

## TABLA DE CONTENIDOS

	página
<b>Dedicatoria</b>	<b>I</b>
<b>Agradecimientos</b>	<b>II</b>
<b>Tabla de Contenidos</b>	<b>III</b>
<b>Índice de Figuras</b>	<b>VII</b>
<b>Índice de Tablas</b>	<b>X</b>
<b>Resumen</b>	<b>XI</b>
<b>Abstract</b>	<b>XII</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Objetivos generales . . . . .	2
1.2. Objetivos específicos . . . . .	2
1.3. Alcances . . . . .	3
1.4. Limitaciones del proyecto . . . . .	3
1.5. Descripción del problema . . . . .	3
<b>2. Marco Teórico</b>	<b>5</b>
2.1. Seguridad . . . . .	5
2.1.1. Seguridad informática . . . . .	5
2.1.2. Seguridad de red . . . . .	6
2.2. Seguridad perimetral . . . . .	6
2.2.1. Amenazas . . . . .	6
2.2.2. Firewall . . . . .	7
2.2.3. Zona desmilitarizada (DMZ) . . . . .	12
2.2.4. Direcciones IP públicas y privadas . . . . .	15
2.2.5. Virtual Private Network o VPN . . . . .	20
2.3. Seguridad acceso Intranet . . . . .	28
2.3.1. Asignación estática . . . . .	28

2.3.2.	Asignación dinámica o DHCP . . . . .	28
2.4.	Servicios para el acceso público . . . . .	31
2.4.1.	Certificado Digital . . . . .	31
2.4.2.	Tecnologías usadas en el correo electrónico . . . . .	32
<b>3.</b>	<b>Metodología</b>	<b>34</b>
3.1.	Estudio de un modelo propuesto por Cisco . . . . .	34
3.2.	Análisis de una red con firewall PIX . . . . .	35
3.3.	Entrevistas al usuario . . . . .	35
3.3.1.	Requerimientos del proyecto . . . . .	36
3.3.2.	Secuencia de desarrollo del proyecto . . . . .	38
<b>4.</b>	<b>Diseño</b>	<b>39</b>
4.1.	Diseño perímetro de seguridad . . . . .	39
4.1.1.	Diseño general de reglas de filtrado . . . . .	43
4.1.2.	Diseño zona desmilitarizada . . . . .	44
4.2.	Diseño del Servidor Web . . . . .	45
4.2.1.	Esquema general del servidor Web . . . . .	47
4.3.	Diseño del servidor de correo electrónico . . . . .	47
4.3.1.	Zimbra . . . . .	49
4.3.2.	Arquitectura de Zimbra . . . . .	50
4.3.3.	Interfaz Web . . . . .	50
4.3.4.	Paquetes libres utilizados por Zimbra . . . . .	51
4.3.5.	DNS del servidor de correo . . . . .	51
4.3.6.	Seguridad del servidor de correo . . . . .	52
4.4.	Diseño del sistema de gestión y control de acceso para la red municipal	53
4.4.1.	Configuración Servidor DHCP . . . . .	53
4.4.2.	Aplicación desarrollada . . . . .	54
<b>5.</b>	<b>Implementación</b>	<b>69</b>
5.1.	Firewall Cisco ASA 5510 . . . . .	69
5.1.1.	Reseteo y creación de usuario administrador . . . . .	69
5.1.2.	Actualización del firewall . . . . .	70
5.1.3.	Configuración inicial e interfaces . . . . .	70
5.1.4.	Configuración SSH y ASDM . . . . .	71

5.1.5.	Configuración para la conexión a Internet . . . . .	72
5.1.6.	Configuración reglas de filtrado . . . . .	73
5.1.7.	Configuración NAT y PAT . . . . .	78
5.1.8.	Acotaciones para las PAT, NAT y reglas de filtrado . . . . .	79
5.1.9.	Configuración VPN . . . . .	80
5.2.	Servidor Web . . . . .	83
5.2.1.	Configuración de certificación . . . . .	83
5.2.2.	Configuración de Apache . . . . .	87
5.3.	Servidor de correo electrónico . . . . .	87
5.3.1.	Instalación y configuración servidor Zimbra . . . . .	88
5.3.2.	Interfaz Web Zimbra . . . . .	91
5.3.3.	Comandos para administración . . . . .	95
5.3.4.	Actualización del antivirus . . . . .	95
5.4.	Sistema de gestión y control de acceso para la red municipal . . . . .	96
5.4.1.	Instalación servidor DHCP . . . . .	96
5.4.2.	Instalación de la aplicación Web para el servidor DHCP . . . . .	98
<b>6.</b>	<b>Pruebas funcionales y resultados</b>	<b>100</b>
6.1.	Firewall Cisco ASA 5510 . . . . .	100
6.2.	Virtual Private Network . . . . .	115
6.2.1.	VPN mediante cliente . . . . .	115
6.2.2.	VPN mediante Web . . . . .	117
6.3.	Sistema de gestión y control de acceso para la red municipal . . . . .	119
6.4.	Servidor de correo electrónico . . . . .	124
<b>7.</b>	<b>Conclusiones y comentarios</b>	<b>127</b>
7.1.	Conclusiones y comentarios . . . . .	127
7.2.	Trabajo futuro . . . . .	128
<b>8.</b>	<b>Anexos</b>	<b>129</b>
8.1.	Archivo de configuración firewall Cisco PIX (DIDECO) . . . . .	129
8.2.	Paquetes libres utilizados por Zimbra . . . . .	131
8.3.	Archivo base servidor DHCP . . . . .	133
8.4.	Parametros servidor DHCP . . . . .	135
8.5.	Script servidor DHCP . . . . .	137

8.6.	Archivo de configuración firewall Cisco ASA 5510 . . . . .	138
8.7.	Configuración firewall Cisco ASA 5510 . . . . .	145
8.7.1.	Actualización del firewall . . . . .	145
8.7.2.	Configuración de interfaces . . . . .	147
8.7.3.	Configuración SSH y ASDM . . . . .	148
8.7.4.	Creación de grupos y enlaces simbólicos . . . . .	149
8.7.5.	Sintaxis de access-list y access-group. . . . .	150
8.7.6.	Configuración reglas de filtrado . . . . .	151
8.7.7.	Configuración NAT y PAT . . . . .	158
8.7.8.	Configuración VPN . . . . .	159
8.8.	Configuración previa e instalación de los paquetes necesarios para la implementación del servidor Web . . . . .	165
8.8.1.	Configuración interfaz de red y repositorios . . . . .	165
8.8.2.	Instalación Apache2, PHP5 y OpenSSL . . . . .	166
8.9.	Configuración Apache . . . . .	167
8.10.	Configuración previa del servidor de correo electrónico . . . . .	169
8.10.1.	Prerrequisitos para instalación de Zimbra . . . . .	169
8.10.2.	Instalación de paquetes servidor Zimbra . . . . .	170
8.11.	Comandos para administración de Zimbra . . . . .	171
8.12.	Configuración de la interfaz e instalación de lo paquetes asociados al del servidor DHCP . . . . .	171
8.13.	Archivo sudores . . . . .	172
8.14.	Análisis de costos . . . . .	173
8.15.	CD con documentación técnica del firewall Cisco ASA 5510 . . . . .	174

## ÍNDICE DE FIGURAS

	página
2.1. Firewall de Aplicación . . . . .	8
2.2. Firewall de filtrado de paquetes . . . . .	9
2.3. Arquitectura con acceso a Internet al exterior del firewall . . . . .	11
2.4. Arquitectura con firewall simple . . . . .	11
2.5. Arquitectura con firewall doble . . . . .	12
2.6. DMZ con router y firewall . . . . .	13
2.7. DMZ con firewall simple . . . . .	14
2.8. DMZ con firewall doble . . . . .	15
2.9. Encriptación DES . . . . .	24
2.10. Encriptación 3DES . . . . .	24
2.11. Fórmula de encriptación 3DES . . . . .	25
2.12. Esquema del funcionamiento del servicio DHCP . . . . .	31
4.1. Esquema red interna . . . . .	40
4.2. Vista frontal Cisco ASA 5510 . . . . .	41
4.3. Vista posterior Cisco ASA 5510 . . . . .	42
4.4. Esquema DMZ municipal . . . . .	45
4.5. Esquema servidor Web . . . . .	47
4.6. Esquema servidor DNS . . . . .	52
4.7. Esquema servidor DHCP . . . . .	53
4.8. Esquema base de datos . . . . .	56
4.9. Protocolo de comunicación de la aplicación socket. . . . .	63
4.10. Arquitectura global de la aplicación . . . . .	64
5.1. Configuración cliente Cisco VPN 1. . . . .	81
5.2. Configuración cliente Cisco VPN 2. . . . .	82
5.3. Menú Superior servidor Zimbra. . . . .	91
5.4. Menú lateral servidor Zimbra. . . . .	92
5.5. Menú principal servidor Zimbra. . . . .	93
5.6. Menú nuevo dominio de correo. . . . .	94
5.7. Menú nueva cuenta de correo. . . . .	94

6.1. Tráfico HTTP desde un funcionario municipal hacia el exterior . . . . .	103
6.2. Tráfico DNS desde la red interna hacia el exterior . . . . .	103
6.3. Tráfico HTTPS desde la red interna hacia el exterior . . . . .	104
6.4. MSN funcionario municipal . . . . .	104
6.5. MSN Dpto. de Informática . . . . .	105
6.6. Tráfico FTP desde un funcionario municipal hacia el exterior . . . . .	105
6.7. Tráfico FTP desde el Dpto. de Informática hacia el exterior . . . . .	106
6.8. Tráfico SQL-Server desde un funcionario municipal hacia el exterior .	106
6.9. Ping desde un funcionario municipal hacia el exterior . . . . .	107
6.10. Tráfico mediante el puerto 2095 (webMail) desde un funcionario municipal hacia el exterior . . . . .	107
6.11. Tráfico http desde Internet hacia el servidor Web . . . . .	108
6.12. Tráfico ssh desde Internet hacia el servidor Web . . . . .	108
6.13. Tráfico a través del puerto 1000 hacia el servidor Web . . . . .	109
6.14. Tráfico smtp desde Internet hacia el servidor Web . . . . .	109
6.15. Tráfico a través del puerto 4200 hacia el servidor Web . . . . .	110
6.16. Tráfico SSH desde Internet hacia el servidor postgre . . . . .	111
6.17. Tráfico a través del puerto 2456 hacia el servidor postgre . . . . .	111
6.18. Tráfico a través del puerto 5432 hacia el servidor postgre . . . . .	112
6.19. Tráfico a través del puerto 1000 hacia el servidor postgre . . . . .	112
6.20. Tráfico a través del puerto 1433 hacia el servidor SQL-Server . . . . .	113
6.21. Tráfico a través del puerto 3389 para escritorio remoto . . . . .	113
6.22. Tráfico a través del puerto 5432 hacia el servidor postgre desde la DMZ	114
6.23. Tráfico SMTP desde la DMZ hacia el exterior . . . . .	114
6.24. Ping desde la inside hacia la DMZ . . . . .	115
6.25. Cliente VPN Cisco. . . . .	116
6.26. Propiedades de la conexión mediante el cliente VPN Cisco. . . . .	116
6.27. Propiedades del adaptador de red virtual Cisco. . . . .	117
6.28. Inicio de sesión WebVPN. . . . .	117
6.29. Menú "Terminal Server". . . . .	118
6.30. Inicio de sesión de Windows. . . . .	118
6.31. Propiedades dispositivo de red. . . . .	119
6.32. Creación de un servidor DHCP mediante el sistema . . . . .	120
6.33. Creación de un equipo mediante el sistema . . . . .	120

6.34. Creación de un funcionario municipal mediante el sistema . . . . .	121
6.35. Creación de una NIC mediante el sistema . . . . .	122
6.36. Reiniciar servidor DHCP mediante el sistema . . . . .	123
6.37. Archivos de respaldos de la configuración del servidor DHCP. . . . .	123
6.38. Log temporales del servidor DHCP. . . . .	124
6.39. Reinicio servidor DHCP. . . . .	124
6.40. Interfaz cliente. . . . .	125
6.41. Interfaz Administrador. . . . .	125
6.42. Interfaz cliente. . . . .	126
6.43. Interfaz cliente. . . . .	126
8.1. Configuración TFTP . . . . .	146
8.2. Configuración Group Policies. . . . .	160
8.3. Configuración de Address Pools. . . . .	160
8.4. Configuración de VPN. . . . .	161
8.5. Configuración de interfaz para VPN. . . . .	162
8.6. Configuración de Internet key Exchange. . . . .	162
8.7. Configuración de NAT para VPN. . . . .	163
8.8. Configuración Group Policy para WebVPN. . . . .	164
8.9. Configuración Connection Profiles para WebVPN. . . . .	164
8.10. Configuración dirección WebVPN. . . . .	165
8.11. Configuración Interfaz WebVPN. . . . .	165

## ÍNDICE DE TABLAS

	página
2.1. Clases de Direcciones IP . . . . .	16
2.2. Direcciones disponibles para las LAN . . . . .	18
4.1. Tabla de led . . . . .	41
4.2. Tabla vista posterior Cisco ASA 5510 . . . . .	42
4.3. Características técnicas de los servidores de correo . . . . .	48
4.4. Características subjetivas del servidores de correo . . . . .	49
4.5. Tabla persona . . . . .	57
4.6. Tabla equipo . . . . .	57
4.7. Tabla nic . . . . .	57
4.8. Tabla usuario . . . . .	58
4.9. Tabla opciones . . . . .	58
5.1. Nombres simbólicos de direcciones IP . . . . .	74
5.2. Propósitos de Certificados X.509 . . . . .	86
6.1. Tabla de direcciones IP . . . . .	101
6.2. Tabla de reglas de filtrado . . . . .	102