulo IDS ^(c)	
		1	1	0	Router	
		1	0	1	Balancedor de carga ^(f)	
		2	0	2	Firewall ^(g)	
		4	2	2	Switch de capa 2 ^(e)	
	Internet	1	1	0	Firewall	
		1	0	1	Router ^(h)	
		1	0	1	Inspector de Contenidos ⁽ⁱ⁾	
		3	0	3	Switch de capa 2 ^(e)	
	VPN y Acceso Remoto	1	0	1	Switch de capa 2 ^(e)	
		1	0	1	Firewall ^(g)	
		1	0	1	Router con protección firewall ^(d)	
	WAN	3	3	0	Router	

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

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

a) 4 switches; para el módulo Central + Distribución de Edificios (2) y el Perímetro de Distribución (2)

- Nivel de conmutación : 3
- Tipo appliance
- Velocidad de conmutación (Throughput): 9 Mpps
- Capacidad de conmutación (Backplane): 12 Gbps
- MAC soportadas: 16000
- ACLs de L2/L3/L4
- VLANs (Protocolo 802.1Q)
- Manejo de enlaces Trunking (Protocolo 802.3AD)
- Monitoreo: SNMP v1/v2/v3, MIB-II, RMON (4 grupos: Alarmas, Eventos, Estadísticas, e Historia), Interfaz WEB, Telnet
- Spanning Tree (Protocolo 802.1D)
- Network Login (Protocolo 802.1X)
- QoS (802.1P)
- Número de Colas por puerto: 8
- Tráfico Multicast
- Soporte de stacking y uplink
- Soporte de protocolos de enrutamiento RIP v1/v2, OSPF
- MTBF mínimo 200000 horas
- Número de puertos habilitados:
 - 8 puertos 10/100/1000 Base-T
 - 1 puerto de consola

b) 3 switches para el módulo de Edificios (Usuarios)

- Nivel de conmutación : 2
- Tipo appliance
- Velocidad de conmutación (Throughput): 13 Mpps
- Capacidad de conmutación (Backplane): 17 Gbps
- MAC soportadas: 8000
- ACLs de L2
- VLANs (Protocolo 802.1Q)

- Manejo de enlaces Trunking (Protocolo 802.3AD)
 - Monitoreo: SNMP v1/v2/v3, MIB-II, RMON (4 grupos: Alarmas, Eventos, Estadísticas, e Historia), Interfaz WEB
 - Spanning Tree (Protocolo 802.1D)
 - Network Login (Protocolo 802.1X)
 - QoS (802.1P)
 - Número de Colas por puerto: 4
 - Tráfico Multicast
 - Soporte de stacking y uplink
 - MTBF mínimo 200000 horas
 - Número de puertos habilitados:
 - 48 puertos 10/100 Base-TX
 - 2 puertos 10/100/1000 Base-T
- c) 3 switches con módulo IDS; para el módulo de Servidores (2), y Comercio Electrónico (1)
- Nivel de conmutación : 3,
 - Incorporado módulo IDS
 - Tipo appliance
 - Velocidad de conmutación (Throughput): 9 Mpps
 - Capacidad de conmutación (Backplane): 12 Gbps
 - MAC soportadas: 16000
 - ACLs de L2/L3/L4
 - VLANs (Protocolo 802.1Q)
 - Manejo de enlaces Trunking (Protocolo 802.3AD)
 - Monitoreo: SNMP v1/v2/v3, MIB-II, RMON (4 grupos: Alarmas, Eventos, Estadísticas, e Historia), Interfaz WEB, Telnet
 - Spanning Tree (Protocolo 802.1D)
 - Network Login (Protocolo 802.1X)
 - QoS (802.1P)
 - Número de Colas por puerto: 8
 - Tráfico Multicast

- Soporte de stacking y uplink
 - Soporte de protocolos de enrutamiento RIP v1/v2, OSPF
 - MTBF mínimo 200000 horas
 - Número de puertos habilitados:
 - 8 puertos 10/100/1000 Base-T
 - 1 puerto de consola
- d) 2 routers con protección firewall; para el módulo de Administración (1) y VPN- Acceso Remoto (1)**
- Tipo appliance
 - Memoria RAM 128 MB
 - Memoria Flash 32 MB
 - Protocolo de transporte: IPSec
 - Protocolo de interconexión: Ethernet, Fast Ethernet
 - Monitoreo: SNMP, HTTP
 - Número de puertos habilitados:
 - 2 puertos LAN 10/100 Mbps
 - 1 puerto de consola
 - 1 puerto auxiliar
- e) 7 switches; para el módulo de Administración (1), Comercio Electrónico e Internet (2), Internet (3) y VPN-Acceso Remoto (1)**
- Nivel de conmutación : 2
 - Tipo appliance
 - Velocidad de conmutación (Throughput): 6 Mpps
 - Capacidad de conmutación (Backplane): 8 Gbps
 - MAC soportadas: 8000
 - ACLs de L2
 - VLANs (Protocolo 802.1Q)
 - Manejo de enlaces Trunking (Protocolo 802.3AD)
 - Monitoreo: SNMP v1/v2/v3, MIB-II, RMON (4 grupos: Alarmas, Eventos, Estadísticas, e Historia), Interfaz WEB

- Spanning Tree (Protocolo 802.1D)
 - Network Login (Protocolo 802.1X)
 - QoS (802.1P)
 - Número de Colas por puerto: 2
 - Tráfico Multicast
 - Soporte de stacking y uplink
 - MTBF mínimo 200000 horas
 - Número de puertos habilitados:
 - 8 puertos 10/100 Base-TX
 - 2 puerto 10/100/1000 Base-T
- f) 1 balanceador de carga; para el módulo de Comercio Electrónico
- Tipo appliance
 - Balanceo de carga en capa 4
 - Persistencia de sesiones capa 4
 - Distribución de tráfico según: ronda diaria (round robin), servidor ponderado (server weighting) y menos conexiones (least connections).
 - Programación de horarios
 - Soporte para Route-Path & Bridge-Path
 - Modo de retorno directo al servidor (Direct Server Return)
 - Alta disponibilidad
 - Modo de mantenimiento de servidores
 - Soporte Multiprotocolo
 - Monitoreo: SNMP v1/v2/v3, Interfaz WEB
 - Monitoreo de rendimiento
 - Estadísticas de tráfico
 - Número de puertos habilitados:
 - 2 puertos LAN 10/100 Mbps

g) 3 firewalls; para los módulos de: VPN y Accesos Remoto (1), Internet (1), y Comercio Electrónico (1).

- Tipo appliance
- Capacidad de procesamiento en Firewall de al menos 80 Mbps y de al menos 25 Mbps en tráfico VPN
- Memoria 128 MB
- 12000 Sesiones concurrentes
- 2000 sesiones nuevas por segundo
- Filtrado de paquetes a nivel de capa 3
- QoS en IPv4 a nivel de capa 3
- Inspección de paquetes a nivel Stateful
- Detección y rechazo de al menos los siguientes tipos de ataques: suplantación IP, inundación SYN, ping de la muerte, ataques de negación de servicio, paquetes malformados, fragmentos IP.
- Capacidad de poder hacer filtraje dentro de puertos TCP conocidos (por ejemplo el puerto 80 de http), aplicaciones potencialmente peligrosas como P2P (KaZaA, Gnutella) o Messengers (Yahoo!, MSN), aun y cuando se haga “tunneling” de estos simulando ser tráfico legítimo del puerto (ejemplo: tráfico legítimo HTTP).
- Rechazar código ActiveX o Java
- Soporte de VLANs (802.1Q)
- Ruteo básico IPv4
- NAT/PAT dinámico y estático
- Monitoreo: SNMP v1/v2/v3, MIB-II, Interfaz WEB
- Generación de alarmas por medio de snmp, syslog, consola
- Análisis de logs del sistema en tiempo real
- Número de puertos habilitados:
 - 4 puertos LAN 10/100 Mbps

h) 1 router; para el módulo de Internet

- Tipo appliance
- Memoria RAM 32 MB

- Memoria Flash 8 MB
 - Protocolo de interconexión: Ethernet, Fast Ethernet
 - Monitoreo: SNMP, HTTP
 - Soporte de VPN, Multiprotocolos
 - Número de puertos habilitados:
 - 2 puertos LAN 10/100 Mbps
 - 1 puerto WAN (Serie)
 - 1 puerto de consola
 - 1 puerto auxiliar
- i) 1 inspector de contenidos; para el módulo de Comercio Electrónico e Internet.
- Tipo appliance
 - Capacidad de procesamiento mínimo en configuración paralela: 40 Mbps
 - Capacidad de almacenamiento: 80 GB
 - Memoria RAM: 2 GB
 - Soporte de stacking
 - Número de puertos habilitados:
 - 2 Interfaces 10/100/1000 Base-T
 - 1 puerto de consola
 - Operación en tiempo real
 - Capacidad de integración con el Firewall Check Point VPN-1 UTM Edge
 - Actualización automática, en línea de las bases de datos (URLs, firmas de ataques, virus, spam, etc.)
 - Envío de alarmas por medio de SNMP, syslog y consola
 - Administración gráfica, remota y segura, desde la consola y el equipo de administración del sistema.
 - Anti-virus, Anti-phishing, Anti-spyware
 - Revisión y filtrado de contenido SMTP, POP3, FTP, HTTP/HTML, applets java, controles ActiveX, archivos comprimidos, scripts, mailtos, spam; con al menos las siguientes capacidades:
 - Bloqueo y protección contra spyware, malware, virus, troyanos, gusanos, keylogging, phishing y fraudes.

- Revisión y filtrado de código Java, Javascript, ActiveX y VBScript para HTTP, SMTP y FTP con al menos las siguientes capacidades:
 - Extracción de tags de applets Java en páginas HTML
 - Extracción de applets Java de las respuestas servidor-cliente, aún si la respuesta es un archivo comprimido
 - Extracción de tags ActiveX de páginas HTML
 - Extracción de tags JavaScript de páginas HTML
 - Extracción de macros de archivos MS Office
- Control de acceso Web con al menos las siguientes capacidades:
 - Filtrado / bloqueo de URL's en base a comodines, archivos y bases de datos de URL's.
 - Capacidad de generar logs y reportes de accesos Web
- Soporte SMTP con al menos las siguientes capacidades:
 - Anti-spam, anti-spoof, anti-virus y anti-relay
 - El antispam debe analizar tanto el correo de entrada: desde el Internet a la empresa; como el correo de salida, desde la empresa al Internet.
 - Soporte para listas blancas y negras personalizadas por el administrador.
 - Bloqueo de mensajes mediante RBL (Real-Time black list)
 - Descartar mensajes de remitentes seleccionados
 - Filtrado por tamaño máximo de mensaje
 - Capacidad de aplicar reglas de anti-spam por redes o dominios
 - Soporte de al menos los siguientes MTAs: Lotus Notes, Exchange.
 - Análisis basado en palabras y extensiones de archivos adjuntos
 - Capacidad de reportar al usuario final los mails retenidos
 - Debe eliminar correos SPAM utilizando tecnologías de última generación como la heurística.
- Filtrado HTTP con al menos las siguientes capacidades:
 - En base a esquemas (HTTP, FTP, SMTP, etc.), métodos (GET, POST, PUT, etc.) y dominios (ej. "*.com").
 - En base a un archivo conteniendo una lista de direcciones IP

3.1.2.2 Equipos Activos - Diseño Básico

A continuación se detallan los equipos requeridos para la implementación del diseño básico, ver Tabla 3.3.

Tabla 3.3 Especificaciones de los Equipos Requeridos - Diseño Básico

Bloque	Módulo "SAFE" de Cisco	Cantidad	Equipos Existentes	Equipos Requeridos	Equipos	
Campus Empresarial	Central + Distribución de Edificios	1	0	1	Switch de capa 3 ^(a)	
	Edificios	2	0	2	Switch de capa 2 ^(b)	
	Servidores	1	1	0	Switch de capa 2	
	Perímetro de Distribución	1	0	1	Switch de capa 3 ^(a)	
	Administración		1	0	1	Router con protección firewall ^(c)
			1	1	0	Switch de capa 2
Perímetro Empresarial	Comercio Electrónico e Internet	1	1	0	Router	
		1	0	1	Inspector de Contenidos ^(d)	
		1	1	0	Firewall	
		2	1	1	Switch de capa 2 ^(e)	
	VPN y Acceso Remoto	1	1	0	Router	
	WAN	3	3	0	Router	

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008

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

a) 2 switches; para el módulo Central + Distribución de Edificios (1) y el Perímetro de Distribución (1)

- Nivel de conmutación : 3
- Hardware tipo appliance
- Velocidad de conmutación (Throughput): 9 Mpps
- Capacidad de conmutación (Backplane): 12 Gbps
- MAC soportadas: 16000
- ACLs de L2/L3/L4
- VLANs (Protocolo 802.1Q)
- Manejo de enlaces Trunking (Protocolo 802.3AD)

- Monitoreo: SNMP v1/v2/v3, MIB-II, RMON (4 grupos: Alarmas, Eventos, Estadísticas, e Historia), Interfaz WEB, Telnet
- Spanning Tree (Protocolo 802.1D)
- Network Login (Protocolo 802.1X)
- QoS (802.1P)
- Número de Colas por puerto: 8
- Tráfico Multicast
- Soporte de stacking y uplink
- Soporte de protocolos de enrutamiento RIP v1/v2, OSPF
- MTBF mínimo 200000 horas
- Número de puertos habilitados:
 - 8 puertos 10/100/1000 Base-T
 - 1 puerto de consola

b) 2 switches para el módulo de Edificios (Usuarios)

- Nivel de conmutación : 2
- Hardware tipo appliance
- Velocidad de conmutación (Throughput): 13 Mpps
- Capacidad de conmutación (Backplane): 17 Gbps
- MAC soportadas: 8000
- ACLs de L2
- VLANs (Protocolo 802.1Q)
- Manejo de enlaces Trunking (Protocolo 802.3AD)
- Monitoreo: SNMP v1/v2/v3, MIB-II, RMON (4 grupos: Alarmas, Eventos, Estadísticas, e Historia), Interfaz WEB
- Spanning Tree (Protocolo 802.1D)
- Network Login (Protocolo 802.1X)
- QoS (802.1P)
- Número de Colas por puerto: 4
- Tráfico Multicast
- Soporte de stacking y uplink

- MTBF mínimo 200000 horas
 - Número de puertos habilitados:
 - 48 puertos 10/100 Base-TX
 - 2 puertos 10/100/1000 Base-T
- c) 1 router con protección firewall; para el módulo de Administración**
- Hardware de tipo appliance
 - Memoria RAM 128 MB
 - Memoria Flash 32 MB
 - Protocolo de transporte: IPSec
 - Protocolo de interconexión: Ethernet, Fast Ethernet
 - Monitoreo: SNMP, HTTP
 - Número de puertos habilitados:
 - 2 puertos LAN 10/100 Mbps
 - 1 puerto de consola
 - 1 puerto auxiliar
- d) 1 Inspector de contenidos; para el módulo de Comercio Electrónico e Internet.**
- Hardware de tipo appliance
 - Capacidad de procesamiento mínimo en configuración paralela: 40 Mbps
 - Capacidad de almacenamiento: 80 GB
 - Memoria RAM: 2 GB
 - Soporte de stacking
 - Número de puertos habilitados:
 - 2 Interfaces 10/100/1000 Base-T
 - 1 puerto de consola
 - Operación en tiempo real
 - Capacidad de integración con el Firewall Check Point VPN-1 UTM Edge
 - Actualización automática, en línea de las bases de datos (URLs, firmas de ataques, virus, spam, etc.)
 - Envío de alarmas por medio de SNMP, syslog y consola

- Administración gráfica, remota y segura, desde la consola y el equipo de administración del sistema.
- Anti-virus, Anti-phishing, Anti-spyware
- Revisión y filtrado de contenido SMTP, POP3, FTP, HTTP/HTML, applets java, controles ActiveX, archivos comprimidos, scripts, mailtos, spam; con al menos las siguientes capacidades:
 - Bloqueo y protección contra spyware, malware, virus, troyanos, gusanos, keylogging, phishing y fraudes.
 - Revisión y filtrado de código Java, Javascript, ActiveX y VBScript para HTTP, SMTP y FTP con al menos las siguientes capacidades:
 - Extracción de tags de applets Java en páginas HTML
 - Extracción de applets Java de las respuestas servidor-cliente, aún si la respuesta es un archivo comprimido
 - Extracción de tags ActiveX de páginas HTML
 - Extracción de tags JavaScript de páginas HTML
 - Extracción de macros de archivos MS Office
 - Control de acceso Web con al menos las siguientes capacidades:
 - Filtrado / bloqueo de URL's en base a comodines, archivos y bases de datos de URL's.
 - Capacidad de generar logs y reportes de accesos Web
 - Soporte SMTP con al menos las siguientes capacidades:
 - Anti-spam, anti-spoof, anti-virus y anti-relay
 - El antispam debe analizar tanto el correo de entrada: desde el Internet a la empresa; como el correo de salida, desde la empresa al Internet.
 - Soporte para listas blancas y negras personalizadas por el administrador.
 - Bloqueo de mensajes mediante RBL (Real-Time black list)
 - Descartar mensajes de remitentes seleccionados
 - Filtrado por tamaño máximo de mensaje
 - Capacidad de aplicar reglas de anti-spam por redes o dominios
 - Soporte de al menos los siguientes MTAs: Lotus Notes, Exchange.
 - Análisis basado en palabras y extensiones de archivos adjuntos

- Capacidad de reportar al usuario final los mails retenidos
 - Debe eliminar correos SPAM utilizando tecnologías de última generación como la heurística.
 - Filtrado HTTP con al menos las siguientes capacidades:
 - En base a esquemas (HTTP, FTP, SMTP, etc.), métodos (GET, POST, PUT, etc.) y dominios (ej. "*.com").
 - En base a un archivo conteniendo una lista de direcciones IP
- e) 1 switch para el módulo de Comercio Electrónico e Internet**
- Nivel de conmutación : 2
 - Hardware tipo appliance
 - Velocidad de conmutación (Throughput): 6 Mpps
 - Capacidad de conmutación (Backplane): 8 Gbps
 - MAC soportadas: 8000
 - ACLs de L2
 - VLANs (Protocolo 802.1Q)
 - Manejo de enlaces Trunking (Protocolo 802.3AD)
 - Monitoreo: SNMP v1/v2/v3, MIB-II, RMON (4 grupos: Alarmas, Eventos, Estadísticas, e Historia), Interfaz WEB
 - Spanning Tree (Protocolo 802.1D)
 - Network Login (Protocolo 802.1X)
 - QoS (802.1P)
 - Número de Colas por puerto: 2
 - Tráfico Multicast
 - Soporte de stacking y uplink
 - MTBF mínimo 200000 horas
 - Número de puertos habilitados:
 - 8 puertos 10/100 Base-TX
 - 2 puerto 10/100/1000 Base-T

3.1.3 DEL SOFTWARE

Con el objetivo de detectar y monitorear eventos ocurridos en la red que comprometan la seguridad del sistema, se debe identificar patrones previamente definidos que impliquen cualquier actividad sospechosa sobre la red y aportar con la capacidad de prevención y alerta anticipada, el diseño completo y el diseño básico contemplan el uso de NIDS, ver Tabla 3.4 y 3.5.

Tabla 3.4 Software Requerido - Diseño Completo

Bloque	Módulo "SAFE" de Cisco	Cantidad	Equipos Existentes	Equipos Requeridos	Equipos
Campus Empresarial	Administración	1	0	1	NIDS
Perímetro Empresarial	Comercio Electrónico	3	0	3	NIDS
	Internet	3	0	3	NIDS
	VPN y Acceso Remoto	1	0	1	NIDS

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008

Tabla 3.5 Software Requerido - Diseño Básico

Bloque	Módulo "SAFE" de Cisco	Cantidad	Equipos Existentes	Equipos Requeridos	Equipos
Campus Empresarial	Administración	1	0	1	NIDS
Perímetro Empresarial	Comercio Electrónico e Internet	2	0	2	NIDS

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

Las características mínimas requeridas para la implementación del software en el diseño completo y básico son:

a) NIDS (Sistema de detección de intrusiones basado en red)

- Disponible bajo licencia GPL (GNU Public License)
- Soporte para arquitectura DIDS (Distributed IDS)
- Multiplataforma
- Interfaz de línea de comando (consola)
- Administración gráfica, remota y segura, desde el equipo de administración del IDS.
- Detección de ataques en capa 2 a capa 7 del modelo OSI

- Detección de tráfico Anómalo: Anomalías en protocolos y aplicaciones
- Identificación y análisis de protocolos (TCP/IP, UDP, ICMP, SMTP, HTTP, DNS, RPC, NETBIOS, NNTP, GRE)
- Implementación de políticas en tiempo real
- Administración de reglas
- Registro de paquetes en archivos logs para su posterior análisis
- Detección de al menos los siguientes tipos de ataques: suplantación IP, inundación SYN, ping de la muerte, rastreo de puertos, ataque de negación de servicio, backdoor, finger, paquetes malformados, barrido de puertos, fragmentación IP, malware.
- Generación de alertas por medio de syslog, eventlog y consola
- Generación de reportes
- Capacidad de interactuar con bases de datos "Open Source"
- Actualización de firmas del IDS en línea

3.1.4 GENERALES

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

- Las versiones del sistema operativo de todos los equipos deben ser las últimas versiones liberadas por el fabricante a la fecha de compra.
- La solución de seguridad debe cumplir con las características mínimas descritas anteriormente y se debe garantizar compatibilidad, integración y operación entre los equipos ofertados con los equipos de comunicación de la empresa: switch 3Com 2024, switch HP 2524, router Cisco 805, router Cisco 1601R, Firewall Check Point VPN-1 UTM Edge.
- Todos los equipos deben ser capaces del envío de registros de eventos y alarmas al equipo de Administración de Sistema.
- Se debe considerar en la propuesta las actualizaciones para: seguridad (parches), IOS, firmas de virus, firmas de intrusiones y ataques, y demás firmas necesarias para el normal funcionamiento de los equipos por al menos un año.
- Incluir los cables de conectividad, administración, manuales y CD's.

3.2 PRESUPUESTO REFERENCIAL

3.2.1 DETALLE DE LAS EMPRESAS

En base a los requerimientos presentados para la implementación del esquema de seguridad, se solicitó proformas con costos referenciales a empresas especializadas en equipos e infraestructura para la seguridad física y de venta de equipos de Networking.

Para el software, se recurrió a instituciones y organizaciones que se dedican a la difusión, capacitación y promoción de herramientas "Open Source".

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

- Equipos e Infraestructura para la seguridad física
 - Arq. Patricio Mogrovejo
 - Contrafuego Internacional
 - Grand Dealer Comunicaciones
 - Rolitar CIA. LTDA.
 - Marketing & Tecnology S.A
 - IMETEL Ingeniería Eléctrica y Mecánica suministros y servicio
 - <http://www.gopower.com>
- Equipos de Networking
 - System Board T.A.
 - Pc Electrosoft
 - <http://www.3com.com>
 - <http://www.cisco.com/global/EC/index.shtml>
 - <http://www.dlinkla.com/home/index.jsp>
- Software
 - <http://www.ecualug.org>
 - <http://www.machangarasoft.com/>

3.2.2 DETALLE DEL COSTO PROMEDIO REFERENCIAL

A continuación se detalla el costo referencial para la implementación de la seguridad física, el diseño completo y el diseño básico.

3.2.2.1 Detalle del Costo - Seguridad Física

En las Tablas 3.6 y 3.7 se detalla el costo referencial de la seguridad física para la red de transmisión de datos de la empresa, que incluirá costo de equipamiento, instalación y configuración de equipos. El detalle completo de las proformas se encuentra en el Anexo 16.

Tabla 3.6 Costo de los Equipos - Seguridad Física

Cant.	Equipos	Total
1	UPS	\$ 3.800,00
1	Planta eléctrica	\$ 18.938,00
Total sin IVA		\$ 22.738,00

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008

Tabla 3.7 Costo de la Infraestructura - Seguridad Física

Detalle	Total
Remodelación de Cuarto de Telecomunicaciones	\$ 1.071,43
2 Puertas Eléctricas	\$ 660,71
Cableado Estructurado	\$ 8.063,97
Sistema contra Incendio	\$ 16.800,00
Total sin IVA	\$ 26.596,12

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008

El costo total referencial para la implementación de la seguridad física, se indica en la Tabla 3.8, valores no incluye IVA.

Tabla 3.8 Costo Total Referencial de la Implementación del Esquema de Seguridad Física

Costo Total Seguridad Física	Costo de Equipos	Costo de Infraestructura
\$ 49.334,12	\$ 22.738,00	\$26.596,12

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

3.2.2.2 Detalle del Costo - Diseño Completo

En la Tabla 3.9; se detalla el costo promedio referencial de los equipos de Networking para la implementación del diseño completo, incluyendo el costo por soporte técnico, mantenimiento y reposición. El detalle completo de las proformas se encuentra en el Anexo 16.

Tabla 3.9 Costo de los Equipos de Networking - Diseño Completo

Módulo "SAFE" de Cisco	Cant.	Equipos	Descripción del Equipo	Costo Unitario	Costo Total
Edificios	2	Switch de capa 2	3Com 4500 50-Puerto	\$ 848,00	\$ 1.696,00
Servidores	2	Switch de capa 3 + IDS	3Com 5500G-EI 24-Puertos	\$ 3.248,00	\$ 6.496,00
Comercio Electrónico	4	Switch de capa 2	3Com 4210 26-Puerto	\$ 379,00	\$ 1.516,00
	1	Switch de capa 3 + IDS	3Com 5500G-EI 24-Puertos	\$ 3.248,00	\$ 3.248,00
	1	Firewall	D-Link DFL-210	\$ 421,80	\$ 421,80
	1	Balanceador de Carga	Barracuda BBF240A	\$ 1424,05	\$ 1424,05
Internet	1	Inspector de Contenidos	3Com X506 Security Platform	\$ 3.444,00	\$ 3.444,00
	1	Firewall	D-Link DFL-210	\$ 421,80	\$ 421,80
	2	Switch de capa 2	3Com 4210 26-Puerto	\$ 379,00	\$ 758,00
	1	Router		\$ 593,75	\$ 593,75
VPN y Acceso Remoto	1	Switch de capa 2	3Com 4210 26-Puerto	\$ 379,00	\$ 379,00
	1	Firewall	D-Link DFL-210	\$ 421,80	\$ 421,80
	1	Router con protección firewall	Cisco 2801 Security Bundle, Adv Security, 64/256D	\$ 2.305,00	\$ 2.305,00
Central + Distribución de Edificios	2	Switch de capa 3	3Com 5500G-EI 24-Puertos	\$ 3.248,00	\$ 6.496,00
Perímetro de Distribución	2	Switch de capa 3	3Com 5500G-EI 24-Puertos	\$ 3.248,00	\$ 6.496,00
Administración	1	Router con protección firewall	Cisco 2801 Security Bundle, Adv Security, 64/256D	\$ 2.305,00	\$ 2.305,00
	1	Switch de capa 2	3Com 4210 26-Puerto	\$ 379,00	\$ 379,00
Total sin IVA					\$ 38.207,45

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

En la Tabla 3.10; se detallan el costo de los accesorios requeridos para la implementación del diseño completo.

Tabla 3.10 Costo de los Accesorios para los Equipos de Networking - Diseño Completo

Cantidad	Descripción del Accesorio	Costo Total
4	Switch 3Com 5500G-EI Stacking Cable (65cm) <i>Cable de Stacking para interconectar los equipos 3Com 5500G-EI</i>	\$2.499,00
1	3Com X500 DVGold Subscription <i>Un año de actualizaciones digitales de vacunas IPS y filtrado de contenido Web, soporte técnico vía telefónica, actualizaciones de software y reemplazo de hardware.</i>	\$1.738,00
1	3Com X506 1 Year Anti-Spam Service <i>Un año de actualizaciones Anti -Spam</i>	\$512,00
Total sin IVA		\$ 4.749,00

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

3.2.2.3 Detalle del Costo - Diseño Básico

En la Tabla 3.11; se detallan los costos promedios referenciales de los equipos de Networking para la implementación del diseño básico, incluyendo el costo por soporte técnico, mantenimiento y reposición. El detalle completo de las proformas se encuentra en el Anexo 16.

Tabla 3.11 Costo de los Equipos de Networking – Diseño Básico

Módulo "SAFE" de Cisco	Cant.	Equipos	Descripción del Equipo	Costo Unitario	Costo Total
Edificios	2	Switch de capa 2	3Com 4500 50-Puertos	\$848.00	\$1.696,00
Comercio Electrónico + Internet	1	Switch de capa 2	3Com 4210 26-Puertos	\$379.00	\$379,00
	1	Inspector de Contenidos	3Com X506 Security Platform	\$3444.00	\$3.444,00
Central	1	Switch de capa 3	3Com 5500G-EI 24-Puertos	\$3248.00	\$3.248,00
Perímetro de Distribución	1	Switch de capa 3	3Com 5500G-EI 24-Puertos	\$3248.00	\$3.248,00
Administración	1	Router con protección firewall	Cisco 2801 Security Bundle, Adv Security, 64F/256D	\$2305.00	\$2.305,00
Total sin IVA					\$14.320,00

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

En la Tabla 3.8; se detallan el costo de los accesorios requeridos, para un mejor desempeño de la red del diseño básico.

Tabla 3.12 Costo de los Accesorios para los Equipos de Networking – Diseño Básico

Cantidad	Descripción del Accesorio	Costo Total
1	Switch 3Com 5500G-EI Stacking Cable (65cm) <i>Cable de Stacking para interconectar los equipos 3Com 5500G-EI</i>	\$357,00
1	3Com X500 DVGold Subscription <i>Un año de actualizaciones digitales de vacunas IPS y filtrado de contenido Web, soporte técnico vía telefónica, actualizaciones de software y reemplazo de hardware.</i>	\$1738,00
1	3Com X506 1 Year Anti-Spam Service <i>Un año de actualizaciones Anti -Spam</i>	\$512,00
Total sin IVA		\$2.607,00

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

El costo referencial para la implementación de los NIDS en el diseño completo y en el diseño básico es nulo, ya que se va a utilizar una herramienta de libre distribución (Open Source), que no exige licenciamiento.

Sin embargo la información para la instalación, configuración y mantenimiento de esta herramienta esta disponible en el Internet. Para mayor información se puede visitar la página oficial de Snort: <http://www.snort.org>.

3.2.3 PROPUESTA PARA LA IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD

3.2.3.1 Propuesta - Diseño Completo

El costo total referencial para la implementación del esquema de seguridad del diseño completo, no incluye IVA, se indica en la Tabla 3.13:

Tabla 3.13 Costo Total Referencial de la Implementación del Esquema de Seguridad – Diseño Completo

Costo Total Referencial	Costo para implementación de la Seguridad Física	Costo de los equipos de Networking	Costo de los accesorios para los Equipos de Networking
\$ 92.290,57	\$ 49.334,12	\$ 38.207,45	\$4.749,00

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

El costo total referencial de la implementación del diseño completo tiene un valor de **\$92.290,57 (NOVENTA Y DOS MIL DOSCIENTOS NOVENTA CON CINCUENTA Y SIETE DÓLARES AMERICANOS) más el IVA**, que incluye el costo de la compra de los equipos e infraestructura para la seguridad física y de los equipos de Networking con sus respectivos accesorios para el diseño basado en “SAFE” de Cisco.

3.2.3.2 Propuesta - Diseño Básico

Mientras que el costo total referencial para la implementación del esquema de seguridad del diseño básica, no incluye IVA, se indica en la Tabla 3.11:

Tabla 3.14 Costo Total Referencial de la Implementación del Esquema de Seguridad – Diseño Básico

Costo Total Referencial	Costo para implementación de la Seguridad Física	Costo de los equipos de Networking	Costo de los accesorios para los Equipos de Networking
\$ 68.292,36	\$ 49.334,12	\$16.038,40	\$2.919,84

Fuente: MAIGUA, Sandra; OLALLA, Víctor. 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. Quito. 2008.

El costo total referencial de la implementación del diseño básico tiene un valor de **\$68.292,36 (SESENTA Y OCHO MIL DOSCIENTOS NOVENTA Y DOS CON TREINTA Y SEIS DOLARES AMERICANOS) más el IVA**, que incluye el costo de la compra de los equipos e infraestructura para la seguridad física y de los equipos de Networking con sus respectivos accesorios para el diseño basado en “SAFE” de Cisco.

Todos los equipos tienen una garantía por dos años para Forza Technologies (UPS), un año para equipos 3Com, Marathon (Motogenerador) y de 90 días para equipos Cisco, que ofrecen las empresas comercializadoras.

CAPITULO 4.

CONCLUSIONES Y RECOMENDACIONES

Una vez finalizado el análisis, el diseño y la propuesta técnica económica del esquema de seguridad, realizado en el presente proyecto de titulación se concluye y se recomienda lo siguiente:

4.1 CONCLUSIONES

- El análisis de las vulnerabilidades y amenazas llevado a cabo para la red de transmisión de datos, nos permite determinar los problemas de seguridad que mantiene la red. Mediante la implementación de un esquema de seguridad, dichos problemas serán minimizados tanto en la red interna como en la red externa de la empresa.
- El análisis de las vulnerabilidades y amenazas se basa en un “Test de Intrusión”, por tanto únicamente se va a conocer las falencias en la seguridad de la red hasta ese momento. Sin embargo la fortaleza de este tipo de análisis radica en que se puede efectuar de manera periódica, lo que permite cuantificar los resultados obtenidos, aplicar los correctivos necesarios y constatar los resultados alcanzados.
- La metodología modular planteada por el modelo de seguridad “SAFE” de Cisco, permite diseñar un esquema de seguridad de manera ágil y flexible, que se ajuste a las necesidades reales de la empresa.

- El presente proyecto propone dos diseños de seguridad: el diseño completo y el diseño básico, ambos garantizan la seguridad, confiabilidad y disponibilidad de la red de transmisión de datos. La principal diferencia entre ambos diseños es el costo de implementación, permitiendo al Gerente de Sistemas decidir la cantidad de dinero a invertir en la seguridad.
- Inicialmente en la empresa se propone implementar el diseño básico de seguridad, pero dependiendo de las necesidades y del presupuesto, este diseño puede evolucionar hacia el diseño completo propuesto en el presente proyecto.
- Adicionalmente a las ventajas que presenta la aplicación del esquema de seguridad, tenemos una mejora en los tiempos de respuesta, ya que las características de los equipo permiten la administración del tráfico que circula por la red.
- En la implementación del esquema de seguridad básico, se utilizarán equipos nuevos y equipos ya existentes; lo que se complementa con el uso de software libre para abaratar los costos de la implementación.
- A pesar de la existencia de políticas y normas de seguridad, la poca difusión de estas dentro de la empresa, impide concienciar a los usuarios sobre la importancia de su rol dentro del esquema de seguridad.
- El esquema de seguridad permite que la administración de la red sea ágil, segura y gestionable, debido a que se integra toda la red a través de módulos, mediante el uso de hardware y software apropiado.

4.2 RECOMENDACIONES

- Para la ejecución de la “Fase 4 - Intentos Activos de Intrusión” de la metodología “Penetration Testing Methodology”²² en los sistemas seleccionados, se recomienda al Departamento de Sistemas y Monitoreo tomar todas las medidas de contingencia y precauciones necesarias, para evitar interrupciones en los servicios que mantiene la empresa, tanto para usuarios internos como externos.
- Se recomienda al Gerente de Sistemas y Monitoreo contratar personal con un buen nivel de conocimiento 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 realizar tareas de aseguramiento de la red.
- Se recomienda planificar la ejecución periódica de un “Test de Intrusión” en la red de transmisión de datos, esto permitirá conocer la evolución de la seguridad conforme avanza el tiempo, y evaluar el resultado de los correctivos aplicados en los problemas con la seguridad de la información.
- La seguridad de la información es un requerimiento básico en una red de transmisión de datos, especialmente cuando se maneja información tan sensible como por ejemplo saber la ubicación exacta de un vehículo en tiempo real, por lo que se recomienda al Gerente de Sistemas realizar un balance entre la importancia de la información que manejan y el rubro asignado para mantenerla segura.
- Debido a que el usuario es el eslabón más frágil en la cadena de la seguridad, se recomienda la difusión y puesta en práctica de todas las Políticas y Normas presentadas en la sección 2.3.

²² <http://www.bsi.de/english/publications/studies/penetration.pdf>

- En base a la experiencia adquirida en esta tesis, se recomienda a los diseñadores y administradores de redes seguir el “Modelo de Seguridad para Redes Empresariales “SAFE” de Cisco, ya que utiliza una arquitectura modular, donde no es probable que el fallo de un sistema ponga en peligro a todos los equipos de la red.
- Se recomienda para el desarrollo de un esquema de seguridad en general, establecer un tiempo prudencial para describir de forma clara y completa la situación actual de la empresa, así también las vulnerabilidades y amenazas que presenta la red, para de este modo determinar un diseño y una propuesta técnica que se acople a los requerimientos físicos, técnicos y económicos de dicha empresa.

BIBLIOGRAFÍA

Tesis

- VINUEZA Rhor Mónica De Lourdes
“Estudio y diseño de un sistema de seguridad para la red de datos del Colegio Los Pinos”, 2003.
- NOLIVOS Cisneros Mónica Catalina
“Análisis y estudio comparativo de las políticas, estándares y tecnologías de seguridad en un intranet local”, 2000.
- CARRANZA Espinoza Hugo Ruperto, GUTIÉRREZ Dávila Luís Antonio
“Políticas y estrategias de seguridad para la intranet de PetroEcuador - Matriz”, 14 de Febrero del 2004.
- MORALES Checa Francisco Fernando
“Estudio y diseño de una red de datos de área local para el servicio social de la fuerza terrestre en la ciudad de Quito”, Diciembre 2003.
- PAUCAR Simbaña Luis Gustavo, PROAÑO Cargua Juan Carlos
“Diseño de un sistema de seguridad para la red de datos de la Escuela Politécnica Nacional”, Enero 2003.
- GUEVARA Flores Adriana del Pilar
“Diseño e implantación de un esquema de seguridad en los servidores de los laboratorios del D.I.C.C” Marzo 2005.

Libros

- SCAMBRA, Joel; SHEMA, Mike; SIMA, Caleb; Hacking Exposed Web Applications. Segunda Edición. McGraw-Hill/Osborne. 2006.
- SEAN, Convery; Network Security Architectures. Cisco Press. Abril 2004.
- SANTOS, Omar; End-to-End Network Security Defense-in-Depth. Primera Edición. Cisco Press. Agosto 2007.
- CLEMM, Alexander; Network Management Fundamentals. Cisco Press. Noviembre 2006.
- MENGA, Justin; TIMM, Carl; CCSP™: Secure Intrusion Detection and SAFE Implementation. SYBEX. 2004.

- SPIVEY, Mark; Practical Hacking techniques And Countermeasures. Taylor & Francis Group. 2007
- BURNS, Bryan; GRANICK, Jennifer; MANZUIK, Steve; Security Power Tools. O'Reilly. 2007.
- BAKER, Andrew; Esler, Joel; Snort® IDS and IPS Toolkit. Syngress Publishing. 2007.

Páginas Web

- Carlink – Sistemas de seguridad y control vehicular
<http://www.carlink.com.ec>; 2007
- A Penetration Testing Model
<http://www.bsi.de/english/publications/studies/penetration.pdf>; 2007
- SAFE: A Security Blueprint for Enterprise Networks
www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.pdf; 2007
- Cisco SAFE: Un modelo de seguridad para las redes de las empresas
www.cisco.com/web/LA/soluciones/comercial/SNF_Blueprint_Full_version_ESP.pdf; 2007
- Black Box Ecuador
<http://www.blackbox.ec/bbe/>; 2007
- Computer Incident Advisory Capability “CIAC”, U. S. Department
<http://www.ciac.org/ciac/index.html>
- Interconexión de redes
<http://www.ilustrados.com/publicaciones/EypEklkpEAJCTOmHJ.php>
Agosto 2003.
- TEMA 9: PROTOCOLOS TCP/IP
<http://www.infase.es/FORMACION/INTERNET/tcpip.html>; Abril 2007.
- Políticas de seguridad
<http://es.tldp.org/Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html>.
Agosto 2003.
- Seguridad Informática
http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica; Abril 2007

- Seguridad Informática
http://www.auditoriasistemas.com/seguridad_informatica.htm; 2004
- Seguridad Informática / Seguridad Lógica
<http://www.w3.org/1999/xhtml>; Diciembre 2005
- Consideraciones de Seguridad en el Diseño de Aplicaciones Web
<http://www.informatizate.net>; 2004.
- Política de comunicación electrónica
<http://estudiantes.sagrado.edu/usoelectronico200608.pdf>; Agosto 2006
- Seguridad en redes de computadoras
<http://www.monografias.com/trabajos30/seguridad-redes/seguridad-redes.shtml>; 1997.
- Seguridad Informática
<http://ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm>.
Noviembre 2002.
- RH Linux 4: Manual de seguridad, Capítulo 9. Detección de intrusos.
<http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-net.html>; 2005
- NAUTOPIA: Privacidad y Seguridad
http://nautopia.coolfreepages.com/snort_cap1.htm; 2002
- Políticas de Seguridad
<http://www.icetex.gov.co/portal/Default.aspx?tabid=271>; 2007
- Políticas y procedimientos en la seguridad de la información
<http://www.monografias.com/trabajos11/seguin/seguin.shtml>; 1997
- Políticas y Procedimientos en la Seguridad de la Información
http://www.segu-info.com.ar/terceros/vcappuccio_politicas-seguridad-informacion.htm; 2000
- Snort
<http://www.snort.org/>. 2007
- OSSTMM 2.1.
<http://isecom.securenetsltd.com/OSSTMM.es.2.1.pdf>

Herramientas de Escaneo

- Ping Probe
<http://www.ping-probe.com/Ping-Probe/Download/Index.htm>. 2007
- Retina® Network Security Scanner
<http://icm.tucows.com/files7/RetinaDemo5417.exe>; 2007
- TENABLE; Network Security
<http://www.nessus.org/nessus/>; 2007
- GFI LanGuard
<ftp://ftp.gfi.com/languardnss8.exe>
- BackTrack
<http://mirror.switch.ch/ftp/mirror/backtrack/bt2final.iso>
- Nmap
<http://download.insecure.org/nmap/dist/nmap-4.20-setup.exe>
- NSTalker
<http://www.nstalker.com/nstalker/updates/index.php>
- Saint
<http://download.saintcorporation.com/downloads/freetrial/saint-install-6.6.3.gz>

ANEXOS

ANEXO 1. Metodología para un Test de Intrusión

ANEXO 2. Herramientas de Escaneo y Vulnerabilidades

ANEXO 3. Nslookup al servidor de nombres

ANEXO 4. Contenido del sitio Web

ANEXO 5. Tipos de Escaneo - Descripción

ANEXO 6. Escaneo Sigiloso de Puertos

ANEXO 7. Identificación de Servicios y Aplicaciones

ANEXO 8. Identificación Remota de Sistemas Operativos

ANEXO 9. Identificación del Banner

ANEXO 10. Escaneo directo del Firewall

ANEXO 11. Escaneo de Vulnerabilidades

ANEXO 12. Escaneo de Vulnerabilidades – Interfaz Web

ANEXO 13. Calculo de la Potencia – UPS y Generador Eléctrico

ANEXO 14. Modelo “SAFE” de Cisco

ANEXO 15. Especificaciones Técnicas - Equipos Existentes

ANEXO 16. Proformas