

Índice de Contenidos

RESUMEN.....	6
CAPÍTULO I.....	7
1. INTRODUCCIÓN.....	7
1.1. INTRODUCCIÓN.....	7
1.2. PLANTEAMIENTO DEL PROBLEMA.....	8
1.3. JUSTIFICACIÓN.....	9
1.4. OBJETIVOS.....	11
1.4.1. Objetivo General.....	11
1.4.2. Objetivos Específicos.....	11
1.5. ALCANCE.....	12
CAPÍTULO II.....	13
2. MARCO TEÓRICO.....	13
2.1. INTRODUCCIÓN.....	13
2.2. REDES DE ÁREA LOCAL (LAN).....	13
2.2.1. Definición de una Red LAN.....	14
2.2.2. Elementos de una Red LAN.....	14
2.2.3. Protocolos de Área Local.....	15
2.2.3.1. Protocolos de Bajo Nivel.....	16
2.2.3.2. Protocolos de Red.....	16
2.2.4. Analizadores de protocolos LAN.....	16
2.3. SISTEMAS DE CABLEADO ESTRUCTURADO.....	17
2.4. REDES DE ÁREA EXTENDIDA (WAN).....	18
2.4.1. Definición de una Red WAN.....	18
2.4.2. Elementos de una Red WAN.....	19
2.4.2.1. Equipos de interconexión.....	19
2.4.2.2. Infraestructura de red.....	20
2.5. PROTOCOLOS DE ÁREA EXTENDIDA.....	20
2.5.1. Capa Física: WAN.....	21
2.5.2. Capa de Enlace de Datos: Protocolos WAN.....	22
2.5.2.1. Synchronous Data Link Control (SDLC).....	23
2.5.2.2. High Level Data Link Control (HDLC).....	23
2.5.2.3. Link Access Procedure Balanced (LAPB).....	23
2.5.2.4. X.25 y Frame Relay.....	24
2.5.2.5. Point to Point Protocol (PPP).....	24
2.6. TECNOLOGÍAS DE ÁREA EXTENDIDA.....	24
2.6.1. Integrated Services Digital Network (ISDN).....	25
2.6.2. Frame Relay.....	25
2.6.3. ATM.....	28
2.6.4. SONET / SDH.....	33
2.6.4.1. PDH.....	33
2.6.5. Jerarquía Digita Síncrona (SDH).....	35
2.7. CALIDAD DE SERVICIO – QoS.....	39
2.8. SEGURIDAD EN REDES.....	41
2.8.1. Introducción.....	41
2.8.2. Riesgos de Seguridad.....	42
2.8.2.1. Intrusión.....	42

2.8.2.2. Rechazo de Servicios.....	42
2.8.2.3. Robo de Información.....	42
2.8.3. Técnicas de ataque.....	43
2.8.3.1. Ingeniería Social.....	43
2.8.3.2. Bugs del Sistema.....	43
2.8.3.3. Back Door.....	43
2.8.3.4. Caballos de Troya.....	43
2.8.3.5. Señuelos.....	44
2.8.3.6. Método del Adivino.....	44
2.8.3.7. Revisión de Basura.....	44
2.8.4. Puntos para mejorar la seguridad.....	44
2.8.4.1. Identificación y Autenticación.....	44
2.8.4.2. Integridad.....	44
2.8.4.3. Confidencialidad.....	45
2.8.5. Estrategias de Seguridad.....	45
2.8.5.1. Mínimos privilegios.....	45
2.8.5.2. Check Point.....	45
2.8.6. Firewalls.....	45
2.8.7. Virus.....	46
2.8.7.1. Tipos de Virus.....	48
2.8.7.2. Sniffing.....	50
2.8.7.3. Spoofing.....	51
CAPÍTULO III.....	52
3. ANÁLISIS Y DISEÑO PROPUESTO PARA LA RED LAN – WAN.....	52
3.1. DESCRIPCIÓN DE LA SITUACIÓN ACTUAL DE LA RED DE DATOS.....	52
3.1.1. Descripción Física de la Red de Datos.....	54
3.1.1.1. Parte Pasiva.....	54
3.1.1.2. Parte Activa.....	55
3.1.2. Descripción Lógica de la Red de Datos.....	58
3.1.2.1. Administración de la Red de Datos.....	58
3.1.2.2. Licenciamiento.....	60
3.1.2.3. Aplicaciones.....	61
3.2. ANÁLISIS DE LAS REDES LAN – WAN.....	63
3.2.1. Resultados de la Medición de Tráfico LAN.....	64
3.2.2. Resultados de la Medición de Tráfico WAN.....	65
3.2.3. Proveedor Andinadatos.....	66
3.2.3.1. Resultados de la Medición de Tráfico.....	67
3.2.3.2. Tráfico de Entrada a la Red de Datos del Municipio.....	68
3.2.3.3. Tráfico de Salida de la Red de Datos del Municipio.....	72
3.2.3.4. Eficiencia del Segmento de Red Entrante.....	73
3.2.4. Proveedor PuntoNet.....	74
3.2.4.1. Resultados del Servicio de Internet.....	77
3.3. DISEÑO PROPUESTO PARA LA RED LAN – WAN.....	79
3.3.1. Módulo de Administración.....	82
3.3.2. Módulo de Building.....	83
3.3.3. Módulo de Building Distribution.....	84
3.3.4. Módulo Core.....	84
3.3.5. Módulo Edge.....	84
3.3.6. Módulo Server.....	85

3.3.7. Módulo Internet Corporativo.....	85
3.3.8. Módulo WAN.....	86
CAPÍTULO IV.....	87
4. SEGURIDAD INFORMÁTICA DE LA RED DE DATOS.....	87
4.1. INTRODUCCIÓN.....	87
4.2. SITUACIÓN ACTUAL.....	89
4.3. ANÁLISIS DE RIESGOS.....	90
4.3.1. Inventariar los Activos e Identificar las Amenazas.....	90
4.3.2. Vulnerabilidades.....	93
4.3.3. Estimar el Impacto de Amenazas se hagan efectivas.....	94
4.3.4. Diseño del Sistema de Seguridad Informático de la Red de Datos.....	95
4.3.5. Arquitectura de Red Segura.....	95
4.3.5.1. Módulo Administración.....	95
4.3.5.2. Módulo de Building.....	96
4.3.5.3. Módulo de Building Distribution.....	96
4.3.5.4. Módulo de Core.....	96
4.3.5.5. Módulo Edge.....	96
4.3.5.6. Módulo Server.....	96
4.3.5.7. Módulo Internet Corporativo.....	97
4.3.5.8. Módulo WAN.....	97
4.3.5.9. Clasificación de los Segmentos de Red.....	98
4.4. ARQUITECTURA DE FIREWALLS.....	100
4.5. ARQUITECTURA DEL SISTEMA DE ANTISPAM, ANTIVIRUS Y NAVEGACIÓN.....	102
4.6. ARQUITECTURA DE IDS/IPS.....	105
4.7. SISTEMA DE ADMINISTRACIÓN.....	106
CAPÍTULO V.....	107
5. CONCLUSIONES Y RECOMENDACIONES.....	107
5.1. CONCLUSIONES.....	107
5.2. RECOMENDACIONES.....	109
BIBLIOGRAFÍA.....	115
ANEXOS.....	117