



UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

ELECTRÓNICA E INDUSTRIAL

Carrera de Ingeniería en Electrónica y Comunicaciones

TEMA:

“RED DE VIDEO-VIGILANCIA MEDIANTE TECNOLOGÍA IP PARA EL ACCESO REMOTO DE LAS UNIDADES OPERATIVAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN.”

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniera en Electrónica y Comunicaciones.

AUTOR: Andrea Jessica Ramos Durán

TUTOR: Ing. M.Sc. Julio Enrique Cuji Rodríguez

Ambato - Ecuador

Diciembre 2012

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de investigación, nombrado por el Honorable Consejo Superior de Pregrado de la Universidad Técnica de Ambato:

CERTIFICO:

Que el trabajo de investigación: **“RED DE VIDEO-VIGILANCIA MEDIANTE TECNOLOGÍA IP PARA EL ACCESO REMOTO DE LAS UNIDADES OPERATIVAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN.”**, presentado por la Srta. Andrea Jessica Ramos Durán, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Diciembre de 2012

EL TUTOR

Ing. M.Sc. Julio Enrique Cuji Rodríguez

AUTORÍA

El presente trabajo de investigación titulado: **“RED DE VIDEO-VIGILANCIA MEDIANTE TECNOLOGÍA IP PARA EL ACCESO REMOTO DE LAS UNIDADES OPERATIVAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN.”**, es absolutamente original, auténtico y personal; en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Diciembre de 2012

Andrea Jessica Ramos Durán

C.I.: 1804160040

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes: Ing. M.Sc. Oswaldo Eduardo Paredes Ochoa, Ing. M.Sc. Geovanni Danilo Brito Moncayo e Ing. M.Sc. Edwin Rodrigo Morales Perrazo, revisó y aprobó el Informe Final del trabajo de graduación titulado **“RED DE VIDEO-VIGILANCIA MEDIANTE TECNOLOGÍA IP PARA EL ACCESO REMOTO DE LAS UNIDADES OPERATIVAS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN.”**, presentado por la Srta. Andrea Jessica Ramos Durán de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

Ing. M.Sc. Oswaldo Eduardo Paredes Ochoa

PRESIDENTE DEL TRIBUNAL

Ing. M.Sc. Geovanni D. Brito M.

DOCENTE CALIFICADOR

Ing. M.Sc. Edwin R. Morales P.

DOCENTE CALIFICADOR

DEDICATORIA:

Especialmente a Dios y a la memoria de mi padre **Ing. Carlos Ramos**, quién en vida supo brindarme su apoyo, consejos, comprensión, amor, fuerzas para seguir adelante y no desfallecer en los problemas que se presentaban, enseñándome a encarar las adversidades. Queda en mí, su ejemplo y esa interminable lucha por conseguir lo propuesto y ser mejor día a día.

Con todo el amor a mi madre **Magdalena Durán**, por ser el pilar fundamental en todo lo que soy, por creer en mí, estar siempre a mi lado brindándome palabras de aliento y ser la luz que guía mis pasos.

A mis hermanos, **Verónica** y **Carlitos** que con su presencia alegran mi vida.

Para mi angelito **Ariel**, por ser la razón de mí existir y el motivo de mis triunfos.

A **Ernesto**, por brindarle a mi vida nuevos sueños, esperanzas y metas.

Jessica Ramos

AGRADECIMIENTO

A mi *madre* por su fortaleza y sacrificio constante.

A mis *abuelitos* y *tíos*, quienes me brindaron su apoyo incondicional.

A *Ernesto*, por su amor y respaldo.

Un agradecimiento especial para el *Ing. Julio Cuji*, quien contribuyo de manera fundamental a la realización de mi trabajo de graduación.

Al personal docente y administrativo de la *Facultad de Ingeniería en Sistemas, Electrónica e Industrial*.

Al *Gobierno Autónomo Descentralizado Municipal de Tulcán*, especialmente a la Jefatura de Sistemas informáticos.

Jessica Ramos

ÍNDICE DE CONTENIDO

Contenido	Página
APROBACIÓN DEL TUTOR.....	II
AUTORÍA.....	III
APROBACIÓN DE LA COMISIÓN CALIFICADORA.....	IV
DEDICATORIA:	V
AGRADECIMIENTO	VI
ÍNDICE DE CONTENIDO	VII
ÍNDICE DE FIGURAS.....	XIII
ÍNDICE DE TABLAS	XVI
RESUMEN EJECUTIVO	XIX
INTRODUCCIÓN	XX
CAPÍTULO I	1
EL PROBLEMA DE INVESTIGACIÓN.....	1
1.1 TEMA	1
1.2 PLANTEAMIENTO DEL PROBLEMA	1
1.2.1 CONTEXTUALIZACIÓN	1
1.2.2 ÁRBOL DEL PROBLEMA.....	3
1.2.3 ANÁLISIS CRÍTICO	4
1.2.4 PROGNOSIS	4
1.2.5 FORMULACIÓN DEL PROBLEMA.....	5
1.2.6 PREGUNTAS DIRECTRICES	5
1.2.7 DELIMITACIÓN DEL PROBLEMA	5
1.3 JUSTIFICACIÓN	6
1.4 OBJETIVOS	7
1.4.1 OBJETIVO GENERAL:.....	7
1.4.2 OBJETIVOS ESPECÍFICOS:.....	7
CAPÍTULO II.....	8
MARCO TEÓRICO.....	8

2.1	ANTECEDENTES INVESTIGATIVOS	8
2.2	FUNDAMENTACIÓN LEGAL.....	9
2.2.1	GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN.....	9
2.2.2	ORGANISMOS: CABLEADO DE RED	11
2.3	GRÁFICA DE INCLUSIÓN DE LAS CATEGORÍAS FUNDAMENTALES	12
2.3.1	CONSTELACIÓN DE IDEAS DE LA VARIABLE INDEPENDIENTE	13
2.3.2	CONSTELACIÓN DE IDEAS DE LA VARIABLE DEPENDIENTE...	14
2.4	CATEGORÍAS FUNDAMENTALES	15
2.4.1	SISTEMAS DE SEGURIDAD	15
2.4.1.1	Características de un Sistema de Seguridad.....	15
2.4.1.2	Sistemas de Seguridad Electrónica	15
2.4.2	LA EVOLUCIÓN HACIA LA TECNOLOGÍA IP.....	16
2.4.2.1	Sistemas tradicionales	16
2.4.2.2	Seguridad y vigilancia IP	17
2.4.3	TECNOLOGÍA IP	18
2.4.3.1	Direccionamiento IP	19
2.4.4	CÁMARA DIGITAL.....	20
2.4.4.1	Componentes que constituyen una cámara IP.....	21
2.4.4.2	Tipos de cámaras de red.....	24
2.4.4.3	Administración de cámaras.....	29
2.4.4.4	Resolución de imagen	30
2.4.4.5	Digitalización de imagen	33
2.4.4.6	Códec	33
2.4.4.7	Compresión	34
2.4.5	GRABADORES DE VIDEO USADOS PARA LA VIDEO-VIGILANCIA	38
2.4.5.1	Digital video Recorder (DVR).....	38
2.4.5.2	Network video recorder (NVR)	38
2.4.6	SISTEMAS DE COMUNICACIÓN.....	39
2.4.6.1	Componentes de un sistema de comunicación.....	39
2.4.6.2	Comunicaciones Inalámbricas	40
2.4.6.3	Comunicaciones Alámbricas.....	41
2.4.7	REDES DE DATOS	44
2.4.7.1	Tipos de Redes.....	44

2.4.7.2	Cableado de la red.....	44
2.4.8	SISTEMA DE TIEMPO REAL (STR).....	48
2.4.8.1	Video en tiempo real.....	48
2.4.8.2	Protocolos de tiempo real.....	50
2.4.8.3	Protocolo de transporte de datos para video en red.....	50
2.5	HIPÓTESIS.....	52
2.6	SEÑALAMIENTO DE VARIABLES.....	52
CAPÍTULO III.....		53
METODOLOGÍA.....		53
3.1	ENFOQUE DE LA INVESTIGACIÓN.....	53
3.2	MODALIDAD BÁSICA DE INVESTIGACIÓN.....	53
3.3	TIPOS DE INVESTIGACIÓN.....	54
3.4	POBLACIÓN Y MUESTRA.....	54
3.5	OPERACIONALIZACIÓN DE VARIABLES.....	55
3.6	TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN.....	57
3.7	RECOLECCIÓN DE INFORMACIÓN.....	57
3.8	PROCESAMIENTO DE LA INFORMACIÓN.....	58
3.9	ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.....	58
CAPÍTULO IV.....		59
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.....		59
4.1	INTRODUCCIÓN.....	59
4.2	RED DEL GADMT.....	60
4.2.1	PUNTOS DE RED DEL GADMT.....	60
4.2.2	EQUIPOS DE RED DEL GADMT.....	61
4.2.3	EQUIPOS SERVIDORES DEL GADMT.....	62
4.2.4	ANÁLISIS DE TRÁFICO DE LA RED ACTUAL DEL GADMT.....	62
4.2.4.1	Determinación del tráfico LAN.....	62
4.2.4.2	Resultados del monitoreo de la red del GADMT.....	65
4.2.4.3	Análisis de tráfico de la red del GADMT.....	68
4.3	ENCUESTA.....	73
4.4	ENTREVISTA.....	85
4.4.1	Objetivos:.....	85
4.4.2	Desarrollo de preguntas y repuestas:.....	85
4.4.3	Análisis e interpretación de la información obtenida:.....	88

CAPÍTULO V	89
CONCLUSIONES Y RECOMENDACIONES	89
5.1 CONCLUSIONES	89
5.2 RECOMENDACIONES	90
CAPÍTULO VI.....	91
PROPUESTA.....	91
6.1 DATOS INFORMATIVOS	91
6.2 ANTECEDENTES	92
6.3 JUSTIFICACIÓN	92
6.4 OBJETIVOS	93
6.4.1 OBJETIVO GENERAL	93
6.4.2 OBJETIVOS ESPECÍFICOS	93
6.5 ANÁLISIS DE FACTIBILIDAD	93
6.5.1 FACTIBILIDAD TÉCNICA	93
6.5.2 FACTIBILIDAD OPERATIVA	94
6.5.3 FACTIBILIDAD ECONÓMICA.....	94
6.6 FUNDAMENTACIÓN CIENTÍFICO – TÉCNICA	95
6.6.1 VIDEO EN RED.....	95
6.6.1.1 Visión general de un sistema de video en red	95
6.6.1.2 Ventajas de un sistema de video-vigilancia de red digital	96
6.6.1.3 Directrices para seleccionar una cámara de red	97
6.6.2 TECNOLOGÍAS DE RED	97
6.6.2.1 Red de área local y Ethernet.....	97
6.6.2.2 Tipos de redes Ethernet.....	98
6.6.2.3 Alimentación a través de Ethernet	99
6.6.3 SISTEMAS DE GESTIÓN DE VÍDEO	100
6.6.3.1 Plataformas de hardware.....	100
6.6.4 CONSIDERACIONES SOBRE ANCHO DE BANDA Y ALMACENAMIENTO	102
6.6.4.1 Requerimiento del sistema	103
6.6.4.2 Requisitos de ancho de banda	104
6.6.4.3 Determinación aproximada del Ancho de Banda requerido	105
6.6.4.4 Calcular requisitos de almacenamiento.....	106
6.6.5 VIRTUAL LOCAL AREA NETWORKS (VLANs).....	107

6.6.5.1	Tipos de VLAN.....	108
6.6.5.2	Modos de puertos del Switch	109
6.6.5.3	Tipos de puertos	109
6.6.5.4	Etiquetado de trama	110
6.6.5.5	Configurar un Enlace Troncal.....	110
6.6.5.6	Enrutamiento entre VLAN.....	111
6.6.6	Comunicación a través de Internet.....	113
6.6.6.1	Conexiones a Internet.....	113
6.6.6.2	Puertos.....	113
6.6.6.3	Configuración de las direcciones IPv4.....	114
6.6.6.4	NAT (Network address translation – Traducción de dirección de red) 114	
6.7	METODOLOGIA	116
6.8	SITUACIÓN ACTUAL DE LA RED DE COMUNICACIONES DEL GADMT	118
6.8.1	GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN	118
6.8.1.1	Niveles de organización y divisiones de trabajo por procesos del GADMT	118
6.8.1.2	Organigrama y descripción de los procesos.....	120
6.8.1.3	Recurso humano del GADMT	122
6.8.1.4	Distribución de unidades /direcciones en el edificio municipal de Tulcán 122	
6.8.2	DESCRIPCIÓN ACTUAL DE LA RED DE COMUNICACIONES INTERNA DEL GADMT.....	123
6.8.2.1	Equipos de red.....	129
6.8.2.2	Servidores	131
6.8.2.3	Topología física de red del GADMT	131
6.8.2.4	Topología lógica de red del GADMT	132
6.8.2.5	Diagrama de comunicaciones del GADMT.....	132
6.8.2.6	Software utilizado en el sistema de comunicaciones	134
6.9	MODELO OPERATIVO	135
6.9.1	DISEÑO DEL SISTEMA DE VIGILANCIA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN	135
6.9.1.1	Análisis Técnico del Lugar	135
6.9.1.2	Ubicación de las cámaras.....	135

6.9.1.3	Fachada frontal del GADMT	146
6.9.1.4	Características de las cámaras requeridas	147
6.9.1.5	Análisis de equipos vigentes en el mercado.....	147
6.9.1.6	Cuadros comparativos: especificaciones técnicas de las cámaras IP ..	156
6.9.1.7	Análisis técnico de las cámaras IP elegidas para el diseño	161
6.9.1.8	Características software y hardware para la gestión de video.....	164
6.9.1.9	Determinación aproximada del ancho de banda requerido	170
6.9.1.10	Diagrama de la red LAN con cámaras IP.....	170
6.9.2	DISEÑO DE LA RED VIRTUAL DE ÁREA LOCAL (VLAN) PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN	
	172	
6.9.2.1	Análisis previo al diseño de VLAN	172
6.9.2.2	Distribución de VLAN.....	172
6.9.2.3	Configuración de VLAN.....	176
6.9.2.4	Disposición de equipos	178
6.9.2.5	Simulación de las redes virtuales	180
6.9.3	ACCESO REMOTO	193
6.9.3.1	Visualización de las cámaras por internet.....	193
6.9.3.2	Configuración del redireccionamiento de puertos mediante NAT para habilitar acceso remoto a la cámara IP.....	194
6.9.4	ANÁLISIS FINANCIERO	197
6.10	CONCLUSIONES	202
6.11	RECOMENDACIONES.....	204
6.12	BIBLIOGRAFÍA	205
6.13	LINKOGRAFÍA	206
6.14	ANEXOS	208
	ANEXO 1. ENCUESTA REALIZADA A LOS EMPLEADOS ADMINISTRATIVOS DEL GADMT	208
	ANEXO 2. ENTREVISTA REALIZADA A LA DIRECTORA DE LA UNIDAD DE INFORMÁTICA DEL GADMT	210
	ANEXO 3. ESPECIFICACIONES TÉCNICAS DE LAS CÁMARAS DE RED SELECCIONADAS.....	212
	ANEXO 4. CARACTERISTICAS DE LOS SWITCHES DE CISCO CATALYST 2960.....	223
	ANEXO 5. FOTOS DE LA RED DE COMUNICACIONES ACTUAL DEL GADMT	227

ÍNDICE DE FIGURAS

Capítulo I

Figura N° 1. 1 Árbol del problema.....	3
--	---

Capítulo II

Figura N° 2. 1 Categorías Fundamentales de la Variable Independiente y Dependiente.	12
Figura N° 2. 2 Constelación de ideas de la variable independiente	13
Figura N° 2. 3 Constelación de ideas de la variable dependiente	14
Figura N° 2. 4 Circuito cerrado de TV analógico usando VCR.....	17
Figura N° 2. 5 Esquema del sistema de video-vigilancia.....	18
Figura N° 2. 6 Cámara de red conectada directamente a la red LAN	20
Figura N° 2. 7 Componentes internos de una cámara IP	21
Figura N° 2. 8 Sensores de imagen: CCD (a la izquierda); CMOS (a la derecha).....	23
Figura N° 2. 9 Cámara fija IP.....	25
Figura N° 2. 10 Cámara domo fija IP.	25
Figura N° 2. 11 Cámara PTZ IP.....	26
Figura N° 2. 12 Cámara domo PTZ IP.....	27
Figura N° 2. 13 Cámara PTZ IP no mecánica.....	28
Figura N° 2. 14 Cámara PTZ IP mecánica.....	28
Figura N° 2. 15 Respuesta de un sensor de imagen a la luz.....	29
Figura N° 2. 16 A la izquierda, diferentes resoluciones de imagen NTSC. A la derecha, diferentes resoluciones de imagen PAL.....	30
Figura N° 2. 17 Esquema básico de compresión y descompresión.....	34
Figura N° 2. 18 Esquema básico de compresión y descompresión.....	35
Figura N° 2. 19 Codificación diferencial	35
Figura N° 2. 20 Esquema básico de compresión y descompresión.....	37
Figura N° 2. 21 Circuito cerrado de TV analógica usando DVR.....	38
Figura N° 2. 22 Sistema de circuito cerrado de TV analógico usando DVR de red	39
Figura N° 2. 23 Tipos de cables: directo, de conexión cruzada y de consola.	42
Figura N° 2. 24 Subsistemas de cableado estructurado	46
Figura N° 2. 25 Esquema básico del Sistema Streaming.	49

Capítulo IV

Figura N° 4. 1 Monitoreo del tráfico LAN del GADMT	63
Figura N° 4. 2 Selección del canal del cual se capturará los paquetes de la WLAN del GADMT	64
Figura N° 4. 3 Captura de paquetes del canal 5 correspondiente a la WLAN del GADMT	65
Figura N° 4. 4 Cantidad de tráfico LAN para un monitoreo de 5 días.....	69
Figura N° 4. 5 Tasa de transferencia LAN para un monitoreo de 5 días.....	69
Figura N° 4. 6 Porcentaje de utilización LAN para un monitoreo de 5 días	70
Figura N° 4. 7 Cantidad de tráfico WLAN para un monitoreo de 5 días	71
Figura N° 4. 8 Tasa de transferencia WLAN para un monitoreo de 5 días.....	71
Figura N° 4. 9 Porcentaje de utilización WLAN para un monitoreo de 5 días	72
Figura N° 4. 10 Existencia de un sistema de vigilancia en el GADMT	73
Figura N° 4. 11 Mecanismo eficiente en el ámbito de la seguridad y vigilancia	74
Figura N° 4. 12 Aceptación a la visualización de información Institucional	75
Figura N° 4. 13 Consentimiento en la inspección de bienes Institucionales.....	76
Figura N° 4. 14 Conocimiento de sucesos indebidos efectuados en el GADMT.....	77
Figura N° 4. 15 Aceptación del almacenamiento de información institucional	78
Figura N° 4. 16 Unidades del GADMT que requieren de un sistema de video-vigilancia.	79
Figura N° 4. 17 Principales utilidades que aporta un sistema de video-vigilancia para el GADMT.....	80
Figura N° 4. 18 Aprobación de la existencia de un sistema de video-vigilancia en el GADMT.....	81
Figura N° 4. 19 Velocidad del internet en el GADMT	82
Figura N° 4. 20 Tipo de información al cual acceden los empleados del GADMT	83
Figura N° 4. 21 Frecuencia del uso de internet en el edificio Municipal.	84

Capítulo VI

Figura N° 6. 1 Sistema de video en red.....	95
Figura N° 6. 2 Sistema de video-vigilancia en red basado en una plataforma abierta de servidor de PC.....	101
Figura N° 6. 3 Sistema de video-vigilancia en red que utiliza un NVR.....	102
Figura N° 6. 4 Red virtual de área local (VLAN)	108
Figura N° 6. 5 Formato de trama 802.1Q.....	110
Figura N° 6. 6 Enlace Troncal entre switch	111
Figura N° 6. 7 Router sin trunk	112
Figura N° 6. 8 Router con trunk (router on-a-stick).....	113
Figura N° 6. 9 Esquema de Trabajo	117

Figura N° 6. 10 Edificio del Gobierno Autónomo Descentralizado Municipal de Tulcán	118
Figura N° 6. 11 Organigrama Estructural del GADMT	121
Figura N° 6. 12 Topología física de red del GADMT.....	132
Figura N° 6. 13 Diagrama de red del GADMT	133
Figura N° 6. 14 Ubicación de las cámaras IP en la Planta baja del GADMT	136
Figura N° 6. 15 Ubicación de las cámaras IP en el Primer piso del GADMT	138
Figura N° 6. 16 Ubicación de las cámaras IP en el Segundo piso del GADMT	140
Figura N° 6. 17 Ubicación de las cámaras IP en el Tercer piso del GADMT.....	142
Figura N° 6. 18 Ubicación de las cámaras IP en el Cuarto piso del GADMT	144
Figura N° 6. 19 Fachada Frontal del GADMT.....	146
Figura N° 6. 20 VIVOTEK FD8134	148
Figura N° 6. 21 VIVOTEK FD7132	149
Figura N° 6. 22 VIVOTEK PZ7132.....	150
Figura N° 6. 23 VIVOTEK SD8121	151
Figura N° 6. 24 TV-IP572PI	152
Figura N° 6. 25 TV-IP672PI	153
Figura N° 6. 26 TV-IP422WN	154
Figura N° 6. 27 Vstarcam H6812L.....	155
Figura N° 6. 28 Vstarcam F6836w.....	155
Figura N° 6. 29 Interfaz gráfica del software SecurView Pro.....	165
Figura N° 6. 30 Captura de video gestionado con el software SecurView Pro.....	165
Figura N° 6. 31 Diagrama de la red LAN con cámaras IP	171
Figura N° 6. 32 Creación de VLAN's para el GADMT.....	172
Figura N° 6. 33 Direccionamiento IP para la red de vigilancia del GADMT	178
Figura N° 6. 34 Cisco Catalyst 2960-24TT-L.....	179
Figura N° 6. 35 Simulación de las VLAN's en Packet Tracer.....	181
Figura N° 6. 36 VLAN creadas en el switch - Packet Tracer.....	183
Figura N° 6. 37 Asignación de puertos de las VLAN en el switch- Packet Tracer.....	184
Figura N° 6. 38 Información del puerto fa0/2 del switch -Packet Tracer	186
Figura N° 6. 39 Información del enlace troncal en el switch- Packet Tracer.....	187
Figura N° 6. 40 Habilitación del puerto del Router - Packet Tracer	192
Figura N° 6. 41 Sub-interfaces del Router - Packet Tracer.....	192
Figura N° 6. 42 Envío de paquetes en tiempo real - Packet Tracer.....	193
Figura N° 6. 43 Visualización de las cámaras del GADMT por internet.....	194
Figura N° 6. 44 Redireccionamiento de puertos	196

ÍNDICE DE TABLAS

Capítulo II

Tabla N° 2. 1 Resoluciones VGA	31
Tabla N° 2. 2 Formatos megapíxel.....	32
Tabla N° 2. 3 Protocolos y puertos TCP/IP habituales utilizados para el video en red	51

Capítulo III

Tabla N° 3. 1 Operacionalización de la variable independiente: Sistema de Vigilancia. .	55
Tabla N° 3. 2 Operacionalización de la variable dependiente: Acceso Remoto	56
Tabla N° 3. 3 Plan de recolección de información.....	57

Capítulo IV

Tabla N° 4. 1 Distribución de puntos de red de Pc's e impresoras en el edificio municipal	60
Tabla N° 4. 2 Equipos de red del GADMT	61
Tabla N° 4. 3 Equipos servidores GADMT	62
Tabla N° 4. 4 Tráfico LAN Lunes 28 de Mayo del 2012.....	66
Tabla N° 4. 5 Tráfico LAN Martes 29 de Mayo del 2012	66
Tabla N° 4. 6 Tráfico LAN Miércoles 30 de Mayo del 2012.....	66
Tabla N° 4. 7 Tráfico LAN Jueves 31 de Mayo del 2012.....	66
Tabla N° 4. 8 Tráfico LAN Viernes 1 de Junio del 2012.....	66
Tabla N° 4. 9 Tráfico WLAN Lunes 28 de Mayo del 2012	67
Tabla N° 4. 10 Tráfico WLAN Martes 29 de Mayo del 2012.....	67
Tabla N° 4. 11 Tráfico WLAN Miércoles 30 de Mayo del 2012.....	67
Tabla N° 4. 12 Tráfico WLAN Jueves 31 de Mayo del 2012	67
Tabla N° 4. 13 Tráfico WLAN Viernes 1 de Junio del 2012.....	68
Tabla N° 4. 14 Existencia de un sistema de vigilancia en el edificio del GADMT	73
Tabla N° 4. 15 Mecanismo eficiente en el ámbito de la seguridad y vigilancia, según los empleados de la dirección de Gestión administrativa del GADMT	74
Tabla N° 4. 16 Aceptación a la visualización de información por parte de lo empleados del GADMT	75
Tabla N° 4. 17 Consentimiento en la inspección de bienes de los empleados en el interior del edificio municipal	76

Tabla N° 4. 18 Conocimiento de sucesos indebidos efectuados en el GADMT	77
Tabla N° 4. 19 Aceptación del almacenamiento de información por parte de lo empleados del GADMT	78
Tabla N° 4. 20 . Unidades del GADMT que requieren de un sistema de video-vigilancia	79
Tabla N° 4. 21 Principales utilidades que aporta un sistema de video-vigilancia para el GADMT	80
Tabla N° 4. 22 Aprobación de la existencia de un sistema de video-vigilancia en el GADMT	81
Tabla N° 4. 23 Velocidad del internet en el GADMT.....	82
Tabla N° 4. 24 Tipo de información al cual acceden los empleados del GADMT	83
Tabla N° 4. 25 Frecuencia del uso de internet en el edificio Municipal	84

Capítulo VI

Tabla N° 6. 1 Clasificaciones de potencia según IEEE 802.3af.....	100
Tabla N° 6. 2 Factores que varían la tasa de bits.....	103
Tabla N° 6. 3 Tasas de bits estimadas para una cámara IP	105
Tabla N° 6. 4 Cálculo de la capacidad de almacenamiento de un sistema.....	106
Tabla N° 6. 5 Niveles de organización y divisiones de trabajo por procesos del GADMT	120
Tabla N° 6. 6 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en la planta baja del edificio municipal.....	124
Tabla N° 6. 7 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el primer piso del edificio municipal.....	125
Tabla N° 6. 8 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el segundo piso del edificio municipal	126
Tabla N° 6. 9 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el tercer piso del edificio municipal.	127
Tabla N° 6. 10 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el cuarto piso del edificio municipal.....	128
Tabla N° 6. 11 Equipos de red existentes en la planta baja del edificio municipal.....	129
Tabla N° 6. 12 Equipos de red existentes en el primer piso del edificio municipal.....	129
Tabla N° 6. 13 Equipos de red existentes en el segundo piso del edificio municipal. ...	130
Tabla N° 6. 14 Equipos de red existentes en el tercer piso del edificio municipal.	130
Tabla N° 6. 15 Equipos de red existentes en el cuarto piso del edificio municipal.	130
Tabla N° 6. 16 Características de los Servidores de red del GADMT	131
Tabla N° 6. 17 Zonas a ser cubiertas por el sistema de cámaras digitales	135
Tabla N° 6. 18 Ubicación de las cámaras IP en la Planta baja del GADMT	137
Tabla N° 6. 19 Ubicación de las cámaras IP en el Primer piso del GADMT.....	139
Tabla N° 6. 20 Ubicación de las cámaras IP en el Segundo piso del GADMT	141
Tabla N° 6. 21 Ubicación de las cámaras IP en el Tercer piso del GADMT	143
Tabla N° 6. 22 Ubicación de las cámaras IP en el Cuarto piso del GADMT.....	145
Tabla N° 6. 23 Características de las cámaras IP para las zonas determinadas	147
Tabla N° 6. 24 Análisis técnico: cámara fija requerida en las oficinas del GADMT	157

Tabla N° 6. 25 Análisis técnico: cámara fija requerida en la biblioteca del GADMT	158
Tabla N° 6. 26 Análisis técnico: cámara PTZ requerida en las oficinas y el salón de usos múltiples del GADMT	159
Tabla N° 6. 27 Análisis técnico: cámara PTZ inalámbrica requerida en el hall y accesos principales	160
Tabla N° 6. 28 Modelo de cámara IP a utilizarse por cada Unidad del GADMT	163
Tabla N° 6. 29 Características del servidor de video	167
Tabla N° 6. 30 Almacenamiento de video	168
Tabla N° 6. 31 Almacenamiento por día	169
Tabla N° 6. 32 Características de la estación remota	169
Tabla N° 6. 33 Estimación del Ancho de Banda por cámara	170
Tabla N° 6. 34 Hosts requeridos para la creación de la subred de la VLAN2	173
Tabla N° 6. 35 Hosts requeridos para la creación de la subred de la VLAN3	174
Tabla N° 6. 36 Hosts requeridos para la creación de la subred de la VLAN4	175
Tabla N° 6. 37 Subredes destinadas para las VLAN''s.....	176
Tabla N° 6. 38 Direccionamiento IP para la red de vigilancia del GADMT	177
Tabla N° 6. 39 Especificaciones Técnicas del switch Cisco Catalyst 2960-24TT-L	179
Tabla N° 6. 40 Asignación de puertos Switch VIGILANCIA1	182
Tabla N° 6. 41 Asignación de puertos Switch VIGILANCIA2	182
Tabla N° 6. 42 Asignación de los puertos de cámaras IP.....	195
Tabla N° 6. 43 Costo de los equipos del proyecto	198
Tabla N° 6. 44 Costo de instalación	198
Tabla N° 6. 45 AB actual	198
Tabla N° 6. 46 AB adicional	198
Tabla N° 6. 47 AB requerido en el proyecto.....	199
Tabla N° 6. 48 Inversión	199
Tabla N° 6. 49 Egresos.....	200
Tabla N° 6. 50 Ingresos.....	200
Tabla N° 6. 51 Flujo de caja.....	200

RESUMEN EJECUTIVO

El presente trabajo de graduación está dirigido a garantizar seguridad e impulsar el desarrollo del Gobierno Autónomo Descentralizado Municipal de Tulcán (GADMT), en aspectos referentes a la calidad de vigilancia, la toma de soluciones oportunas, el acceso local y remoto a la red institucional, fomentando orden y regularidad en el diario accionar de los empleados municipales.

En el primer capítulo se determina el problema existente en el edificio del GADMT debido a la escasa supervisión de las Unidades Operativas, ya que se posee limitaciones en lo concerniente al control de dependencias que requieren supervisión continua. Se plantean también los objetivos que se desean alcanzar en la investigación, respaldando así la ejecución del proyecto de investigación.

El segundo capítulo presenta los antecedentes investigativos, la fundamentación legal, organismos relacionados al tema de estudio, un amplio desarrollo informativo de las categorías fundamentales, sustentando los conocimientos a través de conceptos facultativos, dando lugar al desarrollo la hipótesis.

En el tercer capítulo se establece la metodología que fue utilizada en la investigación, así como las modalidades y técnicas de investigación empleadas y el procesamiento de información, siguiendo un orden de funcionalidades para optimizar tiempo y obtener resultados efectivos.

El cuarto capítulo contiene el análisis e interpretación de los resultados obtenidos en la encuesta, entrevista y el análisis de tráfico de la red del GADMT. Las técnicas investigativas mencionadas permitieron obtener la documentación necesaria a cerca de requerimientos y necesidades existentes para de esta manera poner en marcha el proyecto de diseño. Seguidamente frente a los antecedentes expuestos, en el capítulo cinco se puntualizan las conclusiones y recomendaciones provenientes de las investigaciones efectuadas.

En el sexto capítulo se encuentra el desarrollo de la propuesta, como solución a los problemas existentes. Se detallan los requerimientos y desarrollo del diseño mediante un análisis técnico y financiero.

INTRODUCCIÓN

El documento presentado a continuación, toma como punto de partida el cumplimiento a la demanda de seguridad existente en el Gobierno Autónomo Descentralizado Municipal de Tulcán, con el diseño de un sistema de vigilancia de última tecnología, como alternativa actual y muy versátil, el mismo que potencie la capacidad de monitoreo, con lo que se conseguirá un mecanismo eficiente.

La vigilancia, puesta en marcha a través de cualquier medio, es un servicio de seguridad preventivo, que busca mediante la observación de un lugar en tiempo real, detectar, registrar y permitir responder a posibles violaciones en la seguridad de un predio, ataque contra equipos, sustracción de bienes, etc.

La solución que se propone facultará la protección y resguardo de las unidades operativas ya sea de forma local como de forma remota. Con el avance de la tecnología de video digital IP, los responsables de seguridad y de la jefatura de informática, pueden adoptar una solución verdaderamente integrada que es capaz satisfacer las necesidades de seguridad existentes, mientras que al mismo tiempo reduce los costos operativos al integrarlos a la red de datos, facilitando su administración, protegiendo la inversión y optimizando la demanda de ancho de banda.

La tecnología digital está cada día más extendida, y sustituye progresivamente a las propuestas analógicas. Empleando estándares y protocolos abiertos, de forma que el sistema pueda migrar fácilmente a entornos nuevos y mejorados.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 TEMA

Red de Video-vigilancia mediante tecnología IP para el acceso remoto de las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán.

1.2 PLANTEAMIENTO DEL PROBLEMA

1.2.1 CONTEXTUALIZACIÓN

Los sistemas de monitoreo a través de video IP constituyen una tecnología emergente que está modificando el escenario de la industria de seguridad y vigilancia, dejando atrás los tradicionales CCTV (Circuitos Cerrados de Televisión) analógicos, para de esta manera ofrecer un sinnúmero de beneficios que junto al avance y difusión de la internet, hacen posible la video-vigilancia remota.

Con el incremento del volumen de datos, desarrollo tecnológico y competencia corporativa internacional, muchas compañías han percibido la necesidad no sólo proteger su información, sino también sus recursos humanos e infraestructura que se encuentran al servicio de la compañía.

De esta manera los sistemas de vigilancia por video se están volviendo más comunes en los edificios de oficinas, estructuras externas, hogares, escuelas e incluso en las calles.

En nuestro país los sistemas de video-vigilancia con tecnología IP han tenido un gran auge en los últimos años ya que casi todas las empresas cuentan actualmente con una infraestructura de red a su disposición, en consecuencia se posibilita favorablemente su implementación, proponiendo una solución frente a los sistemas analógicos que requieren de una gran cantidad de cableado y brindan una pobre capacidad de administración de las imágenes.

En la ciudad de Tulcán se está dando paso a la implementación de estos sistemas de vigilancia en empresas y locales debido a las necesidades de contar con una amplia gama de servicios para mantener la seguridad, el orden y el correcto funcionamiento de dichas organizaciones.

El Gobierno Autónomo Descentralizado Municipal de Tulcán (GADMT) actualmente cuenta con un sistema deficiente de vigilancia por lo que posee limitaciones en cuanto se refiere al control de actividades que necesitan supervisión en las distintas unidades de la entidad.

1.2.2 ÁRBOL DEL PROBLEMA

En la Figura N°1.1 se detalla los efectos y causas en un árbol de problemas.

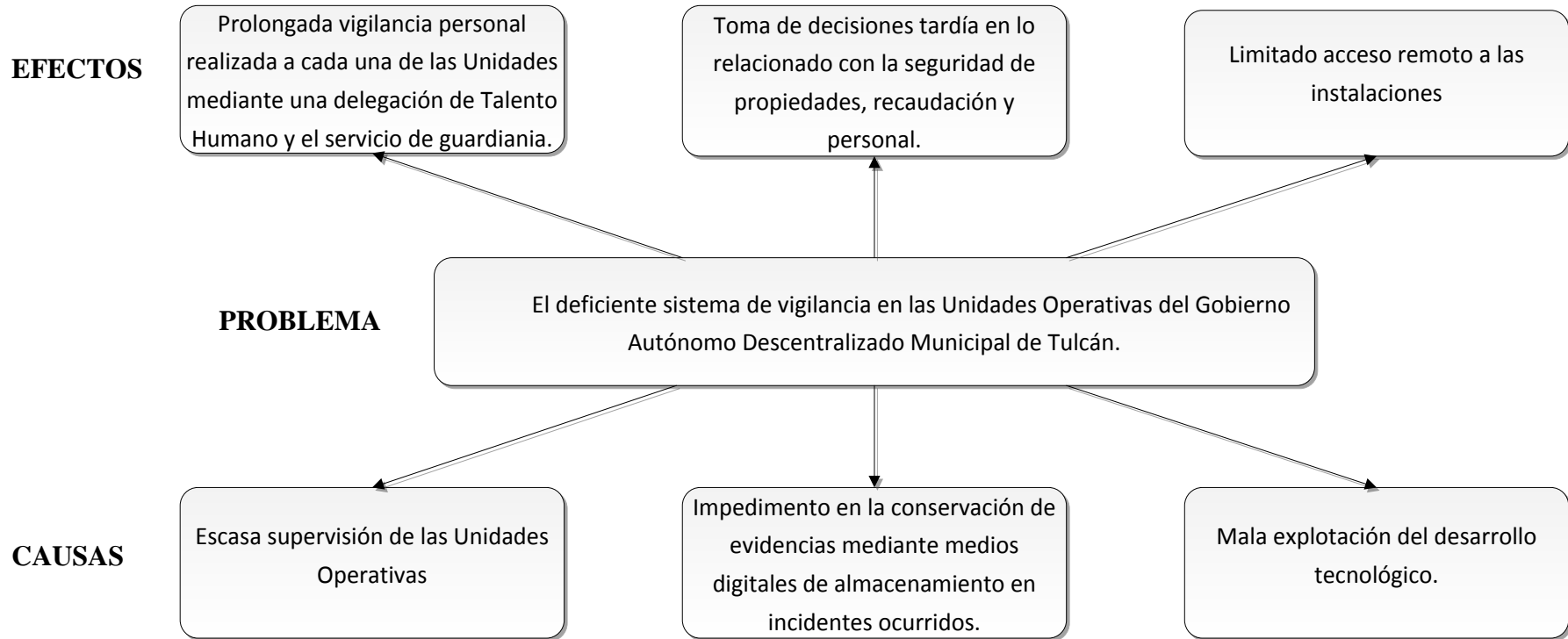


Figura N° 1. 1 Árbol del problema
Elaborado por: El Investigador

1.2.3 ANÁLISIS CRÍTICO

La vigilancia y la seguridad son temas que han adquirido relevancia en la actualidad. Hoy por hoy el Gobierno Autónomo Descentralizado Municipal de Tulcán (GADMT) dispone de un sistema deficiente de vigilancia para el control de actividades que requieren acceso remoto.

La escasa supervisión de las Unidades Operativas de la Institución ocasiona una prolongada inspección realizada a cada una de las mismas, mediante una delegación de la Jefatura de Talento Humano y el servicio de guardianía.

Además se produce un impedimento en la conservación de evidencias mediante medios digitales de almacenamiento en incidentes ocurridos, por lo que se origina una toma de decisiones tardía en caso de encontrarse inconvenientes no solo en lo que se refiere a la vigilancia del personal que ingresa a la entidad, sino también a la seguridad e inspección de recaudación y propiedades del Municipio. En el caso del control del recurso humano se tiene la finalidad de regular las actividades realizadas durante el periodo laboral, verificando que sean cumplidas a cabalidad y bajo los reglamentos de la Institución, sin que ningún tipo de suceso inesperado lo impida. Cabe mencionar también que hay ciertas Unidades en el GADMT que requieren de un control más cuidadoso que otras.

La mala explotación del desarrollo tecnológico da lugar a un limitado acceso remoto a las Instalaciones Municipales, y sin acceso a la amplia gama de beneficios que nos presenta el internet, de igual manera se denota la inhabilidad de supervisión simultánea de las diversas unidades en las instalaciones de la red.

1.2.4 PROGNOSIS

El Gobierno Autónomo Descentralizado Municipal de Tulcán al disponer de un deficiente sistema de vigilancia se verá afectado negativamente en el acceso remoto para el control de las distintas Unidades de la entidad,

palpando un escenario de irregularidad y desorganización en su interior, lo cual limitará el avance de la organización.

1.2.5 FORMULACIÓN DEL PROBLEMA

¿Cómo afecta el deficiente sistema de vigilancia en el acceso remoto de las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán?

1.2.6 PREGUNTAS DIRECTRICES

- ¿Cuáles son las técnicas de acceso remoto para las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán?
- ¿Cuál es el sistema de vigilancia actual empleado por el Gobierno Municipal?
- ¿Se puede Plantear una propuesta que permita mejorar el acceso remoto en las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán mediante un sistema de video-vigilancia con Tecnología IP?

1.2.7 DELIMITACIÓN DEL PROBLEMA

CAMPO: Ingeniería Electrónica y Comunicaciones

ÁREA: Seguridad Electrónica

ASPECTO: Sistema de video-vigilancia

DELIMITACIÓN ESPACIAL: Esta investigación se realizará en la ciudad de Tulcán, en las Unidades del Gobierno Autónomo Descentralizado Municipal de Tulcán.

DELIMITACIÓN TEMPORAL: El presente proyecto de investigación tendrá una duración de 6 meses, a partir de que este sea aprobado por el Honorable Consejo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.3 JUSTIFICACIÓN

La video-vigilancia ha asistido a la humanidad por algunas décadas desde el inicio de los primeros Circuitos Cerrados de Televisión (CCTV) que requieren una infraestructura separada que utiliza cable coaxial y cámaras analógicas, hasta los actuales sistemas de video-vigilancia digital que optimiza las inversiones en infraestructuras de red y aporta un modelo de seguridad más simple, refinado y accesible a los usuarios de una empresa.

Estos sistemas aportan seguridad fomentando el orden y transparencia en el normal accionar diario de una institución. Por lo que resulta de suma importancia contar con un sistema de video-vigilancia con tecnología IP que impulse el desarrollo del Gobierno Autónomo Descentralizado Municipal de Tulcán (GADMT), para de este modo ofrecer soluciones inmediatas y oportunas a lo referente con el control de seguridad personal, recaudación, bienes y equipos.

El presente proyecto aporta también a la integración de un concepto de gran relevancia que es la capacidad de acceso remoto desde la red interna y desde cualquier lugar del mundo a la red de la entidad municipal a través del internet, para que esta manera el personal autorizado pueda obtener una visión en tiempo real de los sucesos ocurridos en sus diferentes unidades.

Cabe señalar como un aspecto substancial el uso de la tecnología IP que convertirá la red de trabajo de la institución a “prueba de futuro” ya que proporcionará desarrollo, escalabilidad, actualizaciones e integraciones con otros sistemas que dispongan de la misma tecnología. Además de presentar un sinfín de ventajas como es el bajo costo de mantención, la facilidad de instalación, calidad de la imagen (superior a la análoga), avanzadas capacidades de búsqueda, la posibilidad de estar grabando y revisando los archivos en forma simultánea, y mejoras en el sistema de almacenamiento.

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL:

Analizar el acceso remoto en las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán y su influencia con el sistema de vigilancia aplicado.

1.4.2 OBJETIVOS ESPECÍFICOS:

1. Analizar técnicas de acceso remoto para las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán
2. Examinar el sistema de vigilancia actual empleado por el Gobierno Municipal.
3. Plantear una propuesta que permita mejorar el acceso remoto en las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán mediante un sistema de video-vigilancia con Tecnología IP.

CAPÍTULO II

MARCO TEÓRICO

2.1 ANTECEDENTES INVESTIGATIVOS

En la biblioteca de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, se obtuvieron los siguientes trabajos de investigación, los mismos que tienen congruencia con el tema planteado:

“Diseño de un Sistema de Seguridad mediante cámaras IP para la Empresa PROALDI de la Ciudad de Pillaro” ” Realizado por: Izurieta Pazmiño, Cecilia Elizabeth. Número de tesis: 562. Año: 2006.

Proyecto de pasantía “Sistema de Video Vigilancia para la Brigada de Caballería Blindada número 11 Galápagos en la ciudad de Riobamba.” Realizado por: Ibarra Córdova, Washington Daniel. Número de tesis: 370. Año: 2008.

“Sistema de vigilancia en tiempo real mediante cámaras IP, para el control de seguridad del Servicio Ecuatoriano de Capacitación Profesional – Centro de Formación Industrial Ambato” Realizado por: Beltrán Mesías, Carmen de las Mercedes. Número de tesis: 562. Año: 2011.

2.2 FUNDAMENTACIÓN LEGAL

2.2.1 GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN.

El Gobierno Autónomo Descentralizado Municipal de Tulcán tiene como labor el cumplimiento de políticas, objetivos y metas institucionales que determinen, normen y agiliten las diferentes acciones de trabajo hacia una gestión efectiva de servicios. Por la transparencia en la gestión administrativa que están obligadas a cumplir todas las Instituciones del estado que conforman el sector público.

Antecedentes Históricos

En 1827, el General Francisco de Paula Santander, Vicepresidente de la Gran Colombia, impulsado por presiones e intereses de orden político restablece la existencia política de la Provincia de Imbabura. En tan dilatada extensión se comprendía la parroquia de Tulcán como propiedad de dicha provincia, para más tarde dar lugar a la instauración del Cantón Tulcán.

Es así que en la Ciudad de Ibarra, el 19 de Diciembre de 1851 se da lugar a la elección de “Consejeros” Municipales del Cantón Tulcán.

Misión Institucional

El Gobierno Municipal de Tulcán es una Institución Autónoma y descentralizada que genera, orienta y norma planificadamente el desarrollo cantonal urbano y rural, dotando de obras de infraestructura y equipamiento básicos con aporte de la comunidad, ofertando servicios de calidad para elevar el nivel de vida de su población con equidad social. En un marco de transparencia potencia los recursos humanos, económicos y

naturales mediante la gestión financiera nacional e internacional y asume con responsabilidad el proceso de descentralización, en cumplimiento de su rol binacional, propicia alianzas de vecindad para el desarrollo regional de la frontera.

Desarrollo integral del Cantón con el respectivo equilibrio en cada una de sus Parroquias, caracterizándose como un proceso dinámico, vivo y participativo, que cada día debe ser enriquecido y perfeccionado, para conseguir el “Bienestar Común” de las Tulcaneñas y Tulcaneños.

Visión de Ciudad

Ciudad fronteriza andina prestadora de servicios, de intercambio comercial y de transferencia nacional e internacional

Visión de Cantón

Que el Cantón Tulcán, sus Parroquias y sus pobladores en general vivan un nuevo ejercicio de democracia, potencializando el cambio no solo a través de un simple canal de demandas sino como un espacio de debate y construcción de la economía, de la sociedad y de la oxigenación de la política local, para lo cuál es importante mantener un proceso permanente y participativo en el que se operativicen conceptos como: Pluriculturalidad, Plurisocietalidad, Equidad Socio Económica, de Género y Generacional actual y futura, Equilibrio y Equidad entre Biodiversidad y Desarrollo Sostenible y Sustentable, construcción de las Identidades y derecho a vivir las diferencias, Gestión Municipal, Descentralización, Gestión Local, Concertación y Gobernabilidad.

2.2.2 ORGANISMOS: CABLEADO DE RED

- **ANSI:** American National Standards Institute. Organización Privada sin fines de lucro fundada en 1918, la cual administra y coordina el sistema de estandarización voluntaria del sector privado de los Estados Unidos.
- **EIA:** Electronics Industry Association. Fundada en 1924. Desarrolla normas y publicaciones sobre las principales áreas técnicas: los componentes electrónicos, electrónica del consumidor, información electrónica, y telecomunicaciones.
- **TIA:** Telecommunications Industry Association. Fundada en 1985 después del rompimiento del monopolio de AT&T. Desarrolla normas de cableado industrial voluntario para muchos productos de las telecomunicaciones y tiene más de 70 normas preestablecidas.
- **ISO:** International Standards Organization. Organización no gubernamental creada en 1947 a nivel Mundial, de cuerpos de normas nacionales, con más de 140 países.
- **IEEE:** Instituto de Ingenieros Eléctricos y de Electrónica. Principalmente responsable por las especificaciones de redes de área local como 802.3 Ethernet, 802.5 Token Ring, ATM y las normas de Gigabit Ethernet.

2.3 GRÁFICA DE INCLUSIÓN DE LAS CATEGORÍAS FUNDAMENTALES

La Figura N° 2.1 representa las inclusiones conceptuales de las variables independiente y dependiente.

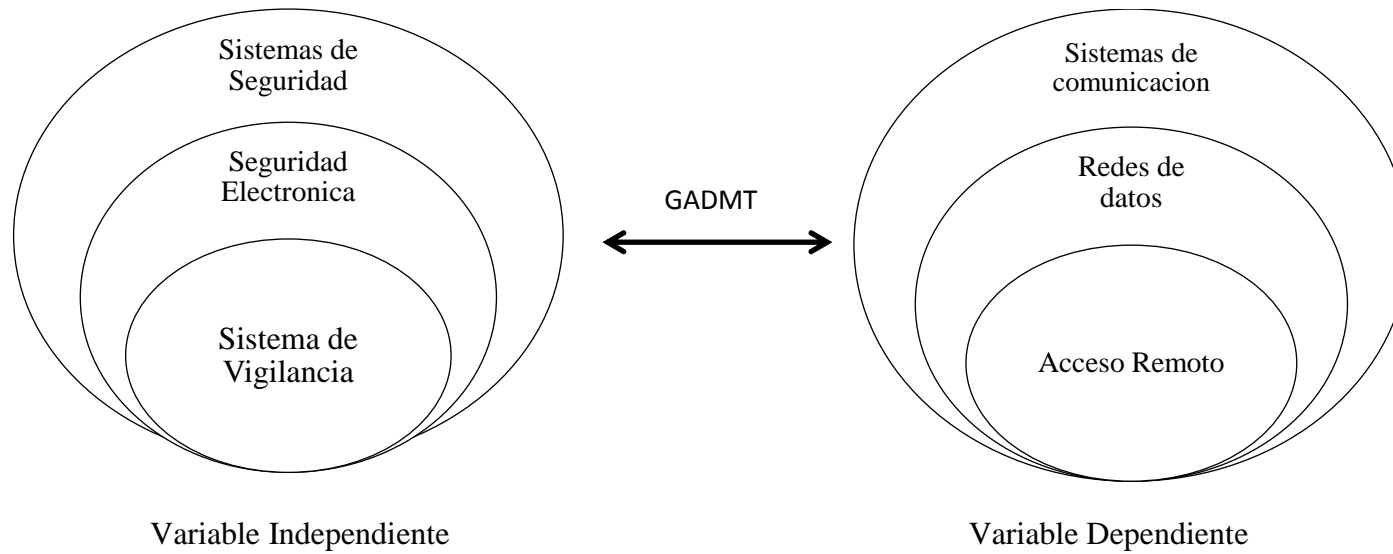


Figura N° 2. 1 Categorías Fundamentales de la Variable Independiente y Dependiente
Elaborado por: El Investigador

2.3.1 CONSTELACIÓN DE IDEAS DE LA VARIABLE INDEPENDIENTE

En la Figura N° 2.2 se expone la variable independiente por medio de una constelación de ideas.

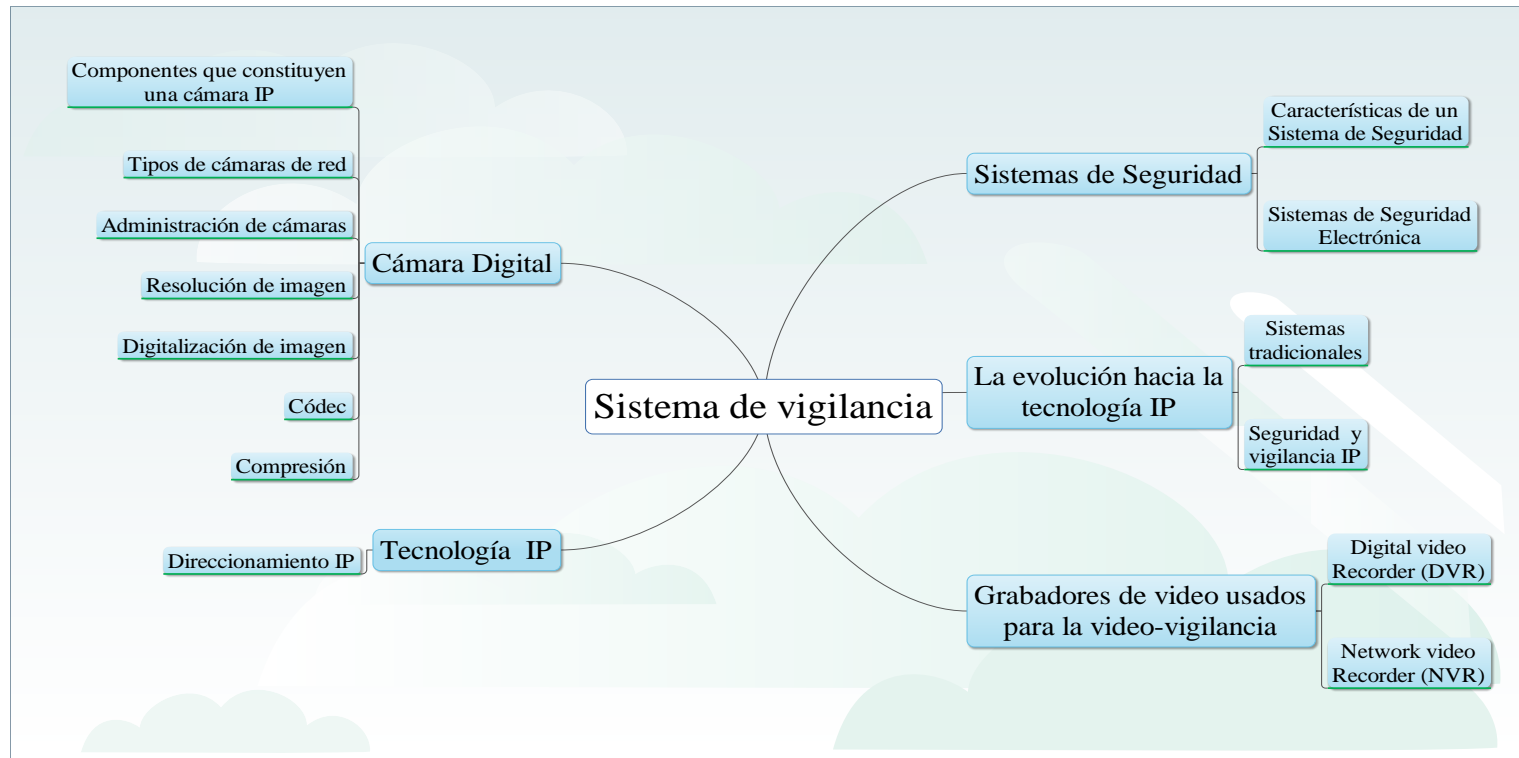


Figura N° 2. 2 Constelación de ideas de la variable independiente
Elaborado por: El Investigador

2.3.2 CONSTELACIÓN DE IDEAS DE LA VARIABLE DEPENDIENTE

En la Figura N° 2.3 se expone la variable dependiente por medio de una constelación de ideas.

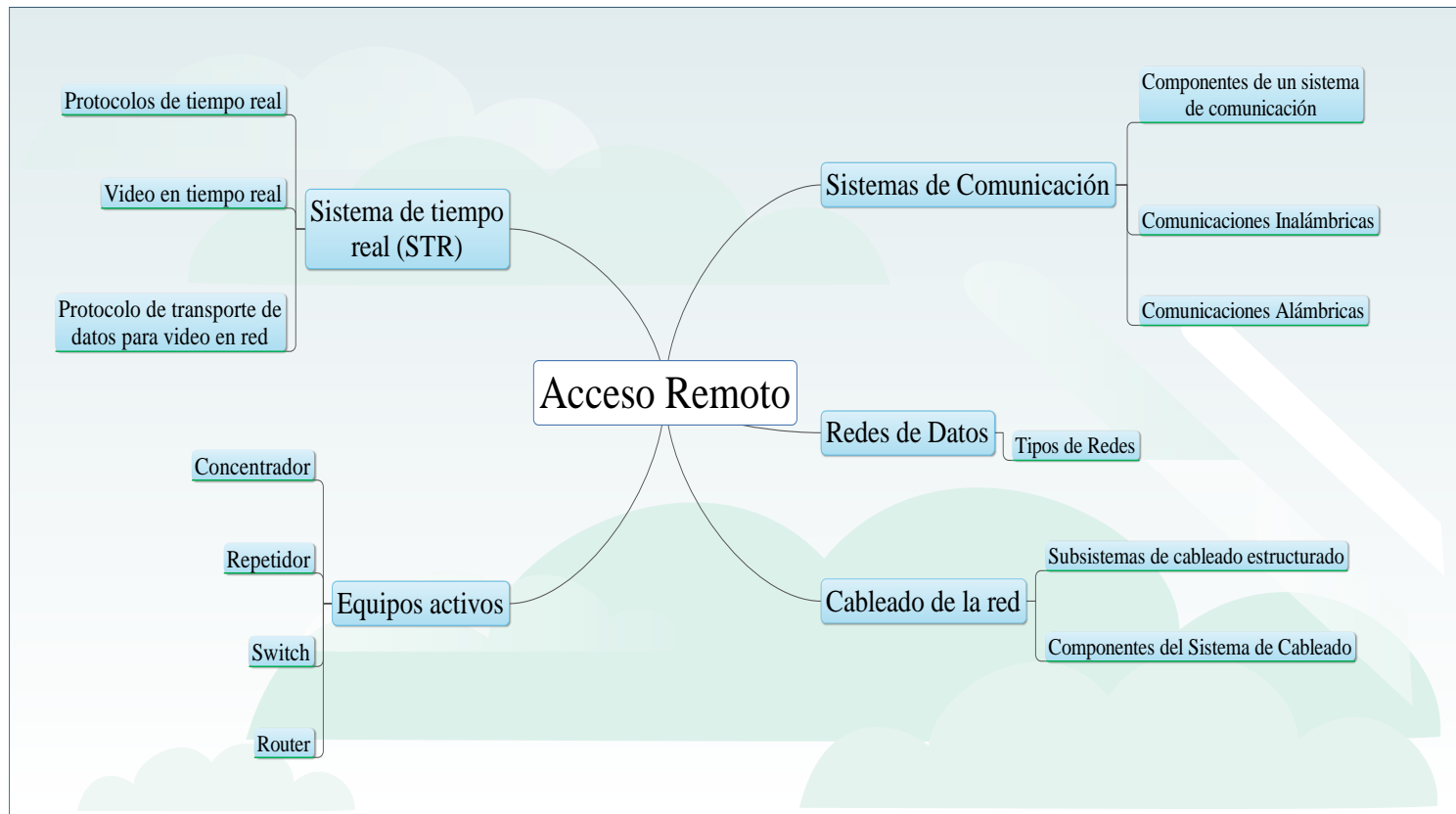


Figura N° 2.3 Constelación de ideas de la variable dependiente

Elaborado por: El Investigador

2.4 CATEGORÍAS FUNDAMENTALES

2.4.1 SISTEMAS DE SEGURIDAD

Un sistema es un conjunto de componentes que actúan simultáneamente para alcanzar un objetivo específico.

El cual consta básicamente de variables que ingresan al mismo, y los productos o respuestas obtenidos.

2.4.1.1 Características de un Sistema de Seguridad

- *Fiabilidad*: asegurar la activación de los dispositivos de prevención.
- *Solidez*: ofrecer resistencia frente a sucesos indebidos.
- *Adaptación*: inmunidad a las posibles condiciones meteorológicas adversas y cambiantes.
- *Sensibilidad*: capacidad para diferenciar el entorno.
- *Disuasión*: persuadir actos ilícitos.
- *Integración*: capacidad de interactuar con otros sistemas.

2.4.1.2 Sistemas de Seguridad Electrónica

Un sistema de seguridad electrónica es la interconexión de recursos, redes y dispositivos, con el fin de precautelar la integridad de las personas y su entorno previniéndolas de peligros y presiones externas. Las principales funciones de un Sistema de Seguridad Electrónica son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico.

a. Clasificación de los sistemas de seguridad electrónica

Se realiza básicamente desde dos criterios, la cantidad de sitios a proteger y la aplicación del sistema.

1. Sistemas Locales de Seguridad Electrónica: Agrupación de elementos y dispositivos electrónicos que interconectados dan seguridad a un sitio.

2. Sistemas Distribuidos de Seguridad electrónica: Un sistema de seguridad electrónica distribuido es un conjunto de sistemas locales de seguridad electrónica, sin embargo estos no funcionan de manera independiente sino que se conectan entre sí permitiendo una mejor gestión en conjunto al manejarse un sistema centralizado, y en ciertos casos incluso manejo de redundancia.

b. Aplicaciones de los sistemas electrónicos de seguridad

Un sistema de seguridad electrónico no tiene límite respecto a sus funciones, y la oferta actual de elementos electrónicos permite que sea adaptable a cualquier medio y necesidad. Ejemplos, de su aplicación:

- Seguridad en la vivienda, establecimientos.
- Seguridad en las cárceles, centrales nucleares.
- Seguridad activa contra incendios, niveles de líquidos, calefacción y cuartos de máquinas. Control de gases, presiones, humedad.

2.4.2 LA EVOLUCIÓN HACIA LA TECNOLOGÍA IP

2.4.2.1 Sistemas tradicionales

Los sistemas tradicionales CCTV requieren una infraestructura separada que utiliza cable coaxial. Este cable fue diseñado para transmisiones punto a punto de video desde una cámara hasta una grabadora en el mismo sitio. El desarrollo de video digital permitió el progreso hacia cables de par trenzado y fibra óptica.

En la figura N° 2.4 se puede apreciar un circuito cerrado de TV que utiliza un VCR (Video Cassette Recorder). Este representa un sistema completamente analógico. El VCR utiliza el mismo tipo de cintas que una grabadora doméstica. El vídeo no se comprime y, si se graba a una velocidad de imagen completa, una cinta durará como máximo 8 horas. En sistemas mayores, se puede conectar un multiplexor entre la cámara y el VCR. El multiplexor permite grabar el vídeo procedente de varias cámaras

en un solo grabador, pero con el inconveniente que tiene una menor velocidad de imagen. Para monitorizar el vídeo, es necesario un monitor analógico.

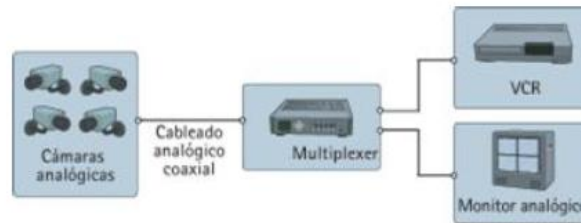


Figura N° 2. 4 Circuito cerrado de TV analógico usando VCR.

Fuente:http://www.axis.com/products/video/camera/about_cameras/overview.htm

2.4.2.2 Seguridad y vigilancia IP

Los sistemas de video-vigilancia IP se basan en la tecnología Internet, con cámaras conectadas en red que emiten información digitalizada. Está demostrado que mejoran los resultados de las convencionales instalaciones de Circuito Cerrado de Televisión, en sencillez y prestaciones. Al ir conectados a Ethernet, las cámaras y servidores de vídeo digitales IP no precisan de ningún otro elemento o software para funcionar y tienen gran capacidad de procesamiento que les permite una toma de decisiones rápida y certera.

La convergencia de voz, vídeo y datos sobre la que se asienta esta nueva tecnología está abriendo la video-vigilancia a nuevos campos de exploración y producción integrados con la inteligencia de negocio en áreas como ventas y marketing. Optimiza las inversiones en infraestructuras de red y aporta un modelo de seguridad más simple, refinado y accesible a los usuarios a través de la empresa. En muchos casos resulta además económicamente más rentable en términos de costes que un sistema de video-vigilancia convencional con cámaras analógicas y grabadoras de vídeo digitales.

Un sistema de video-vigilancia consiste en una comunicación mediante video, con un sitio remoto a través de internet. El esquema de la figura

Nº2.5 muestra a un supervisor que establece video-vigilancia desde la ubicación B, C o D con la ubicación A en donde se lleva a cabo un proceso.

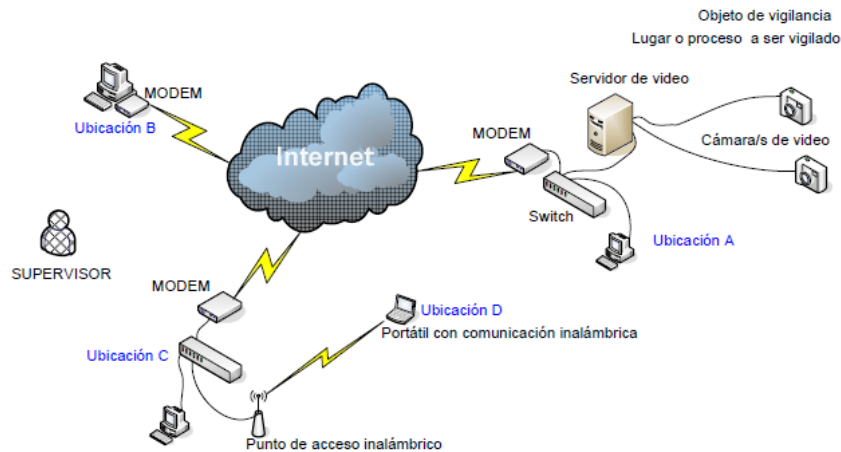


Figura N° 2. 5 Esquema del sistema de video-vigilancia
Fuente: <http://www.alu.ua.es/s/smm47/desc/Especificacion.pdf>

2.4.3 TECNOLOGÍA IP

“Las redes IP son las redes de conmutación por excelencia.”¹ En la cual los datos se dividen en bloques conocidos como paquetes o datagramas para ser enviados y al llegar a su destino son reensamblados a su formato original.

El protocolo IP provee un servicio no orientado a conexión, también llamado del “mejor esfuerzo”. IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

¹ ROLDÁN, David. *Comunicaciones Inalámbricas: Un Enfoque Aplicado*. Primera Edición. Alfaomega Grupo Editor. México, Mayo 2005.

Hay entornos que, por sus especiales características, requieren adoptar una solución híbrida mientras se evoluciona hacia una configuración todo IP en función de las necesidades de la organización, algo que hoy los sistemas de seguridad de vídeo avanzados hacen posible.

2.4.3.1 Direccionamiento IP

El direccionamiento permite determinar el origen y destino de los datos enviados en una red identificando a cada uno de los dispositivos que intervienen en ella. Actualmente existen dos versiones IP:

a. IPv4

Asigna a los equipos un identificador de 4 bytes denominada dirección IP. Es la versión más ampliamente utilizada con direcciones de 32 bits y su notación consta de cuatro números decimales de 8 bits separados por puntos. IPv4 diferencia básicamente 3 tipos de direcciones.

1. Direcciones Públicas: son aquellas que son enrutables hacia internet, es decir aquellas con las cuales podemos tener acceso a internet.
2. Direcciones Privadas: son aquellas que no podemos usar para enrutar hacia internet. Son direcciones útiles para ser usadas en redes locales en entornos domésticos o corporativos.

Hay mecanismos que permiten traducir direcciones privadas en públicas y a la inversa. Esto se conoce como NAT.

Los siguientes rangos de direcciones están reservados para su uso privado (RFC 1918):

Rango de 10.0.0.0 a 10.255.255.255

Rango de 172.16.0.0 a 172.31.255.255

Rango de 192.168.0.0 a 192.168.255.255

3. Direcciones Reservadas: Las direcciones reservadas son grupos de direcciones que han quedado para un uso específico. Las más importantes son las siguientes:

0.0.0.0 Esta es la dirección para referirse a la red.

255.255.255.255 Esta es la dirección de broadcast.

127.X.X.X Este es el rango de ip's de loopback. También llamadas de diagnóstico, 127.0.0.1 es la más usada para referirnos a nuestra máquina de manera local.

b. IPv6

Expansión del espacio de direcciones a 128 bits. Desaparecen los problemas de direccionamiento del **IPv4** actual.

- No son necesarias técnicas como el **NAT** para proporcionar conectividad a todos los ordenadores/dispositivos de nuestra red. Por tanto, todos los dispositivos actuales o futuros podrán tener conectividad completa a Internet.

2.4.4 CÁMARA DIGITAL

Una cámara de red, también llamada cámara IP, puede describirse como una cámara y un ordenador combinados para formar una única unidad.

Además de capturar video, las cámaras de red ofrecen gestión de eventos y funciones de video inteligente, como detección de movimiento, detección de audio, alarma antimanipulación activa y auto seguimiento. La mayoría también disponen de puertos de entrada/salida que habilitan las conexiones con dispositivos externos como sensores y relés. Asimismo pueden incluir prestaciones como funciones de audio y soporte integrado para alimentación por Ethernet (PoE). En la figura N° 2.6 podemos apreciar una cámara de red conectada de manera directa a la Red de Área Local.

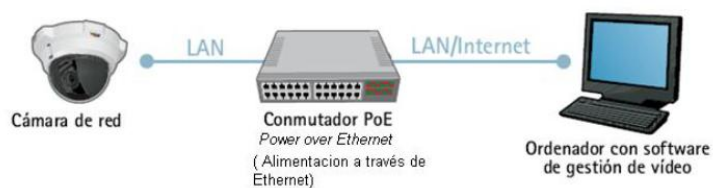


Figura N° 2. 6 Cámara de red conectada directamente a la red LAN
Fuente:http://www.axis.com/products/video/camera/about_cameras/overview.html

2.4.4.1 Componentes que constituyen una cámara IP

a. Partes:

- *Cámara de Video:* En esta sección se encuentran elementos tales como: lentes, sensores y el procesador digital de imagen. Inicialmente el lente de la cámara enfoca la imagen, la misma que pasa a través del filtro óptico, el cual remueve luz infrarroja para que los colores sean mostrados correctamente y finalmente el sensor de imagen transforma las ondas de luz en señales eléctricas, para posteriormente ser convertido a señales digitales.
- *Sistema de Compresión de imagen:* Su principal función es comprimir las imágenes captadas por la cámara en formatos que contengan menos datos y pueden ser transmitidos por la red en forma eficiente, estos formatos son el JPEG, MPEG, MPEG4, entre otros.
- *Sistema de Procesamiento:* El sistema de procesamiento se encarga de la gestión de imágenes, del movimiento de la cámara y de la detección del movimiento. Este sistema está formado por Procesadores, Memoria Flash, software de administración y un módulo Ethernet/WiFi que permiten manejar las aplicaciones de red.

En la figura N° 2.7, se indican los componentes internos de una cámara IP.

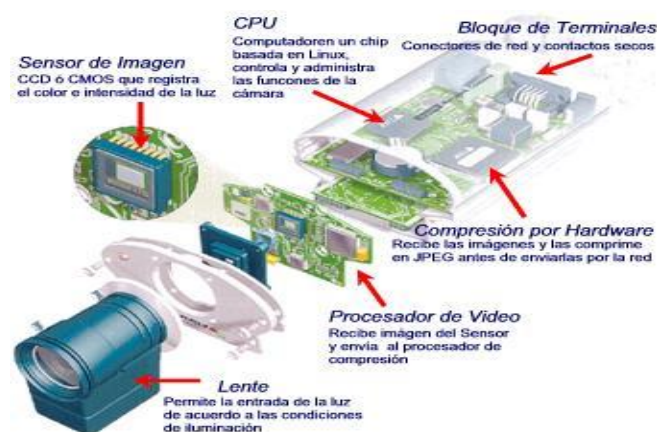


Figura N° 2. 7 Componentes internos de una cámara IP

Fuente: <http://www.gscssoftware.com/teccamaraip>.

b. Medios ópticos:

- *Distancia focal:* es la distancia en milímetros del lente a la superficie del sensor de imagen, cuanto menor sea la distancia más ancho será el ángulo de visión y cuanto mayor sea la distancia, más estrecho será el ángulo de visión.
- *Iris:* controla la cantidad de luz que alcanza al sensor de imagen, de acuerdo a la su apertura.
- *Objetivos:* son aditamentos ópticos que permiten enfocar de mejor manera la imagen en el sensor. Normalmente los objetivos son activos, es decir poseen un sistema de control automático del iris. El objetivo fijo mantiene la distancia focal; el objetivo varifocal permite variar manualmente la distancia focal; el objetivo zoom motorizado varía la distancia focal mediante un sistema automático, acercándonos o alejándonos convenientemente del objeto a captar.

c. Elementos:

- *Sensibilidad lumínica:* Por sensibilidad lumínica o iluminación mínima se entiende el nivel mínimo de iluminación necesario para que una cámara de red produzca una imagen aceptable. La iluminación mínima se indica en lux (lx), que es una medida de iluminancia.
- *Campo de visión:* es el área de cobertura y el grado de detalle que se visualizará. El campo de visión viene determinado por la longitud focal del objetivo y el tamaño del sensor de imagen. La longitud focal del objetivo se define como la distancia entre el objetivo de entrada y el punto en el que convergen todos los rayos de luz hacia un punto (normalmente el sensor de imagen de la cámara). Cuanto mayor es la longitud focal, más estrecho es el campo de visión.
- *Número F y exposición:* Un número f también conocido como f-stop, define la cantidad de luz que puede atravesar un objetivo.

Cuanto menor sea f , mejor será la capacidad de recogida de luz del objetivo, es decir, podrá pasar más luz por el objetivo hasta el sensor de imagen.

- *Sensores de imagen:* El sensor de imagen es un dispositivo que transforma la energía lumínica (fotones) en energía eléctrica (electrones), consiste en una superficie sensible a la luz formando una matriz de puntos, cada punto aporta en la formación de la imagen. Cuando se fabrica una cámara, existen dos tecnologías principales que pueden utilizarse para el sensor de imagen:

Los sensores CCD por regla general, ofrecen una sensibilidad lumínica ligeramente superior y producen menos ruido que los sensores CMOS. Esta mayor sensibilidad lumínica se traduce en mejores imágenes en condiciones de poca luz. Sin embargo, los sensores CCD son más caros y más complejos de incorporar a una cámara.

Los recientes avances en los sensores CMOS los están acercando a sus homólogos CCD en términos de calidad de la imagen. Los sensores CMOS reducen el coste total de las cámaras ya que contienen todas las funciones lógicas necesarias para fabricar cámaras para ellos. En comparación con los sensores CCD, los sensores CMOS permiten mayores posibilidades de integración y más funciones. En la figura N° 2.8 se pueden apreciar los dos tipos de sensores de imagen.

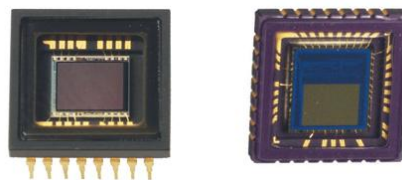


Figura N° 2. 8 Sensores de imagen: CCD (a la izquierda); CMOS (a la derecha).

Fuente:http://www.axis.com/es/products/video/about_networkvideo/image_sensors.htm

2.4.4.2 Tipos de cámaras de red

Las cámaras de red se pueden clasificar en función de si están diseñadas únicamente para su uso en interiores y exteriores, en cuanto a su posición y a su capacidad de visión diurna/nocturna. Las cámaras de red para exteriores suelen tener un objetivo con iris automático para regular la cantidad de luz a la que se expone el sensor de imagen. Una cámara de exteriores también necesitará una carcasa de protección externa, salvo que su diseño ya incorpore un cerramiento de protección. Las carcasas también están disponibles para cámaras para interiores que requieren protección frente a entornos adversos, como polvo y humedad, y frente a riesgo de vandalismo o manipulación.

Se encuentran disponibles diversas variaciones de los tipos de cámaras, entre las que se incluyen:

- Versiones a prueba de agresiones, en función de la carcasa de protección que se use.
- Versiones resistentes a las condiciones climáticas, en función de la carcasa de protección que se use.
- Versiones de visión diurna / nocturna, lo que significa que la cámara puede cambiar automática o manualmente entre modo diurno con vídeo en color y modo nocturno con imágenes en blanco y negro en situaciones de poca luz que pueden mejorarse usando iluminadores de infrarrojos.

Las cámaras de red, pueden clasificarse en:

a. Cámaras Fijas

1. Cámara Fija: Las cámaras fijas formadas por un cuerpo y un objetivo representan el tipo de cámara tradicional. En algunas aplicaciones, resulta sumamente útil que la cámara sea muy visible. Si éste es el caso, una cámara fija representa la mejor elección, puesto que la

cámara es claramente visible al igual que la dirección hacia la cual apunta. En la figura N° 2.9, se observa una cámara fija IP.



Figura N° 2. 9 Cámara fija IP.

Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm

2. Cámara domo fija: Las cámaras domo fijas, también conocidas como mini domo, constan básicamente de una cámara fija preinstalada en una pequeña carcasa domo. La cámara puede enfocar fácilmente el punto seleccionado en cualquier dirección. La ventaja principal radica en su discreto y disimulado diseño, así como en la dificultad de ver hacia qué dirección apunta la cámara. Una de las limitaciones es que las cámaras domo fijas casi nunca disponen de objetivos intercambiables, y en caso de que ofrezcan una selección de objetivos, las posibilidades de intercambiarse se ven limitadas por el espacio en el interior de la carcasa domo. En la figura N° 2.10, se observa una cámara domo fija IP.



Figura N° 2. 10 Cámara domo fija IP.

Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm

b. Cámaras con movimiento

Hasta este momento las cámaras mencionadas han sido fijas con lentes de longitud focal determinada. En muchas aplicaciones el área a cubrir pudiera necesitar muchas cámaras fijas. La solución para esto es la aplicación de cámaras montadas en una plataforma móvil.

Esta plataforma puede ser controlada desde un lugar remoto. En forma alternativa, la plataforma puede ser controlada tanto en el plano horizontal o vertical y es conocida generalmente como una unidad Pan Tilt.

1. Cámaras PTZ: Las cámaras con movimiento vertical/horizontal/zoom (PTZ) poseen la ventaja de obtener una visión panorámica, inclinada, alejada o de cerca de una imagen, manual o automáticamente. Para un funcionamiento manual, la cámara PTZ puede, por ejemplo, utilizarse para seguir los movimientos de una persona. Las cámaras PTZ se utilizan principalmente en interiores y en aquellos lugares donde resulte apropiado ver la dirección hacia la cual apunta la cámara. La mayoría de cámaras PTZ no disponen de un movimiento horizontal completo de 360 grados, y tampoco están hechas para un funcionamiento automático continuo, conocido como “recorrido protegido”. El zoom óptico oscila entre 18x y 26x. En la figura N° 2.11, se observa una cámara PTZ IP.



Figura N° 2. 11 Cámara PTZ IP

Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm

2. Cámaras domo PTZ: Una cámara domo, en comparación con una cámara PTZ, añade la ventaja de permitir una rotación de 360 grados. Asimismo ofrece la resistencia mecánica para un funcionamiento continuo en recorridos protegidos donde la cámara se desplaza de forma continua entre por ejemplo unas 10 posiciones predefinidas, un día tras otro. Con recorridos protegidos, una cámara puede abarcar una zona donde se precisarían 10 cámaras fijas para llevar a cabo el mismo

trabajo. La principal desventaja es que sólo se puede supervisar una ubicación en un momento dado, dejando así las otras 9 posiciones sin supervisar. El zoom óptico oscila, normalmente, entre 18x y 30x. Sin embargo, para instalaciones en el exterior, los factores de zoom superiores a 20x resultan inadecuados debido a las vibraciones y movimientos causados por el viento. En la figura N° 2.12, se observa una cámara domo PTZ IP.



Figura N° 2. 12 Cámara domo PTZ IP.

Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm

3. Cámaras PTZ no mecánicas: Gracias al sensor de megapíxels, la cámara puede abarcar entre 140 y 360 grados y el usuario puede obtener una visión panorámica, inclinada, alejada o de cerca con la cámara, en cualquier dirección, sin tener que realizar ningún movimiento mecánico. La ventaja primordial es que no se produce un desgaste de las piezas móviles. Ofrece además un movimiento inmediato a una nueva posición, lo que en una cámara PTZ tradicional puede tardar hasta 1 segundo. En la actualidad, las mejores cámaras PTZ no mecánicas utilizan un sensor de 3 megapíxels. Con el fin de garantizar una buena calidad de imagen, el movimiento vertical y horizontal deberá limitarse a 140 grados y el zoom a 3x. Para un zoom o una cobertura mayor, la calidad de la imagen se verá seriamente perjudicada.

Una cámara PTZ no mecánica resulta ideal para instalaciones discretas montadas en la pared. . En la figura N° 2.13, se observa una cámara PTZ IP no mecánica.



Figura N° 2. 13 Cámara PTZ IP no mecánica.

Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm

4. Cámaras PTZ mecánicas: Las cámaras de red PTZ mecánicas se utilizan principalmente en interiores y en aplicaciones donde se emplea un operador. El zoom óptico en cámaras PTZ varía normalmente entre 10x y 26x. Una cámara PTZ puede instalarse en el techo o en la pared. En la figura N° 2.14, se observa una cámara PTZ IP mecánica.



Figura N° 2. 14 Cámara PTZ IP mecánica.

Fuente: http://www.axis.com/es/products/video/camera/about_cameras/types.htm

c. Cámaras de red con visión diurna/nocturna

Las cámaras de red a color con visión diurna y nocturna proporcionan imágenes a color a lo largo del día. Cuando la luz disminuye bajo un nivel determinado, la cámara puede cambiar automáticamente al modo nocturno para utilizar la luz prácticamente infrarroja (IR) para proporcionar imágenes de alta calidad en blanco y negro.

La luz casi-infrarroja, que implica desde 700 nanómetros (nm) hasta cerca de 1.000 nm, está más allá de la visión humana, pero la mayoría de los sensores de cámara pueden detectarla y utilizarla. Durante el día, la cámara de visión diurna y nocturna utiliza un filtro de paso IR. La luz

de paso IR se filtra de modo que no distorsiona los colores de las imágenes en el momento en que el ojo humano las ve. Cuando la cámara está en modo nocturno (blanco y negro), el filtro de paso IR se elimina, lo que permite que la sensibilidad lumínica de la cámara alcance los 0,001 lux o un nivel inferior.

El gráfico N° 2.15 muestra cómo un sensor de imagen responde a la luz infrarroja visible y a la luz próxima al espectro infrarrojo. La luz próxima al espectro infrarrojo extiende el intervalo de 700 nm hasta 1.000 nm.

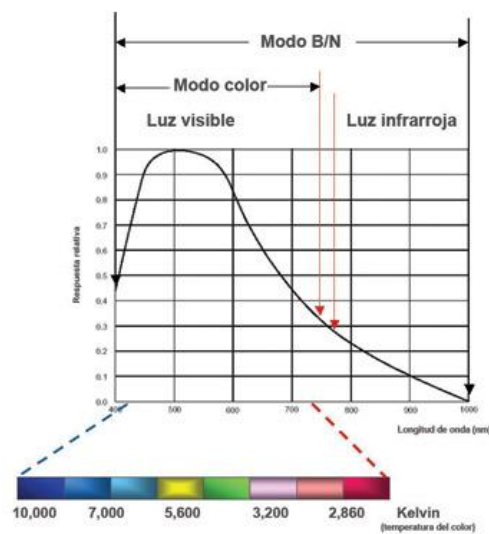


Figura N° 2. 15 Respuesta de un sensor de imagen a la luz

Fuente: http://www.axis.com/es/products/video/camera/about_cameras/day_night.htm

2.4.4.3 Administración de cámaras

Las cámaras IP se conectan directamente a la conexión LAN de la instalación de internet o red doméstica u oficina a través de un router, asignándole una dirección IP interna. Cada una de las cámaras envían la información por medio del servicio de banda ancha y se accede remotamente a él a través de cualquier PC conectada a internet con sólo teclear en el navegador la dirección IP de la cámara que se quiere observar.

2.4.4.4 Resolución de imagen

La resolución de las imágenes digitales se mide en píxeles. La imagen más detallada es la que tiene más datos y por tanto mayor número de píxeles. Las imágenes con más detalles ocupan más espacio en los discos duros y precisan mayor ancho de banda para su transmisión.

a. Resoluciones NTSC y PAL

Las resoluciones NTSC (National Television System Comité: Comité Nacional de Sistemas de Televisión) y PAL (Phase Alternating Line: Línea de Alternancia de Fase) son estándares de vídeo analógico. Son relevantes para el vídeo en red, ya que los codificadores de vídeo proporcionan dichas resoluciones al digitalizar señales de cámaras analógicas. Las cámaras de red actuales también ofrecen resoluciones NTSC y PAL. Ambos estándares proceden de la industria de la televisión. Como se observa en la figura N° 2.16, el NTSC tiene una resolución de 480 líneas y utiliza una frecuencia de actualización de 60 campos entrelazados por segundo (o 30 imágenes completas por segundo). El PAL tiene una resolución de 576 líneas y utiliza una frecuencia de actualización de 50 campos entrelazados por segundo (o 25 imágenes completas por segundo).

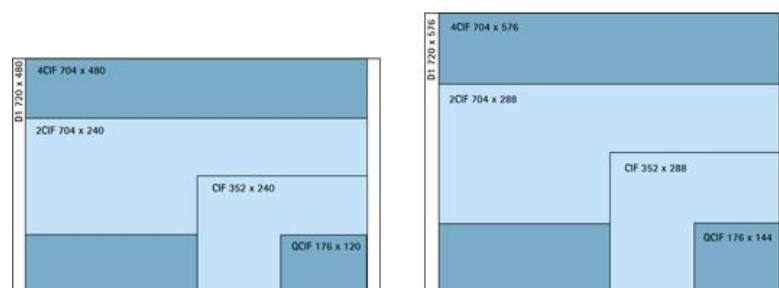


Figura N° 2. 16 A la izquierda, diferentes resoluciones de imagen NTSC. A la derecha, diferentes resoluciones de imagen PAL

Fuente: http://www.axis.com/es/products/video/about_networkvideo/resolution.htm

b. Resoluciones VGA

Con los sistemas 100% digitales basados en cámaras de red se pueden proporcionar resoluciones derivadas de la industria informática y normalizada en todo el mundo, de modo que la flexibilidad es mayor. VGA (Tabla de Gráficos de Vídeo) es un sistema de pantalla de gráficos para PC desarrollado originalmente por IBM. Esta resolución es de 640 x 480 píxeles, un formato habitual en las cámaras de red que no disponen de megapíxeles. La resolución VGA suele ser más adecuada para cámaras de red, ya que el vídeo basado en VGA produce píxeles cuadrados que coinciden con los de las pantallas de ordenador. Los monitores de ordenador manejan resoluciones en VGA o múltiplos de VGA como se indica la tabla N° 2.1.

Formato de visualización	Píxeles
QVGA (SIF)	320x240
VGA	640x480
SVGA	800x600
XVGA	1024x768
4x VGA	1280x960

Tabla N° 2. 1 Resoluciones VGA

Fuente: http://www.axis.com/es/products/video/about_networkvideo/resolution.htm

c. Resoluciones megapíxel

Una cámara de red que ofrece una resolución megapíxel utiliza un sensor megapíxel para proporcionar una imagen que contiene un millón de megapíxeles o más. Cuántos más píxeles tenga el sensor, mayor potencial tendrá para captar más detalles y ofrecer una calidad de imagen mayor. Con las cámaras de red megapíxel los usuarios pueden obtener más detalles, ideal para la identificación de personas y objetos o para visualizar un área mayor del escenario. Esta ventaja supone una importante consideración en aplicaciones de video-vigilancia.

Formato de visualización	Nº de megapíxeles	Píxeles
SXGA	1.3 megapíxeles	1280x1024
SXGA+(EXGA)	1.4 megapíxeles	1400x1050
UXGA	1.9 megapíxeles	1600x1200
WUXGA	2.3 megapíxeles	1920x1200
QXGA	3.1 megapíxeles	2048x1536
WQXGA	4.1 megapíxeles	2560x1600
QSXGA	5.2 megapíxeles	2560x2048

Tabla N° 2. 2 Formatos megapíxel

Fuente: http://www.axis.com/es/products/video/about_networkvideo/resolution.htm

La resolución megapíxel es un área en la que las cámaras de red se distinguen de las analógicas. La resolución máxima que puede proporcionar una cámara analógica convencional tras haber digitalizado la señal de vídeo en una grabadora o codificador de vídeo es D1, es decir, 720 x 480 píxeles (NTSC) o 720 x 576 píxeles (PAL). La resolución D1 corresponde a un máximo de 414.720 píxeles ó 0,4 megapíxeles. En comparación, un formato megapíxel común de 1280 x 1024 píxeles consigue una resolución de 1,3 megapíxeles, tal como se indica en la tabla N° 2.2. Esto es más del triple de la resolución que pueden proporcionar las cámaras analógicas de CCTV.

d. Resoluciones de televisión de alta definición (HDTV)

La HDTV proporciona una resolución hasta cinco veces más alta que la televisión analógica estándar.. Las dos normas HDTV más importantes, definidas por la SMPTE (Society of Motion Picture and Television Engineers - Sociedad de ingenieros de cine y televisión), son la SMPTE 296M y la SMPTE 274M.

- La norma **SMPTE 296M (HDTV 720P)** define una resolución de 1280 x 720 píxeles con una alta fidelidad de color y utiliza el barrido progresivo a 25/30 hercios (Hz) (que corresponde a 25 ó 30 imágenes por segundo, en función del país) y 50/60 Hz (50/60 imágenes por segundo).

- La norma **SMPTE 274M (HDTV 1080)** define una resolución de 1920 x 1080 píxeles con una alta fidelidad de color y utiliza el barrido entrelazado o progresivo a 25/30 Hz y 50/60 Hz.

2.4.4.5 Digitalización de imagen

Digitalizar un video es transformar las imágenes y audio a lenguaje de máquina o formato binario como una secuencia de fotos con sonido en pistas separadas que se mueven en función del tiempo y que al pasar rápido por nuestros ojos se crea la ilusión de imágenes en movimiento.

El proceso de digitalización de imágenes va directamente ligado al uso que se le dará al resultado de la digitalización. La decisión inicial acerca de la digitalización de una imagen es si hacerla a color o sólo en blanco y negro, así como la resolución, que determina el número de puntos por pulgada lineal (dpi) que recorrerá el escáner y la cantidad de información que cada punto deberá contener. A mayor resolución y números de bits por pixel se obtendrá un mayor tamaño del archivo pero una imagen más definida.

2.4.4.6 Códec

El nombre códec viene de la abreviatura de codificador – decodificador. Así un códec es un software, hardware o una combinación de ambos, capaz por una parte de codificar una señal o información con el fin de encriptarla, transmitirla o almacenarla, y por otra decodificarla para su visualización o edición. En los procesos de codificación y decodificación el códec se sirve de unos mecanismos denominados algoritmos de codificación.

En la actualidad los códecs más utilizados en video-vigilancia IP corresponden a la categoría de vídeo códecs H.264, MPEG 4, aunque podemos encontrar casos en los que se utilizan códecs orientados a fotografía (JPEG) para comprimir el vídeo capturado por las cámaras de vigilancia.

2.4.4.7 Compresión

La compresión es un caso particular de codificación, cuya característica principal es que el código resultante tiene menor tamaño que el original.

En la figura N° 2.17 se indica el algoritmo de compresión, el cual toma una entrada X y genera una representación X_c , que necesita menos bits, el algoritmo de reconstrucción toma X_c y genera la señal original X .

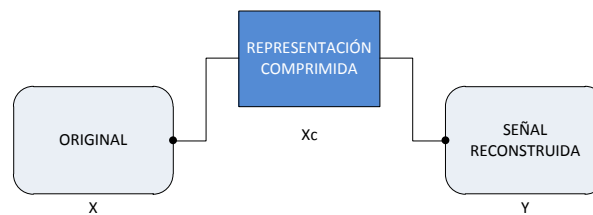


Figura N° 2. 17 Esquema básico de compresión y descompresión
Elaborado por: El investigador

Mediante este procedimiento se retira la redundancia de datos que existe en la captura progresiva de imágenes, quita la información que no es útil para el humano sin desmejorar la imagen. El formato de compresión puede ser propietario pero la mayoría de cámaras usan estándares como MPEG4, Wavelet ó H.264, entre otros.

Los diferentes estándares de compresión utilizan métodos distintos para reducir los datos y, en consecuencia, los resultados en cuanto a frecuencia de bits y latencia son diferentes. Existen dos tipos de algoritmos de compresión:

- *La compresión de imagen* utiliza la tecnología de codificación intrafotograma. Los datos se reducen a un fotograma de imagen con el fin de eliminar la información innecesaria que puede ser imperceptible para el ojo humano. Motion JPEG es un ejemplo de este tipo de estándar de compresión.

En la figura N° 2.18, las tres imágenes de la secuencia se codifican y se envían como imágenes únicas y separadas (fotogramas I), sin que dependan unas de otras.



Figura N° 2. 18 Esquema básico de compresión y descompresión
Fuente: http://www.axis.com/es/products/video/about_networkvideo/compression.htm

- *Los algoritmos de compresión de vídeo como el MPEG-4 y el H.264 utilizan la predicción interfotograma para reducir los datos de vídeo entre las series de fotogramas. Ésta consiste en técnicas como la codificación diferencial, en la que un fotograma se compara con un fotograma de referencia y sólo se codifican los píxeles que han cambiado con respecto al fotograma de referencia. De esta forma, se reduce el número de valores de píxeles codificados y enviados. Cuando se visualiza una secuencia codificada de este modo, las imágenes aparecen como en la secuencia de vídeo original.*

Como se observa en la figura N° 2.19 Con la codificación diferencial sólo la primera imagen (fotograma I) se codifica en su totalidad. En las dos imágenes siguientes (fotogramas P) existen referencias a la primera imagen en lo que se refiere a elementos estáticos, como la casa. Sólo se codifican las partes en movimiento (el hombre que corre) mediante vectores de movimiento, reduciendo así la cantidad de información que se envía y almacena

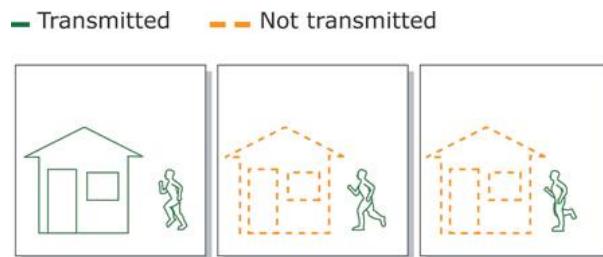


Figura N° 2. 19 Codificación diferencial
Fuente: http://www.axis.com/es/products/video/about_networkvideo/compression.htm

Los Formatos de compresión de video mas utilizados son:

a. Motion JPEG

Motion JPEG o M-JPEG es una secuencia de vídeo digital compuesta por una serie de imágenes JPEG individuales. (JPEG son las siglas de Joint Photographic Experts Group - Grupo de Expertos Fotográficos Unidos). Un vídeo en completo movimiento se percibe a 30 (NTSC) ó 25 (PAL) imágenes por segundo. En una secuencia Motion JPEG, las imágenes se codifican o comprimen como imágenes JPEG individuales. Una de las ventajas de Motion JPEG es que cada imagen de una secuencia de vídeo puede conservar la misma calidad garantizada que se determina mediante el nivel de compresión elegido para la cámara de red o codificador de vídeo. Motion JPEG es un estándar que no requiere licencia. Tiene una amplia compatibilidad y su uso es muy habitual en aplicaciones donde se requieren fotogramas individuales en una secuencia de vídeo y donde se utiliza una frecuencia de imagen de 5 fotogramas por segundo o inferior.

b. MPEG-4

Cuando se menciona MPEG-4 en las aplicaciones de videovigilancia, normalmente nos referimos a MPEG-4 Parte 2, también conocido como MPEG-4 Visual. Como todos los estándares MPEG (Moving Picture Experts Group), requiere una licencia, es decir, los usuarios deben pagar una tasa de licencia por cada estación de supervisión. MPEG-4 es compatible con aplicaciones de ancho de banda reducido y aplicaciones que requieren imágenes de alta calidad, sin limitaciones de frecuencia de imagen y con un ancho de banda virtualmente ilimitado.

c. H.264 o MPEG-4 Part 10/AVC

El H.264, también conocido como MPEG-4 Parte 10/AVC para Codificación de Vídeo Avanzada, es el estándar MPEG más actual para la codificación de vídeo. Sin comprometer la calidad de la imagen, un

codificador H.264 puede reducir el tamaño de un archivo de vídeo digital en más de un 80% si se compara con el formato Motion JPEG, y hasta un 50% más en comparación con el estándar MPEG-4. Esto significa que se requiere menos ancho de banda y espacio de almacenamiento para los archivos de vídeo.

H.264 encuentra su mayor utilidad en aplicaciones donde se necesiten velocidades y resoluciones altas, como en la vigilancia de autopistas, aeropuertos y casinos, lugares donde por regla general se usa una velocidad de 30/25 (NTSC/PAL) imágenes por segundo. Es aquí donde las ventajas económicas de un ancho de banda y un almacenamiento reducidos se harán sentir de forma más clara.

Con el MPEG-4 y el H.264, los usuarios pueden determinar que una transmisión de vídeo codificado tenga una frecuencia de bits variable o constante. La selección óptima dependerá de la aplicación y de la infraestructura de red.

El gráfico N° 2.20 compara la frecuencia de bits, partiendo de la misma calidad de imagen, entre los siguientes estándares de vídeo: Motion JPEG, MPEG-4 Parte 2 (sin compensación de movimiento), MPEG-4 Parte 2 (con compensación de movimiento) y H.264 (perfil de base). El codificador H.264 es al menos tres veces más eficaz que un codificador MPEG-4 sin compensación de movimiento y al menos seis veces más eficaz que Motion JPEG.

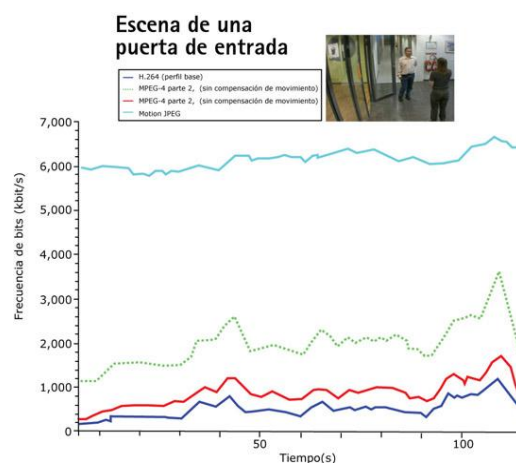


Figura N° 2. 20 Esquema básico de compresión y descompresión

Fuente: http://www.axis.com/es/products/video/about_networkvideo/compression_compare.htm

2.4.5 GRABADORES DE VIDEO USADOS PARA LA VIDEO-VIGILANCIA

Además de visualizar en tiempo real las imágenes que captura una cámara de video-vigilancia, las empresas y organismos de seguridad precisan revisar los videos capturados ya sea para analizar dichas imágenes con fines comerciales, para prevención de riesgo o ante incidencias de seguridad.

2.4.5.1 Digital video Recorder (DVR)

Los DVR son los dispositivos encargados de la grabación de imágenes en una solución de video-vigilancia analógica (CCTV), cada cámara tiene una conexión física (cable coaxial). Una vez definida su ubicación no puede ser trasladada fácilmente a no ser que rediseñemos completamente el cableado de la red CCTV.

Constituye un sistema analógico con grabación digital. En un DVR, la cinta de vídeo se sustituye por discos duros para la grabación de vídeo, y es necesario que el vídeo se digitalice y comprima para almacenar la máxima cantidad de imágenes posible de un día. En la figura N° 2.21 se observa un circuito cerrado de TV analógica usando DVR.

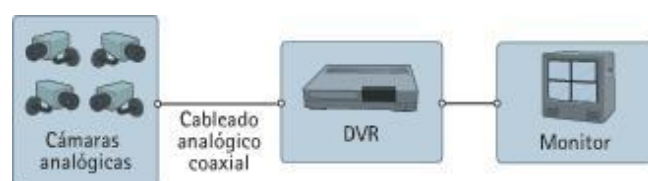


Figura N° 2. 21 Circuito cerrado de TV analógica usando DVR

Fuente: http://www.axis.com/products/video/camera/about_cameras/overview.htm

2.4.5.2 Network video recorder (NVR)

Entre los elementos clave de la video-vigilancia IP se encuentran los NVR's, que permiten la grabación de video en red en formato digital en distintos medios de almacenamiento como discos duros. De forma genérica se puede decir que los NVR's están compuestos por una parte hardware y

otra software. La parte hardware establece la capacidad de proceso, almacenamiento y conectividad con otros dispositivos, mientras que el elemento software otorgará la inteligencia y funcionalidades del NVR.

Un NVR está diseñado para ofrecer un rendimiento óptimo para un conjunto de cámaras y normalmente es menos escalable que un sistema basado en servidor de PC. Esto permite que la unidad resulte más adecuada para sistemas más pequeños donde el número de cámaras se encuentra dentro de los límites de la capacidad de diseño de un NVR.

En la actualidad existen dispositivos denominados NVR's híbridos cuya función es grabar en un mismo dispositivo las imágenes procedentes tanto de cámaras IP digitales como de cámaras analógicas con el fin de dar servicio desde un único equipo a instalaciones que requieren mantener simultáneamente soluciones de video-vigilancia IP y CCTV. En la figura N° 2.22 se observa un circuito cerrado de TV analógica usando DVR.

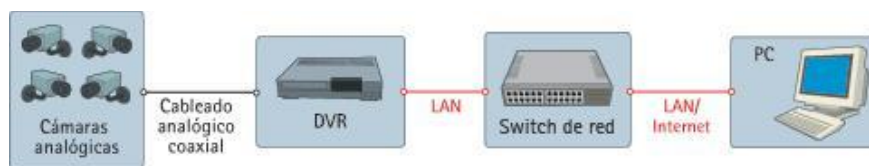


Figura N° 2. 22 Sistema de circuito cerrado de TV analógico usando DVR de red
Fuente: http://www.axis.com/products/video/camera/about_cameras/overview.htm

2.4.6 SISTEMAS DE COMUNICACIÓN

Un sistema de comunicación de datos tiene como objetivo el transmitir información desde una fuente a un destinatario a través de un canal.

2.4.6.1 Componentes de un sistema de comunicación

- *Emisor o transmisor:* debe convertir la señal a un formato que sea reconocible por el canal.
- *Canal:* conecta al emisor y receptor. Puede ser cualquier medio de transmisión.

- *Receptor*: acepta la señal del canal y la procesa para permitir que el usuario final la comprenda.

2.4.6.2 Comunicaciones Inalámbricas

“Es el proceso de comunicar información mediante un soporte electromagnético a través de una cierta distancia, atravesando el espacio libre en lugar de utilizar conductos físicos”²

Esta tecnología facilita el acceso a recursos en lugares donde se imposibilita la utilización de cables, como zonas rurales poco accesibles.

a. Medios no guiados

1. Señales de radio: Son capaces de recorrer grandes distancias, atravesando edificios incluso. Son ondas omnidireccionales: se propagan en todas las direcciones. Su mayor problema son las interferencias entre usuarios.
2. Señales de Microondas: Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente. Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Km de distancia.
3. Señales de Infrarrojo: Son ondas direccionales incapaces de atravesar objetos sólidos, paredes por ejemplo, que están indicadas para transmisiones de corta distancia.

b. Estándar IEEE 802.11

Familia de especificaciones desarrolladas por la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos), constituyéndose en un conjunto de

² NICHOLS, Randall. *Seguridad para Comunicaciones Inalámbricas*. Primera Edición en Español por McGraw-Hill/Interamericana de España 2003.

protocolos de nivel de enlace para redes inalámbricas de área local, que trabaja en las bandas de 2.4 y 5 Ghz.

- *Recomendación original, 1997:* La versión original del estándar IEEE, especifica dos velocidades de transmisión teóricas de 1 y 2 Mbps que se transmiten por señales infrarrojas (IR). Opera en la banda de 2.4 Ghz.
- *IEEE 802.11a, 1999:* opera en la banda de 5 Ghz y utiliza orthogonal frequency-division multiplexing (OFDM) con una velocidad máxima de 54 Mbps.
- *IEEE 802.11b, 1999:* tiene una velocidad máxima de transmisión de 11 Mbps, funciona en la banda de 2,4 GHz y emplea el Espectro ensanchado por secuencia directa (DSSS).
- *IEEE 802.11g, 2003:* es la evolución del estándar 802.11b, Este utiliza la banda de 2,4 Ghz, opera a una velocidad teórica máxima de 54 Mbps. Utiliza OFDM.
- *IEEE 802.11n, 2009:* Alcanza una velocidad teórica de más de 600 Mbps. Utiliza la técnica MIMO (Multiple Input, Multiple Output). Opera en las bandas de frecuencia de 2.4 y 5 Ghz siendo compatibles con todas la versiones anteriores. Actualmente ya existen varios productos que cumplen con un máximo de 300 Mbps.

2.4.6.3 Comunicaciones Alámbricas

Una red alámbrica es un conjunto de equipos conectados por medio de cables, los cuales sirven para el transporte de datos, compartiendo información, recursos, servicios. Proporcionando a los usuarios una adecuada seguridad y la capacidad de mover muchos datos de manera rápida y efectiva.

a. Medios Guiados

1. Par trenzado: En su forma más simple, un cable de par trenzado consta de dos hilos de cobre aislados y entrelazados. El número total de pares que hay en un cable puede variar, su velocidad varía entre 10 y 100 Mbps.

Hay dos tipos de cables de par trenzado:

- *Cable de par trenzado sin apantallar (UTP)*: El cableado UTP, con una terminación de conectores RJ-45, es un medio común basado en cobre para interconectar dispositivos de red como computadoras y dispositivos intermedios como switches. A continuación se mencionan los principales tipos de cables que se obtienen al utilizar convenciones específicas de cableado.

- Cable directo Ethernet
- Cruzado de Ethernet
- Consola

La figura N° 2.23 muestra la aplicación típica de estos cables:

Tipo de cable	Estándar	Aplicación
Cable directo de Ethernet	Un extremo T568A, otro extremo T568B	Conexión de un host de red a un dispositivo de red como un switch o hub.
Cruzado Ethernet	Un extremo T568A, otro extremo T568B	Conexión de dos hosts de red. Conexión de dos dispositivos intermedios de red (switch a switch o router a router).
Transpuesto	Propietario de Cisco	Conecte el puerto serial de una estación de trabajo al puerto de consola de un router utilizando un adaptador.

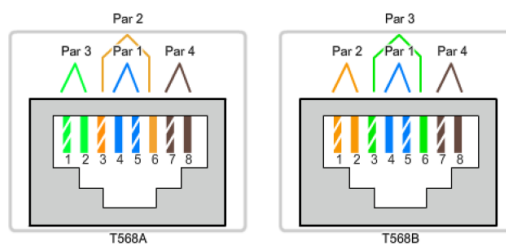


Figura N° 2. 23 Tipos de cables: directo, de conexión cruzada y de consola.

Fuente: Cisco Networking Academy. CCNA Exporation 4.0

- *Cable de par trenzado apantallado (STP)*: Otro tipo de par trenzado utilizado en las redes, utiliza dos pares de alambres que se envuelven en una malla de cobre tejida. Durante muchos años fue la estructura de cableado de uso específico en instalaciones de red Token Ring, con la

disminución del uso de esta red también se redujo la demanda del cable blindado. El nuevo estándar de 10 GB para Ethernet incluye una disposición para el uso del cableado STP.

2. Cable coaxial: El cable coaxial consta de un alambre de cobre en su parte central, el cual se encuentra rodeado por un material aislante. Este material aislante está rodeado por un conductor cilíndrico que frecuentemente se presenta como una malla de tejido trenzado. El conductor externo está cubierto por una capa de plástico protector. Posee gran ancho de banda y una excelente inmunidad al ruido. El ancho de banda que se puede obtener depende de la longitud del cable, es el medio mas frecuente para transportar señales elevadas de radiofrecuencia, especialmente señales de televisión por cable.
3. Fibra óptica: Un cable de fibra óptica consta de tres secciones concéntricas. La más interna, el núcleo, consiste en una o más hebras o fibras hechas de cristal o plástico. Cada una de ellas lleva un revestimiento de cristal o plástico con propiedades ópticas distintas a las del núcleo. La capa más exterior, que recubre una o más fibras, debe ser de un material resistente como el teflón o PVC. Se pueden clasificar los cables de fibra óptica en dos clases:
 - *Monomodo*: Este tipo de fibras necesitan el empleo de emisores láser para la inyección de la luz, lo que proporciona un gran ancho de banda y una baja atenuación con la distancia, por lo que son utilizadas en redes metropolitanas y redes de área extensa.
 - *Multimodo*: Se transmiten varios modos electromagnéticos por la fibra, denominándose por este motivo fibra multimodo. Las fibras multimodo son las más utilizadas en las redes locales por su bajo coste.

2.4.7 REDES DE DATOS

Una red de datos es un sistema que enlaza dos o más puntos por un medio, el cual sirve para enviar o recibir un determinado flujo de información.

2.4.7.1 Tipos de Redes

Según el lugar y el espacio que ocupen, las redes se pueden clasificar en:

- a. **Redes PAN:** Red de administración personal, es la interconexión de dispositivos de tecnología de la información dentro del rango de una persona individual, llega a cubrir un radio de 10 metros por lo habitual y pueden estar conformadas por no más de ocho equipos.
- b. **Redes LAN:** La red de área local, es aquella que se expande en un área relativamente pequeña. Comúnmente se encuentra dentro de un edificio o un conjunto de edificios contiguos.

Las redes de área local proveen una excelente velocidad de transferencia, que va desde los 10 hasta los 1.000 Mbps. Esto se debe a la corta distancia existente entre las computadoras, lo cual evita las interferencias

- c. **Redes MAN:** Red de área metropolitana, se caracterizan por ser redes que se extienden sobre áreas geográficas de tipo urbano, como una ciudad. Son implementadas generalmente por los proveedores de servicio de internet.
- d. **Redes WAN:** Red de área extensa, se caracteriza por tener una muy amplia cobertura por lo general cubre un país o un continente a diferencia de las redes locales, cuya infraestructura es generalmente propiedad y responsabilidad del usuario. Las redes WAN normalmente utilizan redes de proveedores.

2.4.7.2 Cableado de la red

La mayor parte de redes de área local emplean cables como medios de transmisión, debido a su rapidez y a la capacidad de proteger información confidencial.

“Aunque el cableado representa solo una pequeña parte del coste total de una red, tan pequeña como el 6%, se estima que es responsable de hasta el 75% del tiempo sin servicio de red”³ Por tal motivo resulta importante la instalación correcta y la inversión en medios de calidad que permitan obtener una red óptima y duradera.

a. Subsistemas de cableado estructurado

Subsistemas relacionados con el sistema de cableado estructurado:

- *Punto de demarcación*: es donde los cables del proveedor externo de servicios se conectan a los cables del cliente en su edificio.
- *Salas de equipamiento y de telecomunicaciones*: Ubicación de equipamiento de telecomunicaciones, tal como la interfaz entre el cableado horizontal y vertical.

Espacio dedicado para la instalación de los racks de comunicaciones, cuyas características principales se enumeran a continuación:

- Área exclusiva dentro de un edificio para el equipo de telecomunicaciones.
 - Debe proveerse un ambiente controlado.
- *Cableado vertical (Backbone)*: Conecta los armarios de telecomunicaciones, las salas de equipamiento y entrada de un edificio, así como también el cableado de conexión entre edificios.

Infraestructura principal de la red q debe estar lo suficientemente dimensionado para ser capaz de soportar el número máximo de usuarios y aplicaciones simultáneas, por lo que deberá proveer estabilidad frente al crecimiento de las necesidades de los usuarios del sistema.

³ CRAIG ZACKER, *Manual de referencia Redes*. Primera Edición en Español por McGraw-Hill/Interamericana de España

- *Cableado Horizontal:* El cableado horizontal incorpora el sistema de cableado que se extiende desde el área de trabajo de telecomunicaciones hasta el cuarto de telecomunicaciones. Cableado horizontal incluye:
 - Las salidas (cajas/placas/conectores) de telecomunicaciones en el área de trabajo.
 - Cables y conectores de transición instalados entre las salidas del área de trabajo y el cuarto de telecomunicaciones.
 - Paneles de parcheo (patch panels) y cordones de parcheo (patch cables) utilizados para configurar las conexiones de cableado horizontal en el cuarto de telecomunicaciones.

- *Área de trabajo:* se extienden desde la terminación del cableado horizontal en la salida de información, hasta el equipo en el cual se está corriendo una aplicación sea de voz, datos, video o control.

En la figura 2.24 se puede apreciar los subsistemas relacionados con el sistema de cableado estructurado:

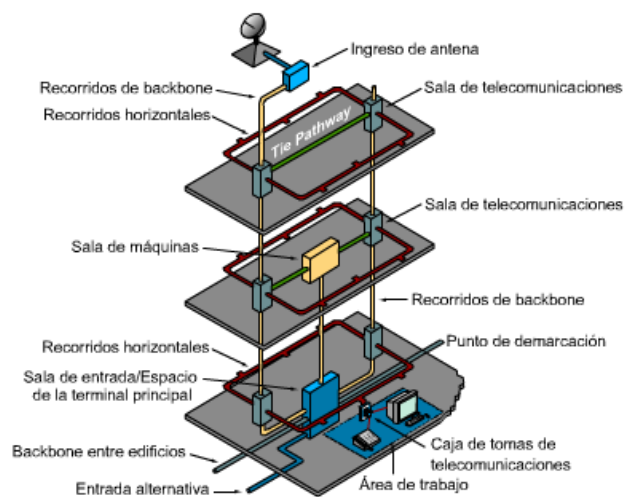


Figura N° 2. 24 Subsistemas de cableado estructurado

Fuente:http://www.esepoch.edu.ec/Descargas/noticias/dacee2_CCNA1_CS_Structured_Cabling_es.pdf.

b. Componentes del Sistema de Cableado

1. Equipo pasivo: Elementos no electrónicos de una red. Por ejemplo: cable, conectores, cordones de parcheo, paneles de parcheo, bastidores.

2. Equipo activo: Los equipos electrónicos. Ejemplos de equipos activos: concentrador, repetidores, switch , router.

- *El concentrador*: Es un elemento de hardware que permite concentrar el tráfico de red que proviene de múltiples hosts y regenerar la señal. Al igual que un repetidor, el concentrador funciona en el nivel 1 del modelo OSI. Es por ello que a veces se lo denomina repetidor multipuertos.
- *Repetidores*: Un repetidor es un dispositivo sencillo utilizado para regenerar una señal entre dos nodos de una red. De esta manera, se extiende el alcance de la red. El repetidor funciona solamente en el nivel físico, es decir que sólo actúa sobre la información binaria que viaja en la línea de transmisión y que no puede interpretar los paquetes de información. Por otra parte, un repetidor puede utilizarse como una interfaz entre dos medios físicos de tipos diferentes, es decir que puede, por ejemplo, conectar un segmento de par trenzado a una línea de fibra óptica.
- *Switch*: Un conmutador o *switch* es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red. Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local
- *Router*: Un router es un dispositivo de interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Cuando un usuario accede a una URL, el cliente web (navegador) consulta al servidor de nombre de dominio, el cual le indica

la dirección IP del equipo deseado. La estación de trabajo envía la solicitud al router más cercano, es decir, a la pasarela predeterminada de la red en la que se encuentra. Este router determinará así el siguiente equipo al que se le enviarán los datos para poder escoger la mejor ruta posible. Para hacerlo, el router cuenta con tablas de enrutamiento actualizadas, que son verdaderos mapas de los itinerarios que pueden seguirse para llegar a la dirección de destino. Existen numerosos protocolos dedicados a esta tarea. Además de su función de enrutar, los routers también se utilizan para manipular los datos que circulan en forma de datagramas, para que puedan pasar de un tipo de red a otra.

2.4.8 SISTEMA DE TIEMPO REAL (STR)

Es aquel sistema digital que interactúa activamente con un entorno físico de dinámica conocida y responde a los estímulos de éste dentro de un plazo de tiempo determinado, por tanto para que el funcionamiento de estos sistemas sea correcto un STR ha de ejecutar secuencialmente una serie de acciones, agrupadas normalmente en tareas, con un tiempo de respuesta determinado que puede, o no, superar el tiempo límite establecido.

Encontramos sistemas de tiempo real en numerosos campos de aplicación: control de electrodomésticos, vehículos, procesos industriales, comunicaciones, etc.

2.4.8.1 Video en tiempo real

Streaming de video, o vídeo en tiempo real, es la tecnología que permite la transmisión y recepción de imágenes y sonidos de manera continua a través de una red. A diferencia de otros formatos de audio y vídeo, en los que es necesario esperar que el archivo sea cargado en el equipo para su visualización, esta tecnología permite apreciar el contenido conforme se va teniendo acceso a la información del archivo.

El servidor de streaming permite visionar el vídeo de forma continua

porque hace uso de un buffer, donde van cargándose algunos segundos de la secuencia antes de que sean mostrados. Entonces cuando se detecta un periodo de congestión de red, se visualizarán los datos que tenemos ya almacenados en el buffer. De esta forma el cliente obtiene los datos tan rápido como el servidor y la red lo permitan.

El streaming puede decirse que funciona de forma inteligente ya que asegura al usuario que recibirá la más alta calidad posible dependiendo de la velocidad de conexión o de los problemas de conexión de la red. Tradicionalmente la congestión de la red forzaba al usuario a detener la visualización del vídeo almacenando en un buffer la información para posteriormente continuar mostrando la secuencia. Con los nuevos formatos de streaming como el MPEG-4, el cliente y el servidor pueden degradar la calidad de forma inteligente para asegurar una reproducción continua del vídeo.

Si se dan problemas de congestión de red, primeramente el servidor de vídeo disminuye el número de fotogramas que está enviando para mantener la calidad del audio e ir llenando el búffer mínimamente. Si las condiciones empeoran, el servidor deja de mandar frames de vídeo, pero mantiene la calidad del audio.

Finalmente, si la calidad del audio empieza a degradarse, el cliente reconstruye de manera inteligente las secuencias que tiene almacenadas para no perder calidad. En la figura N° 2.25, se representa el esquema básico del sistema streaming.

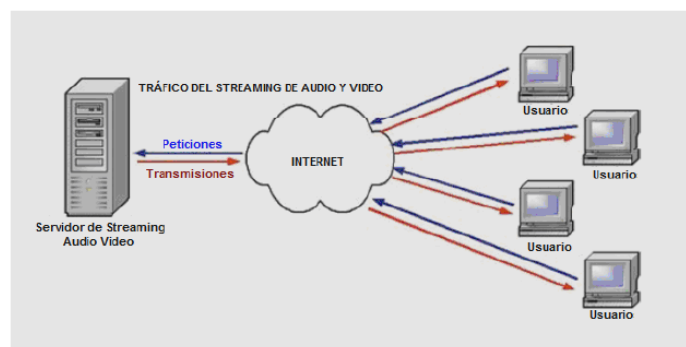


Figura N° 2. 25 Esquema básico del Sistema Streaming.

Fuente:http://www.etsit.ulpgc.es/cat_telefonica/Proyectos_Tesis/PI+D/PI%20I+D.htm

2.4.8.2 Protocolos de tiempo real

- a. **Protocolo RTP:** Protocolo de tiempo real (RTP, Real Time Protocol) proporciona funciones de transporte extremo a extremo, para aplicaciones de transmisión de datos en tiempo real. Trabaja a nivel de aplicación y no garantiza calidad de servicio ni reserva de recursos para los servicios de tiempo real.

El lado emisor en una aplicación multimedia, añade campos de cabecera de audio y video antes de pasarlas a la capa de transporte, dentro del paquete RTP se transporta información de formatos de audio como: PCM, GSM y MP3 y MPEG, H.263 para video, es ampliamente implementado en cientos de productos y prototipos de investigación; SIP y H.323 lo utilizan.

- b. **Protocolo RTCP:** Protocolo de control en tiempo real (RTCP, Real Time Control Protocol) está diseñado para proveer realimentación sobre la calidad de servicio a los participantes de la sesión de la sesión RTP.
- c. **Protocolo RTSP:** Protocolo de streaming en tiempo real (RTSP, Real Time Streaming Protocol), trabaja a nivel de aplicación y controla la de sesión para la realización de streaming de medios sobre Internet. Una de las funciones principales de RTSP es el soporte de funciones como: parada, pausa, resumir, avance rápido y retroceso rápido. RTSP funcionan tanto en difusión punto a punto como en multidifusión, permite controlar múltiples sesiones y escoger protocolos de transporte a utilizar como UDP o TCP.

2.4.8.3 Protocolo de transporte de datos para video en red

El Protocolo de control de transmisión TCP (Transmission Control Protocol-Protocolo de Control de Transmisión) y el UDP (User Datagram Protocol - Protocolo de datagramas de usuario) son los protocolos basados en IP que se utilizan para enviar datos. Estos

protocolos de transporte actúan como portadores para muchos otros protocolos. Por ejemplo, HTTP (Hyper Text Transfer Protocol-protocolo de transferencia de hipertexto), que se utiliza para visualizar páginas web en servidores de todo el mundo a través de Internet. En la tabla N°2.2 se detallan los protocolos y puertos TCP/IP habituales utilizados para el video en red.

Protocolo	Protocolo de transporte	Puerto	Uso habitual	Uso de video en red
FTP (Protocolo de transferencia de ficheros)	TCP	21	Transferencia de archivos a través de Internet/intranets	Transferencia de imágenes o video desde un codificador de video/cámara de red a un servidor FTP o a una aplicación
SMTP (Protocolo simple de transferencia de correo)	TCP	25	Envío de mensajes de correo electrónico	Un codificador de video/cámara de red puede enviar imágenes o notificaciones de alarma utilizando su cliente de correo electrónico integrado
HTTP (Protocolo de transferencia de hipertexto)	TCP	80	Se utiliza para navegar por la red, por ejemplo, para recuperar páginas web de servidores	Es el modo más habitual para transferir video de un codificador de video/cámara de red, en el que el dispositivo de video en red funciona básicamente como servidor web que pone el video a disposición del usuario o del servidor de aplicaciones que lo solicita
HTTPS (Protocolo de transferencia de hipertexto sobre capa de sockets seguros)	TCP	443	Acceso seguro a páginas web con tecnología de cifrado	Transmisión segura de video procedente de codificadores de video/cámaras de red
RTP (Real Time Protocol)	UDP/TCP	No definido	Formato de paquete RTP estandarizado para la entrega de audio y de video a través de Internet (a menudo utilizado en sistemas de transmisión multimedia o videoconferencia)	Un modo habitual de transmitir video en red basado en H.264/MPEG y de sincronizar video y audio, ya que RTP proporciona la numeración y la datación secuencial de paquetes de datos, lo que permite volver a unirlos en el orden correcto. La transmisión se puede realizar mediante unidifusión o multidifusión
RTSP (Protocolo de transmisión en tiempo real)	TCP	554	Utilizado para configurar y controlar sesiones multimedia a través de RTP	

Tabla N° 2. 3 Protocolos y puertos TCP/IP habituales utilizados para el video en red
Fuente: <http://www.marcelopedra.com.ar/blog/2009/08/09/tabla-de-puertos-tcp/>

- *TCP*: proporciona un canal de transmisión fiable basado en la conexión, gestiona el proceso de división de grandes bloques de datos en paquetes más pequeños y garantiza que los datos enviados desde un extremo se reciban en el otro. La fiabilidad de TCP en la retransmisión puede producir retrasos significativos, por lo que en general se utiliza cuando la fiabilidad de la comunicación prevalece sobre la latencia del transporte.
- *UDP*: es un protocolo sin conexión que no garantiza la entrega de los datos enviados, dejando así todo el mecanismo de control y comprobación de errores a cargo de la propia aplicación. No proporciona transmisiones de pérdida de datos, por lo que no provoca retrasos adicionales.

2.5 HIPÓTESIS

El Sistema de vigilancia afecta el acceso remoto para el control de las Unidades Operacionales del Gobierno Autónomo Descentralizado Municipal de Tulcán.

2.6 SEÑALAMIENTO DE VARIABLES

Variable Independiente: Sistema de Vigilancia.

Variable Dependiente: Acceso Remoto.

CAPÍTULO III

METODOLOGÍA

3.1 ENFOQUE DE LA INVESTIGACIÓN

La presente investigación comprendió un enfoque cuali-cuantitativo, debido a que la recolección de datos se la realizó directamente en el Gobierno Autónomo Descentralizado Municipal de Tulcán, logrando obtener datos reales. Efectuándose de esta manera una indagación objetiva y en consecuencia con un margen aceptable de confiabilidad.

3.2 MODALIDAD BÁSICA DE INVESTIGACIÓN

Esta investigación asumió la modalidad de campo porque se situó en las Unidades del Gobierno Autónomo Descentralizado Municipal de Tulcán donde se encontraba el problema y fue respaldada con una investigación documental, la cual permitió plasmar una solución de forma eficaz basada en la interacción con el lugar de indagación y apoyada de conceptualizaciones bibliográficas.

3.3 TIPOS DE INVESTIGACIÓN

El nivel de investigación que se efectuó tuvo un nivel exploratorio porque permitió deducir el problema en un contexto particular. Un nivel descriptivo ya que detalló la realidad e involucró las variables. De tipo explicativo ya que permitió comparar las variables dentro del contexto y de esta manera determinar la factibilidad de la investigación. Y por último de tipo asociación de variables, estableciéndose los vínculos y la correspondencia de las mismas.

3.4 POBLACIÓN Y MUESTRA

Población:

El Gobierno Autónomo Descentralizado Municipal de Tulcán consta actualmente con 21 personas en la Dirección de Gestión Administrativa pertenecientes a las Unidades detalladas a continuación:

DIRECCIÓN DE GESTIÓN ADMINISTRATIVA	
Dirección Administrativa.....	2
Talento Humano.....	5
Informática.....	7
Compras Públicas.....	2
Servicios Generales.....	2
Control de Bienes y Activos.....	3
TOTAL.....	21

Muestra:

Considerándose el tamaño de la población se va a tomar como muestra a las 21 personas que conforman la Dirección de Gestión Administrativa de la entidad municipal, para de esta manera alcanzar resultados confiables.

3.5 OPERACIONALIZACIÓN DE VARIABLES

Tabla N° 3. 1 Operacionalización de la variable independiente: Sistema de Vigilancia.

<p>Sistema de Vigilancia: Son sistemas de seguridad que poseen accesorios de gran complejidad y que son prácticamente ineludibles. Las redes de vigilancia con tecnología IP involucran entre otras cosas: secuencias de imágenes y sonido, los mismos q al integrarse con estándares y normas adicionales forman un mecanismo inteligente con múltiples servicios.</p>	Redes IP	Hardware de red	¿Cuáles son las especificaciones técnicas de los equipos que cumplan los requerimientos de la red IP?	Entrevista
		Software de red	¿Qué sistema de administración de cámaras IP se utilizará?	
	Imagen	Alcance	¿Cuáles son las Unidades del GADMT que demandan de un sistema de Video-vigilancia?	Observación
		Resolución	¿Qué tipo de cámara IP cumple con las condiciones solicitadas por la Institución Municipal?	
	Sonido	Calidad de la señal audible		Bibliográfica
	Estándares y normas	Compresión	¿Cuáles son las ventajas de contar con normas y mecanismos de compresión?	
		Protocolos	¿Cuál es el sistema actual de supervisión para las Unidades del GADMT?	
	Sistema inteligente	Integración de servicios		Encuesta
		Seguridad	¿Cuáles son los beneficios que aporta un sistema de video-vigilancia para el GADMT?	
			Almacenamiento de información	

Elaborado por: El Investigador

Tabla N° 3. 2 Operacionalización de la variable dependiente: Acceso Remoto

Acceso Remoto: permite controlar un equipo de forma remota desde cualquier lugar con conexión a Internet, siempre que se cuente con los requisitos necesarios	Conexión a Internet	Formatos de streaming	¿Cuáles son las condiciones que debe cumplir un sistema de vigilancia para el acceso remoto?	Entrevista
		Reproducción continua de datos		Observación
	Requerimientos de Calidad	Acceso a recursos de la Red	¿El GADMT cuenta actualmente con una red que soporte servicios de convergencia IP?	
		Ancho de banda disponible	¿Se considera necesario que el GADMT cuente con un mecanismo de supervisión de personal y seguridad?	Encuesta
Perdida y retardo de paquetes				

Elaborado por: El Investigador

3.6 TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

Las técnicas empleadas en la presente investigación fueron: la observación, la entrevista y la encuesta.

Observación.- La observación permitió palpar la realidad del entorno investigado, recabando datos de gran importancia para la interpretación de resultados y el discernimiento de las conclusiones.

Entrevista.- Mediante la entrevista se logró obtener un panorama más claro de los aspectos técnicos del proyecto, siendo dirigida al jefe de la Unidad de Sistemas Informáticos del GADMT.

Encuesta.- La encuesta nos permitió establecer parámetros e información significativa por escrito, la cual facultó la obtención de datos válidos. Esta fue realizada al personal que conforma la Dirección de Gestión Administrativa del GADMT que es la encargada de coordinar e implementar el sistema de desarrollo organizacional, delegar y regularizar las relaciones de trabajo en la Municipalidad

3.7 RECOLECCIÓN DE INFORMACIÓN

Tabla N° 3. 3 Plan de recolección de información

PREGUNTAS BÁSICAS	
¿Para qué?	Para lograr los objetivos de la investigación
¿De qué personas u objetos?	Recurso Humano, recaudación, bienes del GADMT
¿Sobre qué aspectos?	Constelación de ideas de las variables
¿Quién?	Investigador: Andrea Ramos
¿Cuándo?	Abril – Mayo /2012
¿Dónde?	Instalaciones del GADMT
¿Cuántas veces?	Las necesarias
¿Qué técnicas de recolección?	Observación, entrevista y encuesta
¿Con qué?	Cuestionarios

Elaborado por: El Investigador

3.8 PROCESAMIENTO DE LA INFORMACIÓN

Para realizar un apropiado procesamiento de la información se estableció el siguiente orden de funcionalidades para optimizar tiempo y obtener resultados efectivos:

- Revisión crítica de la información recogida, es decir limpieza de información defectuosa, contradictoria, incompleta, no pertinente, etc.
- Repetición de la recolección, en casos para corregir las fallas de contestación
- Tabulación en cuadros según variables de cada hipótesis
- Cuadro de cartas de control: por variables,
- Manejo de la información estudio estadístico de datos para presentación de resultados

3.9 ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

- Análisis de los resultados estadísticos, destacando tendencias relacionadas fundamentalmente de acuerdo con los objetivos e hipótesis.
- Interpretación de los resultados porcentuales, gráficos y estadísticos con apoyo del marco teórico, en el aspecto pertinente.
- Comprobación de hipótesis, para la investigación estadística conviene seguir la asesoría de un especialista en el tema.
- Restablecimiento de conclusiones y recomendaciones.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 INTRODUCCIÓN

El siguiente análisis corresponde al estudio de equipos, al tráfico de red, a los resultados extraídos de la encuesta realizada a 21 servidores públicos de la Dirección de Gestión Administrativa y a la entrevista dirigida al jefe de la Unidad de Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal de Tulcán.

Se estableció la situación de la red actual en cuanto a puntos y dispositivos que lo conforman, lo cual permitió la determinación y diagnóstico de la utilización de la misma.

En cuanto a la encuesta y entrevista el personal municipal mostró total disposición y participación en el desarrollo del proceso investigativo, proporcionando una clara visión del sistema de vigilancia actual empleado en la entidad municipal y sus necesidades.

La información adquirida fue tabulada y analizada de forma sistemática de acuerdo a las interrogantes planteadas, siendo interpretada estadísticamente para lograr resultados concisos y confiables.

4.2 RED DEL GADMT

4.2.1 PUNTOS DE RED DEL GADMT

El Gobierno Autónomo Descentralizado Municipal de Tulcán cuenta con 162 puntos de red distribuidos en las diferentes Unidades del edificio institucional que consta de una planta baja y cuatro pisos. Los mismos que son utilizados para conexión con PC's e impresoras. En Tabla N°4.1 se observa su distribución según sus Unidades:

DIRECCIÓN/UNIDAD	PUNTOS DE RED OCUPADOS
CAFE NET	4
RENTAS	6
RECAUDACIÓN	7
BIENES Y ACTIVOS	4
COMISARÍA	2
ADMINISTRACIÓN DE MERCADOS	2
GESTIÓN AMBIENTAL Y RIESGOS	6
PROYECTOS	8
TRÁNSITO Y TRANSPORTE	2
PLANIFICACIÓN	9
CONSTRUCCIONES	4
ZONAS AZULES	4
AVALUOS Y CATASTROS	10
DIRECCIÓN FINANCIERA	6
TESORERÍA	4
COACTIVAS	4
CONTABILIDAD	4
COMPRAS PÚBLICAS	2
PLANEACION ESTRATÉGICA	12
COMUNICACIONES	7
ALCALDÍA	4
SECRETARÍA GENERAL	2
DIRECCIÓN ADMINISTRATIVA	2
SERVICIOS GENERALES	2
TALENTO HUMANO	5
FISCALIZACIÓN	7
OBRAS PÚBLICAS	6
SINDICATURA	4
AUDITORIA INTERNA	2
CULTURA	6
DESARROLLO SOSTENIBLE	3
BIBLIOTECA	3
SALON MÚLTIPLE	1
ASOCIACIÓN DE EMPLEADOS	1
INFORMÁTICA	7
TOTAL	162

Tabla N° 4. 1 Distribución de puntos de red de Pc's e impresoras en el edificio municipal
Elaborado por: El Investigador

4.2.2 EQUIPOS DE RED DEL GADMT

En Tabla N°4.2 se indican los equipos de red actuales del GADMT:

CANTIDAD	EQUIPO	MODELO	PUERTOS	IMAGEN
4	Switch	D-LINK DES-1024R+	24 puertos	
1	Switch	D-LINK DES-3526	24 puertos	
2	Switch	CNET CSH-1600	16 puertos	
2	Switch	D-LINK DES-1228	28 puertos	
1	Switch	DELL 2724	24 puertos	
1	Switch	TRENDNET TE100-S8	8 puertos	
1	Switch	CISCO CATALYST 3550	48 puertos	
1	Switch	D-LINK DES-1008D	8 puertos	
1	Router	Cisco 800 Series	4 puertos	
2	Central Telefónica	NEC IP2AP-924M-KSU PABX Main Equipment		
2	Access Point	UBIQUITI-UniFi Enterprise WiFi System		
1	Access Point	DWL-3200AP 802.11G		

Tabla N° 4. 2 Equipos de red del GADMT
Elaborado por: El Investigador

4.2.3 EQUIPOS SERVIDORES DEL GADMT

En Tabla N°4.3 se detallan los equipos servidores actuales del GADMT:






MARCA/ MODELO	IMAGEN
HP PROLIANT ML-150 G2	
HP PROLIANT DL-380 G6	
HP PROLIANT ML-150 G2	
COMPAQ PROLIANT 800	
HP PROLIANT ML-150 G2	

Tabla N° 4. 3 Equipos servidores GADMT
Elaborado por: El Investigador

4.2.4 ANÁLISIS DE TRÁFICO DE LA RED ACTUAL DEL GADMT

4.2.4.1 Determinación del tráfico LAN

El tráfico de redes de área local se mide como la cantidad de información promedio que se transfiere a través del canal de comunicación y a la velocidad de transferencia. El análisis de tráfico del edificio del GADMT se lo realizó mediante la utilización del software CommView versión 6.0 para el monitoreo de tramas ethernet y CommView for WiFi versión 6.3 para el análisis de tramas 802.11.

Para realizar la captura de paquetes la tarjeta del computador debe estar en modo promiscuo. El modo promiscuo significa que las tarjetas Ethernet operan de modo que

el tráfico que reciben viene marcado con su dirección MAC y aceptan el paquete, caso contrario lo rechazan.

a. CommView versión 6.0

Es un programa que permite monitorear la actividad de Internet y redes de área local siendo capaz de capturar y analizar paquetes de red. Recoge información acerca del tráfico de datos a través de su conexión telefónica o su tarjeta Ethernet y decodifica los datos analizados.

En la figura N° 4.1 se observa la interfaz del programa que contiene seis pestañas que le permiten ver los datos y realizar diversas acciones sobre los paquetes capturados. Para comenzar la captura de paquetes, seleccione un adaptador de red desde la lista del menú en la barra de herramientas, haga clic en el botón Iniciar Captura o seleccione Archivo => Iniciar Captura en el menú. Si el tráfico de red pasa a través del adaptador seleccionado, CommView comenzará a mostrar la información.

IP Local	IP Remota	Entrada	Salida	Dirección	Sesiones	Puertos	Nombre de Host	Bytes	Proceso
? 192.168.100.11	? 192.168.100.255	0	343	Paso	0	netbios-ns		37.730	
? 192.168.100.233	? 192.168.100.255	0	128	Paso	0	netbios-ns		11.898	
? 192.168.100.249	? 192.168.100.255	0	43	Paso	0	netbios-ns		4.107	
? 192.168.100.20	? 192.168.100.255	0	17	Paso	0	netbios-ns		1.564	
? 192.168.100.156	? 192.168.100.255	0	38	Paso	0	netbios-ns		3.744	
? 192.168.100.200	? 192.168.100.252	8	8	Salida	0	domain		1.600	svchost.exe
? 192.168.100.183	? 192.168.100.255	0	9	Paso	0	netbios-ns		828	
? 192.168.100.139	? 192.168.100.255	0	3	Paso	0	netbios-ns		276	
? fe80::e86a9187-062...	? ff02::0001:0002	0	3	Paso	0	dhcpv6-...		483	
? fe80::b8b39ba1-49f...	? ff02::0001:0002	0	2	Paso	0	dhcpv6-...		302	
? 192.168.100.116	? 192.168.100.255	0	3	Paso	0	netbios-ns		276	
? 192.168.100.252	? 192.168.100.53	0	1	Paso	0	49418.2221	SERVIDOR_CAFE...	74	
? fe80::e87c-d191-a10...	? ff02::0001:0002	0	1	Paso	0	dhcpv6-...		158	
? 192.168.100.156	? 192.168.100.223	0	12	Paso	0	2195.net...	ALAMIRO_MON...	2.093	
? 192.168.100.156	? 192.168.100.205	0	6	Paso	0	2199.net...	ALVARO_NOGUE...	1.125	
? fe80::5c31-a23-e57...	? ff02::0001:0002	0	1	Paso	0	dhcpv6-...		152	
? 192.168.100.156	? 192.168.100.246	0	1	Paso	0	netbios-ns	ALCALDIA-HP	104	
? 192.168.100.252	? 192.168.100.179	0	1	Paso	0	netbios-ns	nataly_burbano	105	
? 192.168.100.67	? 239.255.255.250	0	1	Paso	0	55382_ssdp		175	
? 192.168.100.110	? 224.0.0.251	0	1	Paso	0	5353		81	

Figura N° 4. 1 Monitoreo del tráfico LAN del GADMT
Fuente: Imagen capturada del software CommView versión 6.0

b. CommView for WiFi versión 6.3

Es una edición especial de CommView diseñado para capturar y analizar paquetes de red sobre redes inalámbricas 802.11a/b/g. CommView for WiFi recoge información del adaptador inalámbrico y decodifica los datos analizados.

Con CommView for WiFi puede ver la lista de conexiones de red, estadísticas vitales de IP y examinar paquetes individuales.

Previo a seleccionar el canal del cual se va a capturar los paquetes, se realiza un barrido de todos puntos de acceso y estaciones que se encuentran disponibles alrededor de nuestra red. En la figura N° 4.2 se puede apreciar que el canal 5 es el correspondiente a la red inalámbrica del GADMT.

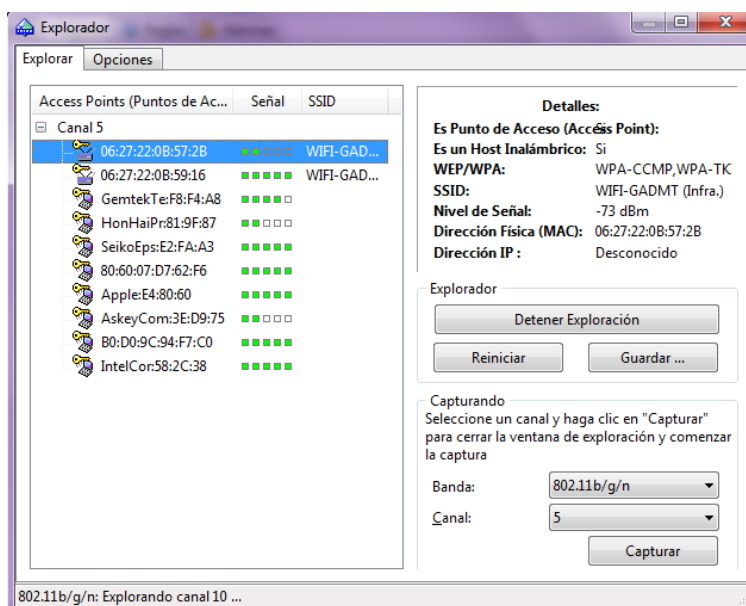


Figura N° 4. 2 Selección del canal del cual se capturará los paquetes de la WLAN del GADMT

Fuente: Imagen capturada del software CommView for Wifi versión 6.3

Una vez se seleccione el canal a analizar, se procede a capturar los paquetes que atraviesan o circulan por dicho canal, en la figura N° 4.3 se muestran los paquetes capturados correspondientes sólo al canal 5.

Dirección Física (MAC)	Canal	Tipo	SSID	Encriptación	Señal	Velocidad	Bytes	Paquetes	Reintentar	Errores ICV
06:27:22:08:57:2B	5	AP	WIFI-GADMT	WPA-CCMP,W...	-89/-76/-69	1,5,55/24	2.156.034	13.448	628	0
06:27:22:08:59:16	5	AP	WIFI-GADMT	WPA-CCMP,W...	-91/-40/-31	1,9,44/54	4.856.142	32.770	2.176	0
AskeyCom3E09:75	5	STA		WPA	-72/-69/-64	36/51,84/54	189.418	838	14	0
GemtekTef8:F4:A8	5	STA		WPA	-71/-50/-45	36/52,54/54	1.688.708	4.950	84	0
IntelCon58:2C:38	5	STA		WPA	-64/-61/-79	1,9,64/24	247.876	1.904	8	0
HonHaiPr81:9F:87	5	STA		WPA	-90/-82/-78	1,1,62/12	387.570	8.934	160	0
50:CC:F8:35:E3:B5	5	STA			-77/-74/-71	1/1/1	37.240	562	0	0
Apple70:4D:F2	5	STA			0/0/0	0/0/0	1.598	104	0	0
AppleE4:80:60	5	STA		WPA	-88/-85/-80	1/1/1	9.592	124	6	0

Figura N° 4. 3 Captura de paquetes del canal 5 correspondiente a la WLAN del GADMT
Fuente: Imagen capturada del software CommView for Wifi versión 6.3

4.2.4.2 Resultados del monitoreo de la red del GADMT

El monitoreo de tráfico se realizó durante un período efectivo de 5 días, en horario de trabajo comprendido desde las 9:30 am, hasta las 11:30 am.

Para los días de pruebas los usuarios de las unidades operativas del GADMT implicados en el estudio, estuvieron trabajando normalmente en sus actividades, es decir conectados a sus equipos efectuando sus labores habituales en cuanto a conexiones de las diferentes aplicaciones que se utilizan, tal como los sistemas integrados de contabilidad y catastros, acceso a Internet, acceso a los servidores, etc.

Los software CommView versión 6.0 y CommView for WiFi versión 6.3 determinaron el desempeño de la red en el GADMT, analizando direcciones IP privadas de clase C, realizando un barrido desde la 192.168.100.1 hasta la 192.168.100.254.

a. LAN GADMT

En las tablas N° 4.4, 4.5, 4.6, 4.7 y 4.8 se observan las mediciones realizadas en la LAN del GADMT monitoreadas desde el Lunes 28 de Mayo hasta el Viernes 1 de Junio del 2012.

Lunes

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	2.033	4.731	52.698
Bytes	323.887	533.998	5.788.410
Bytes por segundo	187	308	2.336

Tabla N° 4. 4 Tráfico LAN Lunes 28 de Mayo del 2012

Elaborado por: El Investigador

Martes

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	87.273	71.843	147.971
Bytes	16.040.641	74.386.918	17.543.070
Bytes por segundo	2.237	10.372	2.446

Tabla N° 4. 5 Tráfico LAN Martes 29 de Mayo del 2012

Elaborado por: El Investigador

Miércoles

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	104.194	85.429	215.452
Bytes	26.197.628	68.790.363	23.779.359
Bytes por segundo	3.538	9.291	3.212

Tabla N° 4. 6 Tráfico LAN Miércoles 30 de Mayo del 2012

Elaborado por: El Investigador

Jueves

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	26.816	38.990	171.244
Bytes	5.365.120	6.609.371	19.588.953
Bytes por segundo	767	945	2.800

Tabla N° 4. 7 Tráfico LAN Jueves 31 de Mayo del 2012

Elaborado por: El Investigador

Viernes

Item \ Dirección	Entrante	Saliente	Pasante
Paquetes	87.382	71.954	147.982
Bytes	16.040.752	74.386.929	17.543.181
Bytes por segundo	2.348	10.483	2.557

Tabla N° 4. 8 Tráfico LAN Viernes 1 de Junio del 2012

Elaborado por: El Investigador

b. WLAN GADMT

En las tablas N° 4.9, 4.10, 4.11, 4.12 y 4.13 se observan las mediciones realizadas en la WLAN del GADMT, monitoreadas desde el lunes 28 de Mayo hasta el Viernes 1 de Junio del 2012.

Lunes

Item \ Dirección	Pasante
Paquetes	682.441
Bytes	83.883.324
Bytes por segundo	50.931

Tabla N° 4. 9 Tráfico WLAN Lunes 28 de Mayo del 2012

Elaborado por: El Investigador

Martes

Item \ Dirección	Pasante
Paquetes	1.115.060
Bytes	93.875.154
Bytes por segundo	56.654

Tabla N° 4. 10 Tráfico WLAN Martes 29 de Mayo del 2012

Elaborado por: El Investigador

Miércoles

Item \ Dirección	Pasante
Paquetes	495.024
Bytes	113.496.980
Bytes por segundo	68.230

Tabla N° 4. 11 Tráfico WLAN Miércoles 30 de Mayo del 2012

Elaborado por: El Investigador

Jueves

Item \ Dirección	Pasante
Paquetes	623.640
Bytes	109.791.684
Bytes por segundo	63.321

Tabla N° 4. 12 Tráfico WLAN Jueves 31 de Mayo del 2012

Elaborado por: El Investigador

Viernes

Item \ Dirección	Pasante
Paquetes	784.746
Bytes	106.796.396
Bytes por segundo	60.796

Tabla N° 4. 13 Tráfico WLAN Viernes 1 de Junio del 2012

Elaborado por: El Investigador

4.2.4.3 Análisis de tráfico de la red del GADMT

El desempeño de la red se caracterizó utilizando los siguientes parámetros:

- Cantidad de Tráfico: cantidad de información promedio que se transfiere a través del canal de comunicación,
- Tasa de Transferencia: velocidad de transmisión que pasa por una línea de telecomunicación.
- Porcentaje de Utilización: relación entre de tráfico medido al tráfico máximo que el puerto puede administrar.

A continuación se muestra el análisis de la red LAN y WLAN del Gobierno Autónomo Descentralizado Municipal de Tulcán.

a. LAN GADMT

En la Figura N° 4.4 se puede observar la cantidad de bytes o de tráfico LAN que se generó en la red durante los 5 días de mediciones.

Para el tercer día de la prueba la cantidad de información que corresponde al día Miércoles revela que hubo un aumento considerable de los datos circulantes en la red, mientras que el Lunes se registra como el día que posee menor tráfico; también se pudo evidenciar que el resto de los días de las pruebas el tráfico se mantuvo similar en cuanto a la cantidad.

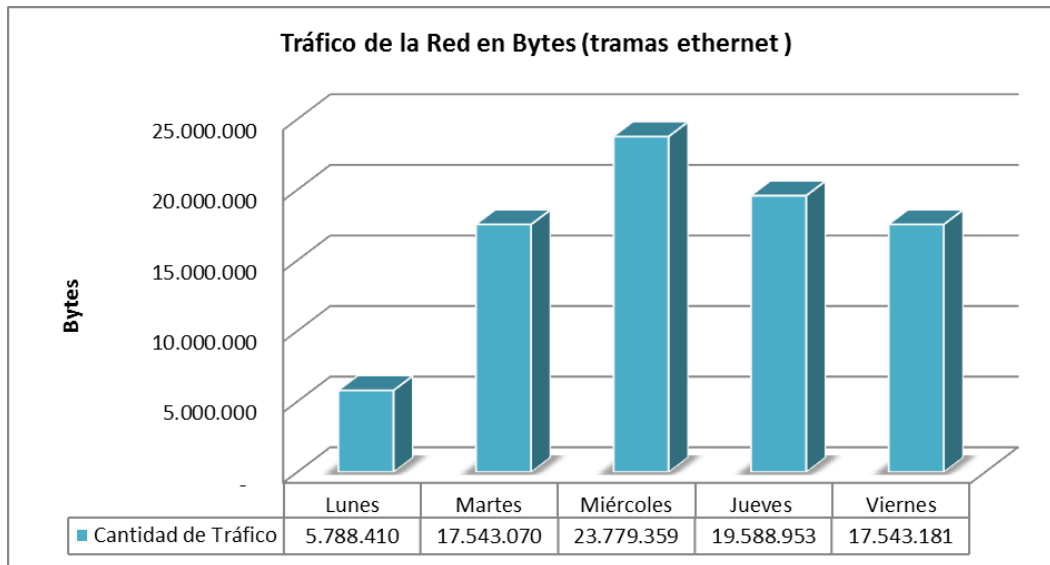


Figura N° 4. 4 Cantidad de tráfico LAN para un monitoreo de 5 días
Elaborado por: El Investigador

La Figura N° 4.5 muestra la tasa de transferencia o velocidad medida en Bytes por segundo, en la que se observa que en el día miércoles la velocidad incrementó a 3212 Bytes por segundo (26Kbps) debido a la cantidad de información requerida, lo que acrecentó la transferencia con respecto al resto de días de la semana.

De igual forma el día lunes presenta la menor tasa de transferencia y en los restantes 3 días de las pruebas, la velocidad se mantuvo casi al mismo nivel, ya que no hubo alguna variación en cuanto a los accesos a la red.

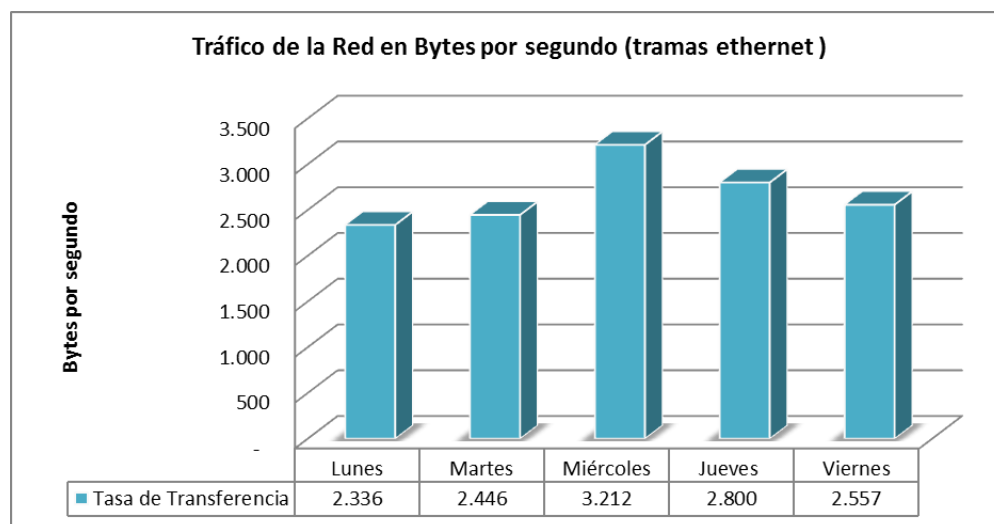


Figura N° 4. 5 Tasa de transferencia LAN para un monitoreo de 5 días
Elaborado por: El Investigador

El porcentaje de utilización de la Red es la proporción de tráfico de red corriente al tráfico máximo que el puerto pueda manejar. Esto indica el uso del ancho de banda.

En la Figura N° 4.6, puede observarse el porcentaje de utilización de la red del GADMT en los días laborables, el cual es bajo. Frente a estos aspectos se concluye que la red LAN Municipal tiene un desempeño óptimo.

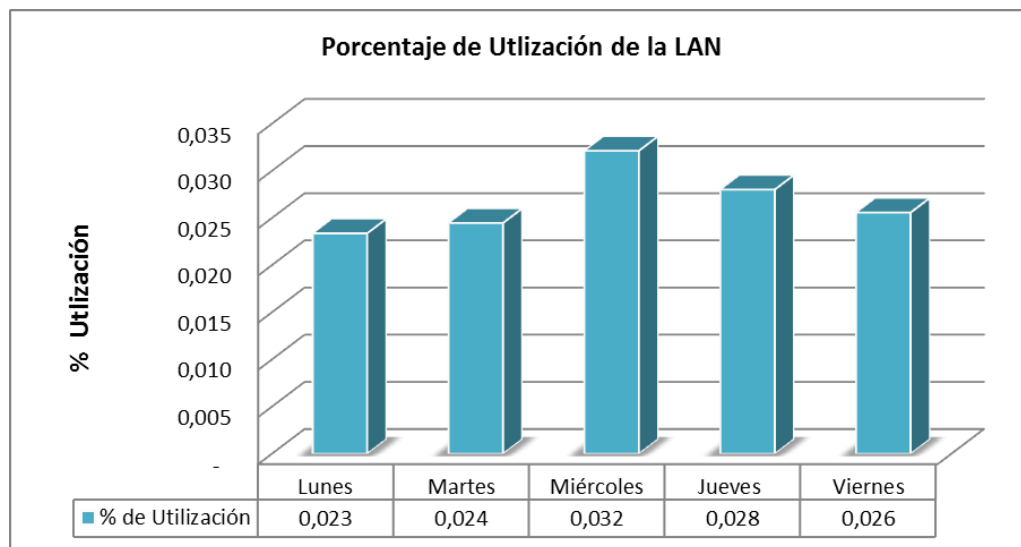


Figura N° 4. 6 Porcentaje de utilización LAN para un monitoreo de 5 días
Elaborado por: El Investigador

b. WLAN GADMT

En la Figura N° 4.7 se puede observar la cantidad de bytes o de tráfico WLAN que se generó en la red durante los 5 días de mediciones.

Los datos obtenidos se muestran que el día miércoles hubo un aumento de la información circulante en la red inalámbrica, mientras que el lunes es el día de menor tráfico, también se puede apreciar que el resto de días el tráfico se mantuvo similar.

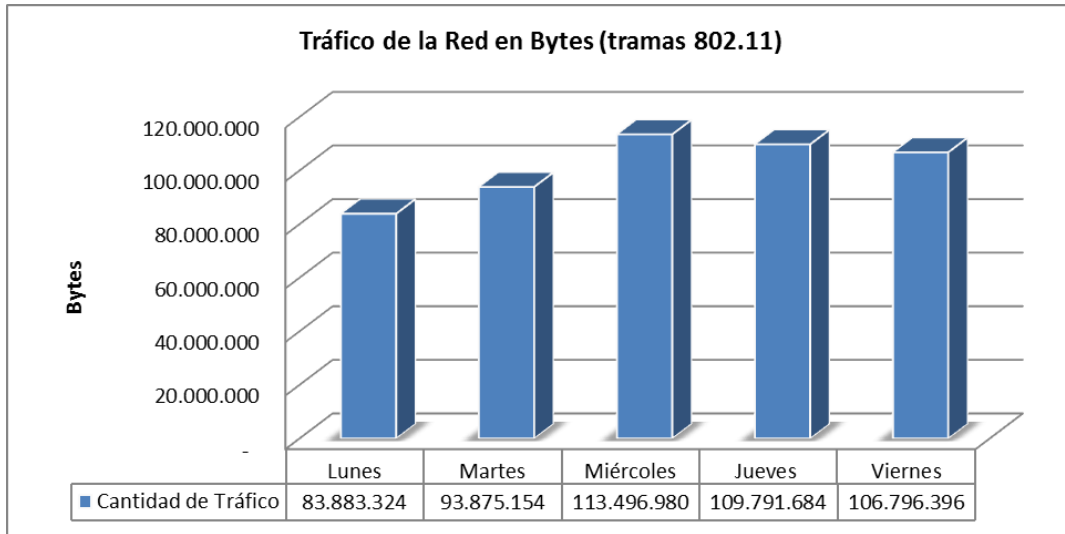


Figura N° 4. 7 Cantidad de tráfico WLAN para un monitoreo de 5 días
Elaborado por: El Investigador

La Figura N° 4.8 determina la tasa de transferencia medida en Bytes por segundo, en la que se observa que en el día miércoles la velocidad aumentó a 68230 Bytes por segundo (546 Kbps), de manera opuesta el día lunes presenta la menor tasa de transferencia y en los restantes 3 días de pruebas la velocidad se mantuvo.

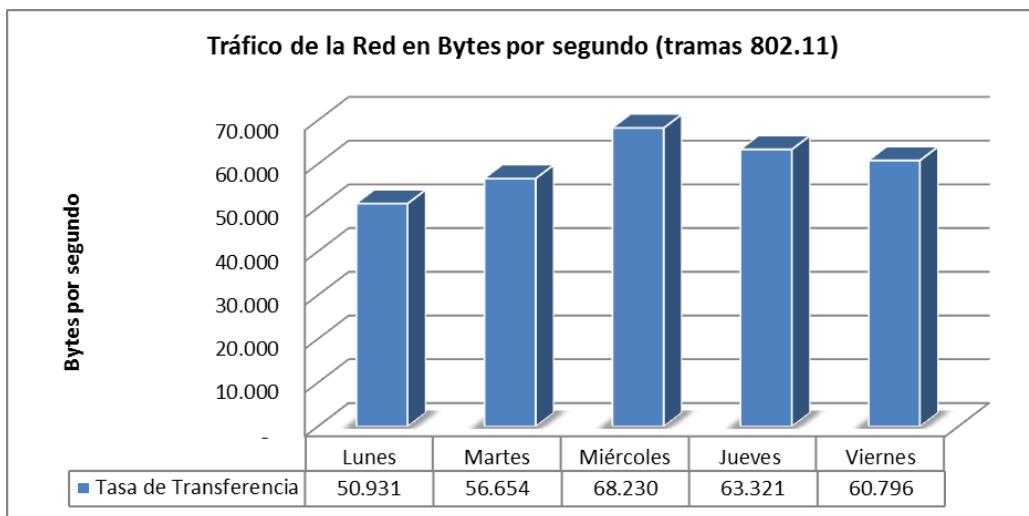


Figura N° 4. 8 Tasa de transferencia WLAN para un monitoreo de 5 días
Elaborado por: El Investigador

En la Figura N° 4.9, se indica que el porcentaje de utilización de la red inalámbrica en los días laborables es bajo. Frente a estos aspectos se concluye que la red WLAN del GADMT tiene un desempeño favorable.

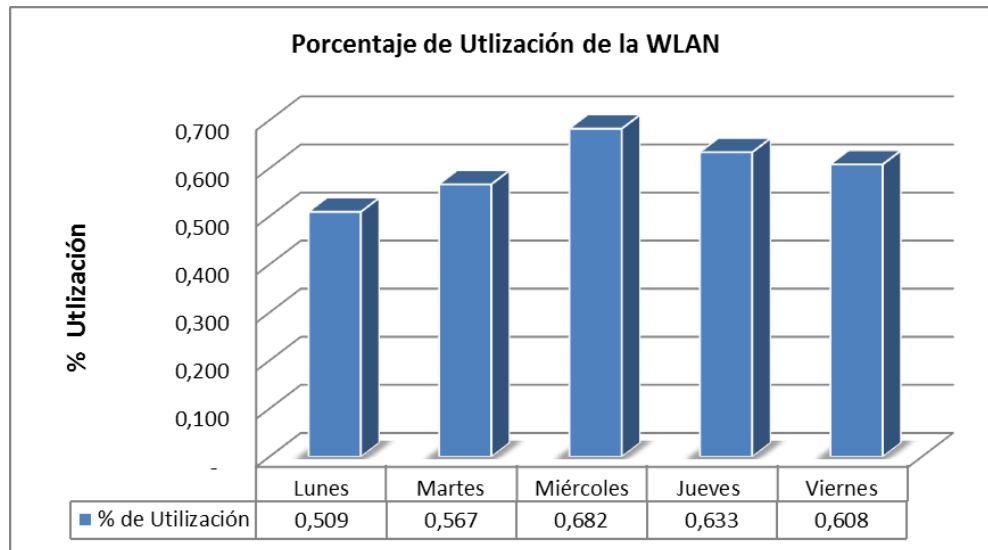


Figura N° 4. 9 Porcentaje de utilización WLAN para un monitoreo de 5 días
Elaborado por: El Investigador

En consecuencia, los datos y mediciones obtenidas en el monitoreo de la LAN y la WLAN revelan que el tráfico de la red del Gobierno Autónomo Descentralizado Municipal de Tulcán es bajo con tasas de transferencia máximas de 26 Kbps y 546 Kbps respectivamente, por lo que su servicio es aceptable, con tiempos de respuestas apropiados, contribuyendo a la disminución de problemas potenciales como el decremento de colisiones que ha menudo se producen como resultado de contar con demasiados usuarios o demasiada información existente en la red.

4.3 ENCUESTA

Encuesta dirigida al personal que conforma la Dirección de Gestión Administrativa del GADMT.

- **Pregunta 1**

¿Considera usted que el GADMT cuenta con un sistema de vigilancia que permita la continua supervisión de las instalaciones del edificio municipal?

Item	Frecuencia	Porcentaje (%)
Si	1	5 %
No	20	95 %
Total	21	100 %

Tabla N° 4. 14 Existencia de un sistema de vigilancia en el edificio del GADMT

Elaborado por: El Investigador



Figura N° 4. 10 Existencia de un sistema de vigilancia en el GADMT

Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.

Elaborado por: El Investigador

Análisis e Interpretación: De lo observado en figura N° 4.10 se determina que el 95% de los encuestados atestigua la inexistencia de un sistema de vigilancia que permita la supervisión continua de las instalaciones del edificio municipal, mientras el 5% considera que si existe.

De los datos obtenidos se aprecia que actualmente el GADMT no cuenta con un sistema de vigilancia que permita la inspección permanente del edificio municipal por lo cual su seguridad se torna vulnerable.

- **Pregunta 2**

¿Cual de las siguientes opciones considera usted de mayor eficiencia en el ámbito de seguridad y vigilancia institucional?

Item	Frecuencia	Porcentaje (%)
Guardias	0	0 %
Video-vigilancia electrónica	3	14 %
Las dos opciones anteriores	18	86 %
Total	21	100 %

Tabla N° 4. 15 Mecanismo eficiente en el ámbito de la seguridad y vigilancia, según los empleados de la dirección de Gestión administrativa del GADMT

Elaborado por: El Investigador

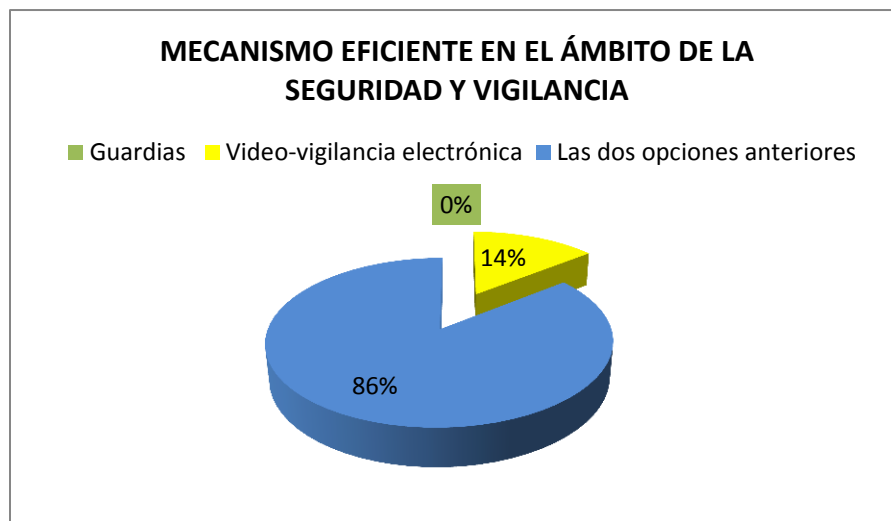


Figura N° 4. 11 Mecanismo eficiente en el ámbito de la seguridad y vigilancia

Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.

Elaborado por: El Investigador

Análisis e Interpretación: Analizando la figura N° 4.11 se concluye que el 86% del personal de Gestión Administrativa del GADMT considera que la video-vigilancia en conjunto con los guardias proveen eficiencia en el ámbito de la seguridad y control para el edificio municipal, el 14% opina que únicamente un sistema electrónico proporciona la eficiencia requerida.

- **Pregunta 3**

¿Esta de acuerdo que la información procedente de un sistema de vigilancia de oficinas municipales sea visualizada?

Item	Frecuencia	Porcentaje (%)
Si	16	76 %
No	5	24 %
Total	21	100 %

Tabla N° 4. 16 Aceptación a la visualización de información por parte de lo empleados del GADMT
Elaborado por: El Investigador

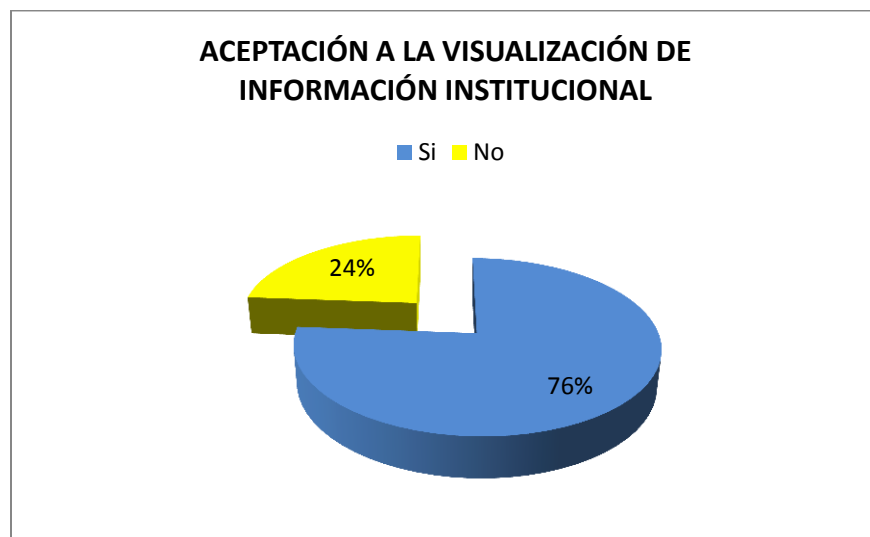


Figura N° 4. 12 Aceptación a la visualización de información Institucional
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: Considerando la figura N° 4.12 se establece que el 76% de los servidores municipales de la dirección administrativa está de acuerdo que la información procedente de un sistema de vigilancia sea visualizada a diferencia del 24% que no coincide con este planteamiento.

En su mayoría los encuestados están conscientes del sinnúmero de beneficios que trae consigo la adopción de un mecanismo en el cual pueda visualizarse frecuentemente las unidades del GADMT.

- **Pregunta 4**

¿Cree conveniente la inspección de bienes a cualquier hora del día en el interior del edificio municipal?

Item	Frecuencia	Porcentaje (%)
Si	20	95 %
No	1	5 %
Total	21	100 %

Tabla N° 4. 17 Consentimiento en la inspección de bienes de los empleados en el interior del edificio municipal

Elaborado por: El Investigador

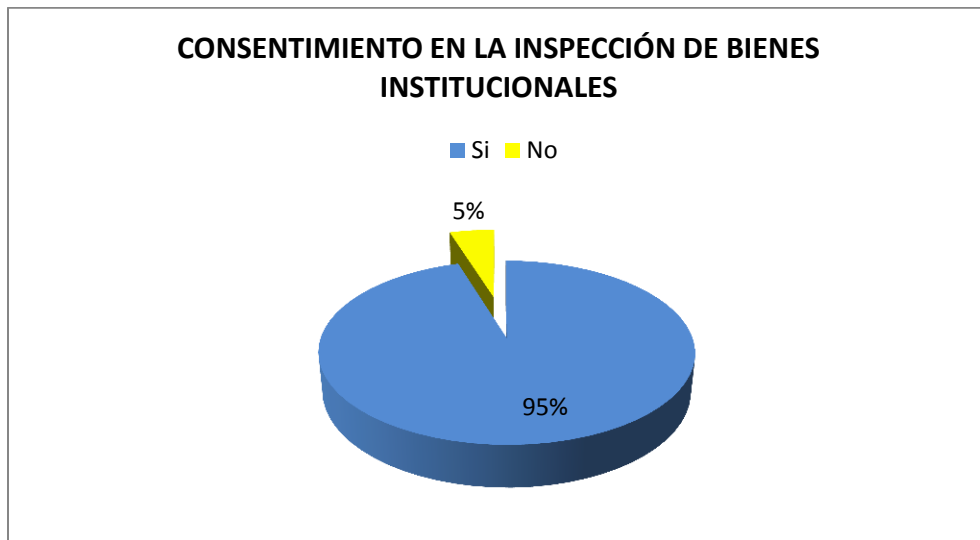


Figura N° 4. 13 Consentimiento en la inspección de bienes Institucionales
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.

Elaborado por: El Investigador

Análisis e Interpretación: Los resultados de la figura N° 4.13 muestran que el 95% de los encuestados cree conveniente la inspección de bienes a cualquier hora del día en el interior del edificio municipal, mientras que el 5% restante no lo considera necesario.

La adquisición y preservación de bienes institucionales es una de las principales funciones y propósitos de la Dirección Administrativa Municipal, por lo que se hace necesario disponer de un sistema que garantice el buen estado y resguardo de los mismos.

- **Pregunta 5**

Tiene usted conocimiento de sucesos que se hayan efectuado en la institución, tales como:

Item	Frecuencia	Porcentaje (%)
Hurto de bienes institucionales	11	39 %
Hurto de bienes personales	10	36 %
Hurto de dinero	2	7 %
Ningún suceso indebido	5	18 %
Total	28	100 %

Tabla N° 4. 18 Conocimiento de sucesos indebidos efectuados en el GADMT
Elaborado por: El Investigador

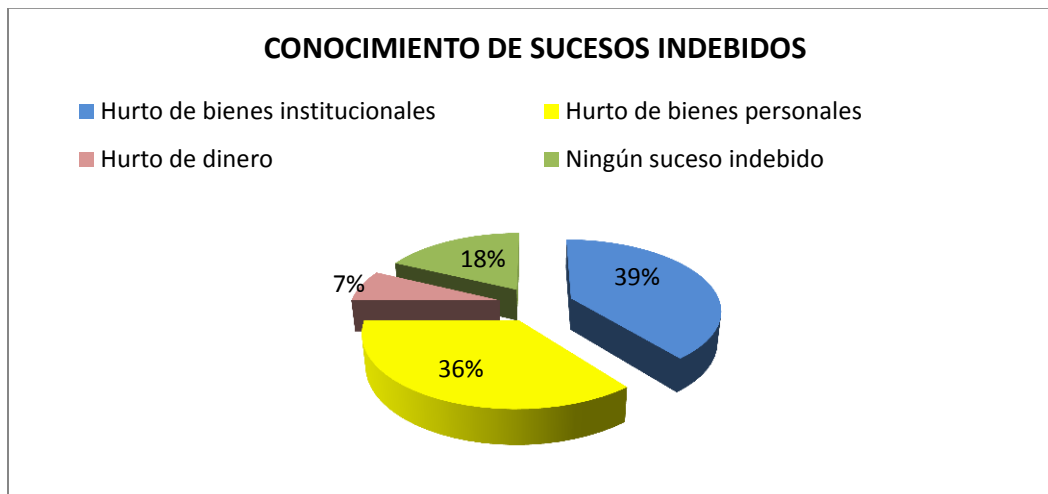


Figura N° 4. 14 Conocimiento de sucesos indebidos efectuados en el GADMT
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: Observando la figura N° 4.14 la misma que corresponde a una pregunta de selección múltiple se deduce que el 39% del personal de Gestión Administrativa tiene conocimiento a cerca del hurto de bienes en el interior de la institución municipal, el 36% manifiesta estar al tanto sobre casos de hurto de bienes personales, el 7% indica conocer incidentes de hurto de dinero, mientras que el 18% de los empleados señala no tener cognición de sucesos indebidos en el edificio municipal.

De acuerdo a los resultados obtenidos se denota la necesidad por parte de los empleados municipales de contar con un mecanismo de seguridad que evite la ocurrencia de hechos perjudiciales y afiance su protección.

- **Pregunta 6**

¿Cómo califica el hecho de contar con un mecanismo de seguridad que almacene información de modo que pueda aportar como indicio para esclarecer un suceso indebido?

Item	Frecuencia	Porcentaje (%)
Bueno	20	95 %
Malo	0	0 %
Regular	1	5 %
Total	21	100 %

Tabla N° 4. 19 Aceptación del almacenamiento de información por parte de lo empleados del GADMT
Elaborado por: El Investigador

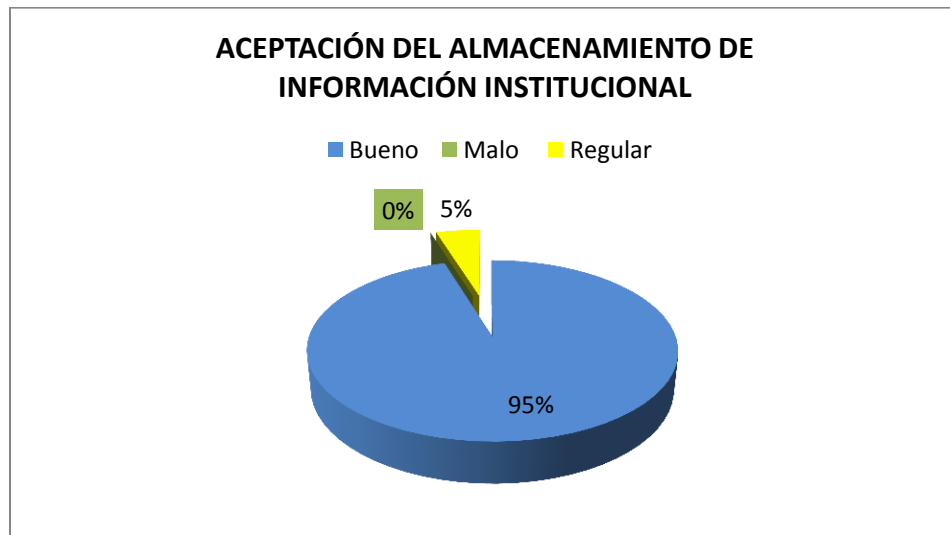


Figura N° 4. 15 Aceptación del almacenamiento de información institucional
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: La figura N° 4.15 permite establecer el porcentaje de aceptación de los encuestados a cerca del hecho de contar con un mecanismo de seguridad que almacene información de modo que pueda aportar como indicio para esclarecer un suceso indebido, frente a lo planteado el 95% lo califica como bueno, el 5% lo señala como regular y ningún miembro del personal 0% lo define como malo.

En la presente pregunta se concluye que los empleados municipales consideran importante el resguardo y preservación de evidencias en la entidad.

- **Pregunta 7**

¿A su criterio cuáles son las oficinas de la entidad municipal que requieren esencialmente de un sistema de video-vigilancia?

Aquellas que tienen a su cargo:

Item	Frecuencia	Porcentaje (%)
Recursos económicos	1	4 %
Bienes/Equipos Institucionales	3	14 %
Todas las unidades	18	82 %
Total	22	100 %

Tabla N° 4. 20 . Unidades del GADMT que requieren de un sistema de video-vigilancia
Elaborado por: El Investigador

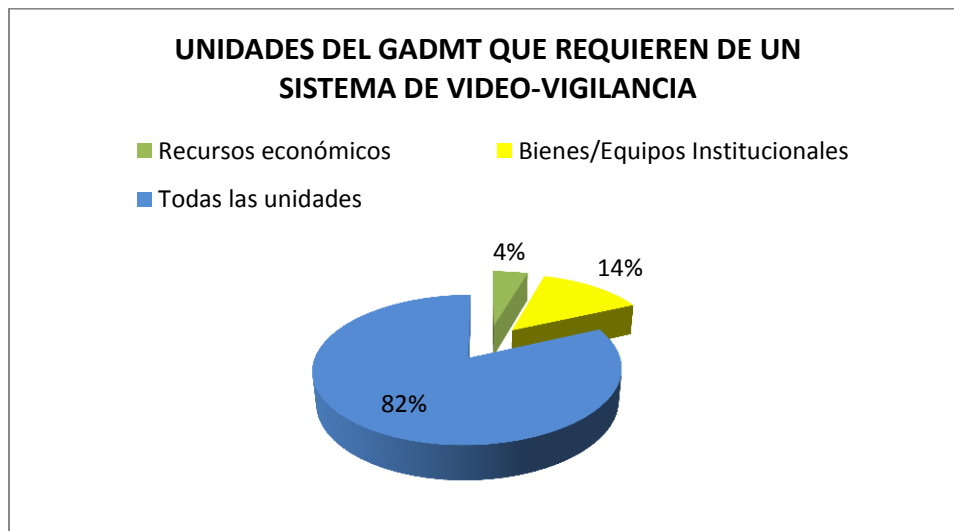


Figura N° 4. 16 Unidades del GADMT que requieren de un sistema de video-vigilancia.
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: De la figura N° 4.16 que corresponde al resultado de la presente interrogante de selección múltiple, se determina que el 82% del personal administrativo indica que se requiere de un sistema de video-vigilancia en todas las unidades del edificio del GADMT, el 14% opina que únicamente se requiere del sistema en las unidades que tengan almacenados una cantidad razonable de bienes y equipos institucionales, mientras que el 4% sugiere la necesidad del mismo en las oficinas que tengan bajo su dominio recursos económicos.

De los datos obtenidos se destaca la necesidad de contar con un sistema de video-vigilancia en todas las oficinas del edificio municipal, permitiendo impulsar el orden y desarrollo de la institución.

- **Pregunta 8**

A su juicio seleccione la(s) principal(es) utilidad(es) que aportará un sistema de video-vigilancia en el GADMT:

Item	Frecuencia	Porcentaje (%)
Seguridad para empleados municipales	3	11 %
Conservación de evidencias	6	22 %
Supervisión durante las 24 horas del día	5	19 %
Todas los anteriores	13	48 %
Total	27	100 %

Tabla N° 4. 21 Principales utilidades que aporta un sistema de video-vigilancia para el GADMT
Elaborado por: El Investigador

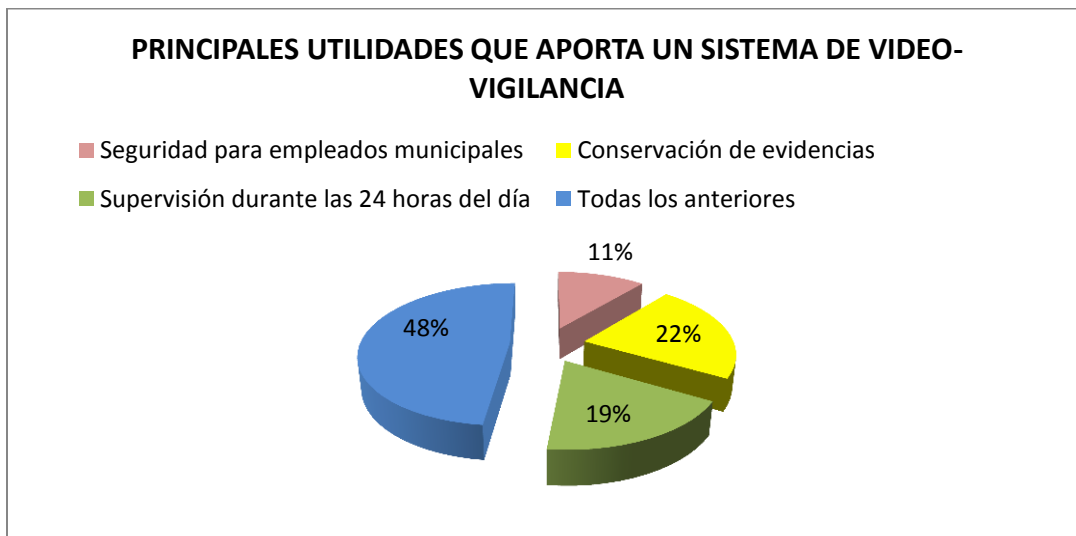


Figura N° 4. 17 Principales utilidades que aporta un sistema de video-vigilancia para el GADMT
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: Tomando en cuenta los resultados de selección múltiple de la octava pregunta representados en la figura N° 4.17 se estipula que el 11% de servidores públicos de la gestión administrativa considera que la principal utilidad que aportará un sistema de video-vigilancia en el GADMT es la seguridad de los empleados, el 19% opina que es primordial la supervisión de las instalaciones del edificio durante las 24 horas del día, el 22% establece la importancia de contar con un mecanismo de conservación de evidencias, frente al 48% que precisa la trascendencia de contar con todas estas utilidades en un solo sistema, lo cual es posible mediante la adopción de un mecanismo electrónico de video-vigilancia IP.

- **Pregunta 9**

¿Como contempla usted el hecho de que el GADMT cuente con un sistema de video-vigilancia IP?

Item	Frecuencia	Porcentaje (%)
Bueno	20	95 %
Malo	1	5 %
Regular	0	0 %
Total	21	100 %

Tabla N° 4. 22 Aprobación de la existencia de un sistema de video-vigilancia en el GADMT
Elaborado por: El Investigador

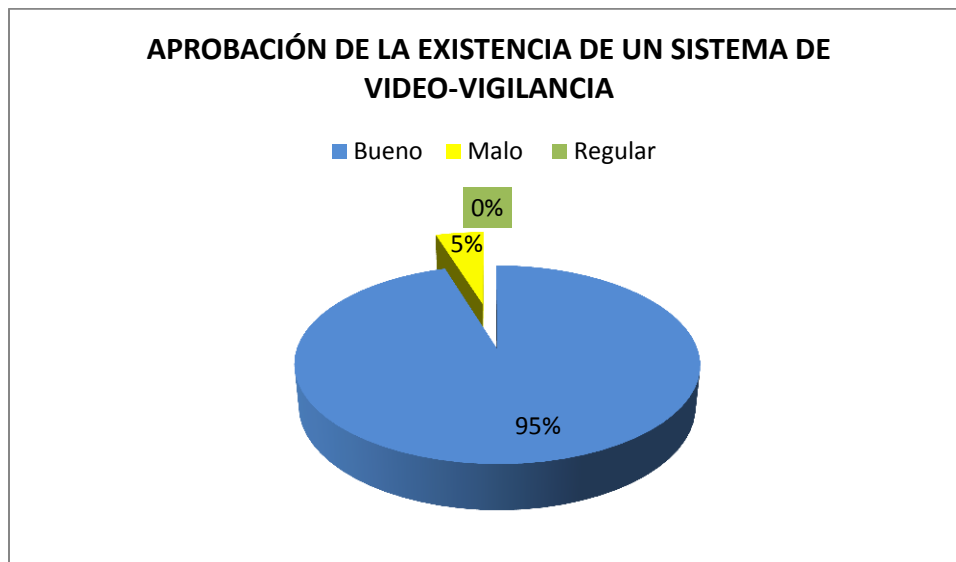


Figura N° 4. 18 Aprobación de la existencia de un sistema de video-vigilancia en el GADMT
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: Apreciando la figura N° 4.18 se resuelve que el 95% de los encuestados aprueba la existencia de un sistema de video-vigilancia calificándolo como bueno, el 5% constituyéndose un porcentaje mínimo desapruaba dicha propuesta.

Los empleados administrativos en su mayoría están de acuerdo con la existencia de una red de video-vigilancia en el GADMT, siendo conscientes de la infinidad de ventajas que proveerá.

- **Pregunta 10**

¿Cómo considera la velocidad de internet del GADMT?

Item	Frecuencia	Porcentaje (%)
Buena	11	52 %
Aceptable	8	38 %
Mala	2	10 %
Regular	0	0 %
Total	21	100 %

Tabla N° 4. 23 Velocidad del internet en el GADMT
Elaborado por: El Investigador

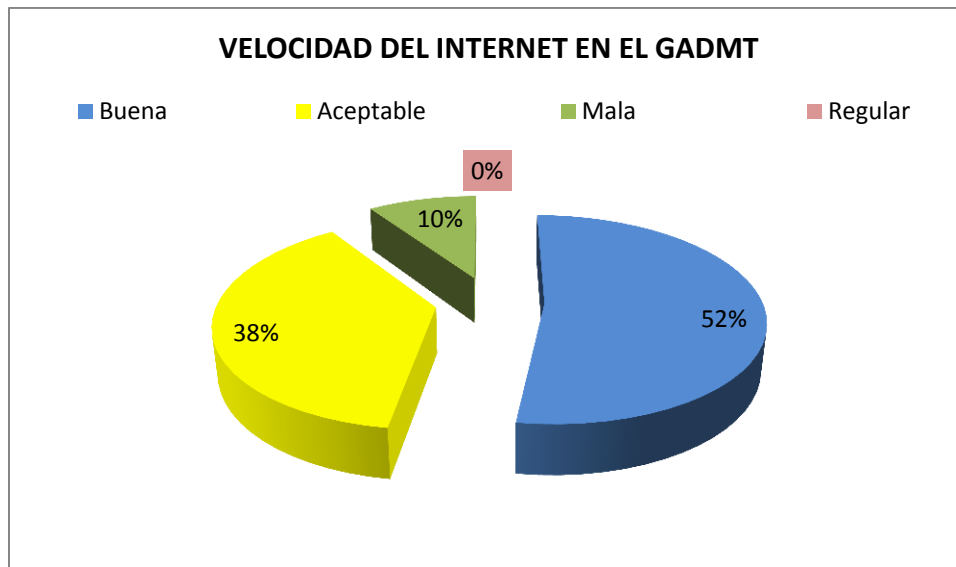


Figura N° 4. 19 Velocidad del internet en el GADMT
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: De lo indicado en la figura N° 4.19 se precisa que el 52% de los empleados de la dirección administrativa consideran buena la velocidad del internet del GADMT, el 38% lo define como aceptable, un mínimo porcentaje correspondiente al 10% determina como malo.

Analizando los resultados obtenidos se concluye que la velocidad de internet del Gobierno Municipal de Tulcán es óptima, situación que garantizará la calidad y fluidez de la información procedente de las cámaras de un sistema de video-vigilancia IP.

- **Pregunta 11**

¿Cuál es el tipo de información por internet al cual accede?

Item	Frecuencia	Porcentaje (%)
Música	2	7 %
Video	5	19 %
Datos	20	74 %
Total	27	100 %

Tabla N° 4. 24 Tipo de información al cual acceden los empleados del GADMT
Elaborado por: El Investigador

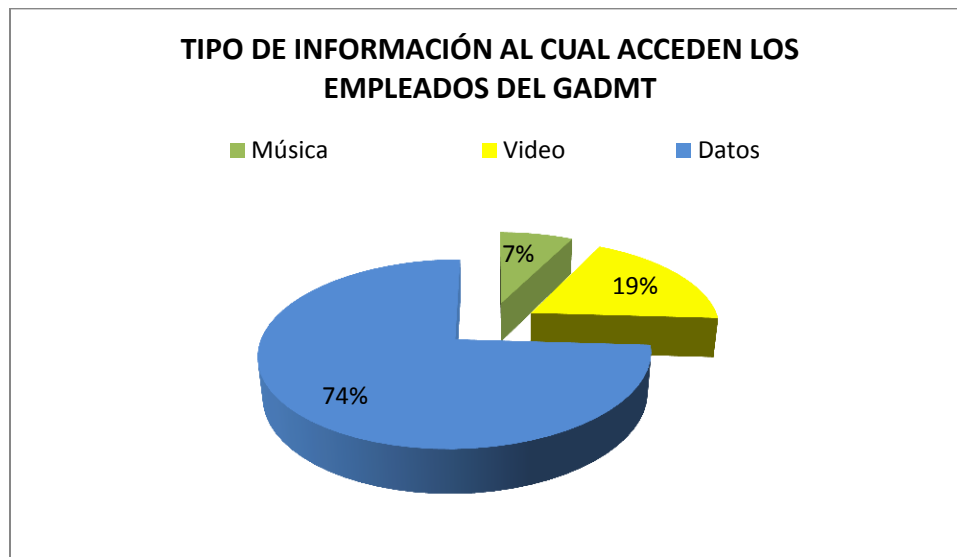


Figura N° 4. 20 Tipo de información al cual acceden los empleados del GADMT
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: De la presente pregunta de selección múltiple realizada a los trabajadores administrativos y examinando su resultado en la figura N° 4.20 se puede manifestar que el tipo de información al cual accede en su mayoría el personal son datos obteniéndose un 74% en este ítem, el 19% elige videos y el 7% selecciona música.

Se pone en evidencia que la mayoría de los servidores municipales ingresa al correo municipal, efectuando transferencias de archivos, recibiendo disposiciones y circulares de determinadas áreas del GADMT, realizando consultas técnicas. Siendo mínimo pero no menos necesario el acceso a videos y música con un fin justificado, el hecho de utilizar información que requiere de menor ancho de banda disminuye el tráfico de red haciendo técnicamente factible la ejecución de un sistema de vigilancia IP.

- **Pregunta 12**

¿Con que frecuencia usa internet?

Item	Frecuencia	Porcentaje (%)
Mucho	20	95 %
Poco	1	5 %
Nada	0	0 %
Total	21	100 %

Tabla N° 4. 25 Frecuencia del uso de internet en el edificio Municipal
Elaborado por: El Investigador

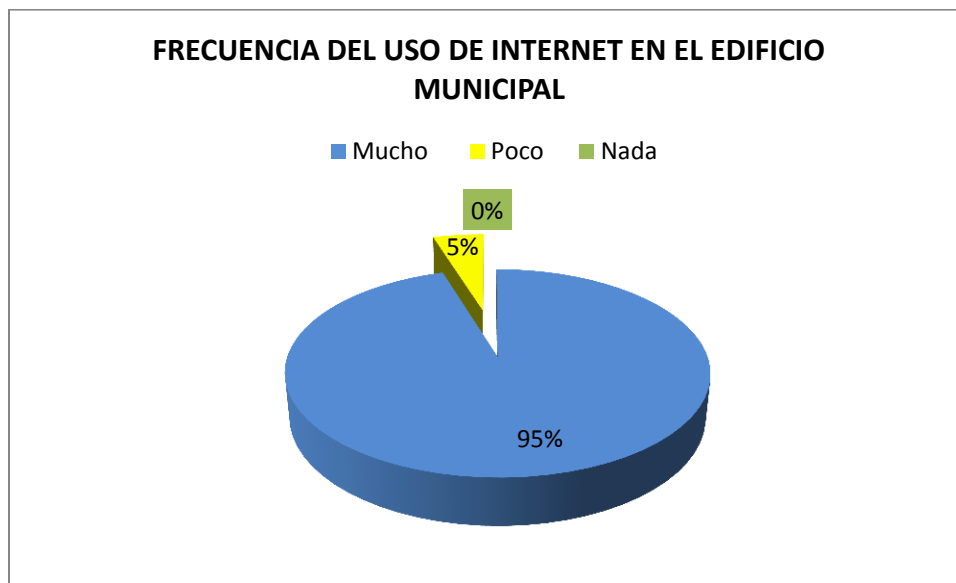


Figura N° 4. 21 Frecuencia del uso de internet en el edificio Municipal.
Fuente: Empleados de la Dirección de Gestión Administrativa del GADMT.
Elaborado por: El Investigador

Análisis e Interpretación: Examinando la figura N° 4.21 se determina la frecuencia del uso de internet por parte de los empleados de Gestión Administrativa, el cual refleja la situación actual de la totalidad de servidores del edificio municipal, obteniéndose un 95% que expone su uso frecuente, el 5% lo establece como poco y ninguno de ellos 0% indica que puede prescindir de este servicio.

El internet constituye una importante herramienta de trabajo en el GADMT, siendo de uso permanente. Tomándose en cuenta que el tipo de información habitualmente manejada son datos.

4.4 ENTREVISTA

El presente análisis de resultados es producto de la entrevista realizada a la Directora de la Unidad de Informática, Ingeniera Magaly Rodríguez.

4.4.1 Objetivos:

- Conocer la situación actual de la red del GADMT.
- Determinar la factibilidad técnica y requerimientos para un sistema de video-vigilancia IP.
- Establecer la importancia de un sistema de video-vigilancia en la institución municipal.

4.4.2 Desarrollo de preguntas y repuestas:

1. ¿Podría proporcionar una breve explicación a cerca de la red del Municipio?

- El proveedor de internet: CNT
- Medio de transmisión: Fibra Óptica.

2. ¿Como considera usted la velocidad del internet proporcionado en el edificio del GADMT?

Buena, considerando que son pocos usuarios y el ancho de banda es de 8 Mbits/segundo, siendo el adecuado para las actividades en el GADMT.

3. ¿Cuál es la situación de la red municipal en lo referente al tráfico de datos?

El tráfico de datos es bajo ya que únicamente se maneja bases de datos y acceso controlado a internet.

4. Tomando en cuenta la situación actual de la red, ¿Existen propuestas o medidas a tomarse para un mejor desempeño de la misma?

Si, en cuanto a cambio tecnológico y restructuración de cableado de acuerdo a las normativas y estándares respectivos.

5. ¿De qué forma se realiza la asignación de IP's para cada punto de red de la institución? (fijas-dinámicas)

Por DHCP, manteniendo fijas las IP que poseen privilegios para mayor facilidad en cuanto a configuración.

6. ¿Qué páginas web son permitidas a cada usuario de la red? (existen privilegios)

De acuerdo a un estudio realizado de las páginas web y herramientas que requiere cada Unidad Operativa del Gobierno Autónomo Descentralizado Municipal de Tulcán, a cada usuario se le ha asignado la capacidad de acceso necesario para su buen desempeño laboral.

7. ¿Cuál es su percepción a cerca de los beneficios y ventajas que ofrece un sistema de vigilancia que permita el acceso remoto?

- Tener acceso desde cualquier lugar y horario.
- Seguridad
- Monitoreo permanente.

8. ¿Cuán importante considera usted la existencia de un sistema de video-vigilancia en una institución pública?

Es muy importante contar con un mecanismo que proporcione seguridad. Dedicado a evitar perdidas de equipos y materiales en sitios que sean vulnerables a la seguridad.

9. ¿Estaría de acuerdo con que la entidad municipal cuente con un sistema de video-vigilancia IP?

Si, sería un gran aporte para salvaguardar la integridad de la institución. El cual contribuiría al control continuo de seguridad y recopilación de imágenes o sucesos que se presenten en la institución.

10. ¿Cuáles son las expectativas que debe cumplir un sistema de video-vigilancia en la institución?

- Acceso remoto
- Sin interrupciones
- Monitoreo desde cualquier lugar
- Alto nivel de sensibilidad lumínica para interiores y exteriores, visión diurna y nocturna, ajuste de la distancia.
- Gestión de seguridad institucional.
- Acceso a puntos principales del edificio
- Acceso a las oficinas

11. ¿A su criterio cuáles serían los principales aspectos que requieren controlarse con un sistema de video-vigilancia en las oficinas del GADMT?

- Seguridad
- Equipos y bienes institucionales.

12. ¿A su parecer cuáles son las oficinas del edificio Municipal que requieren de un sistema de video-vigilancia?

En todas las dependencias. Porque el personal de seguridad no es suficiente para dar cobertura a todas las instalaciones, lo cual requiere un sobreesfuerzo por parte de los vigilantes y en consecuencia aumenta el estado de alerta en la institución.

13. ¿Alguna recomendación en cuanto al tipo de cámaras a emplearse en un sistema de video-vigilancia IP para el GADMT?

Equipos que tengan la mayor cantidad de aplicaciones útiles para la municipalidad.

Características:

- Movimiento horizontal, vertical, zoom
- Visión diurna y nocturna
- Soporte integrado de audio bidireccional
- Cámara de alta resolución
- Detección de movimiento integrado

4.4.3 Análisis e interpretación de la información obtenida:

La ejecución de la entrevista permite corroborar los resultados obtenidos en las encuestas, proporcionando información a cerca de la situación actual de la red del Gobierno Autónomo Descentralizado Municipal de Tulcán, reiterar la necesidad de contar con un sistema de video-vigilancia y determinar la factibilidad de ser implementada.

La Ingeniera Magaly Rodríguez indicó que actualmente la red municipal cuenta con un ancho de banda de 8 Mbps proporcionado por la CNT el cual es el suficiente para las actividades hasta hoy realizadas, menciona además que el tráfico de datos generado en la institución es bajo. Frente a estos antecedentes es importante mencionar que no se descarta la posibilidad de mejorar el desempeño de la misma usando nuevas tecnologías, ampliando y rediseñando la red a futuro.

En lo referente al tipo de páginas web permitidas a cada usuario de la red señaló que están habilitadas únicamente las necesarias para el desempeño laboral y actividad de cada Unidad, tal es el caso de los videos, música y redes sociales que solamente son facultadas a un número limitado de dependencias como lo es la Unidad de Comunicaciones y Protocolo. La asignación de IP's se la realiza por DHCP manteniendo exclusivamente fijas aquellas que gozan de privilegios, es decir requieren de internet sin restricciones.

Estableció la importancia y ventajas de contar con una red de video-vigilancia IP en el GADMT, priorizando el acceso remoto desde cualquier lugar y horario. Además estipuló que todas las dependencias del edificio requieren de un mecanismo de inspección principalmente para el control de los equipos y bienes institucionales.

Frente a las referencias de la red ya antes mencionadas asiente que es factible la implementación de dicho sistema electrónico de seguridad, para lo cual recomienda realizar el diseño tomando en cuenta equipos con la mayor cantidad de aplicaciones y que cumplan las expectativas de un sistema sin interrupciones.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Actualmente el Gobierno Autónomo Descentralizado Municipal de Tulcán cuenta con un servicio tradicional de vigilancia, ya que dispone de guardias de seguridad que son los encargados de proteger la integridad física de las personas y los bienes materiales de la institución.
- Los servidores Municipales están de acuerdo que la información procedente de un sistema de vigilancia sea visualizada, de manera que permita monitorear en tiempo real las instalaciones del edificio municipal.
- El diseño de una Red de Video-vigilancia para el acceso remoto de las Unidades Operativas de la municipalidad es de gran importancia., ya que actualmente se cuenta con un sistema de vigilancia que posee limitaciones en cuanto se refiere al control de actividades que necesitan supervisión continua.
- La existencia de un mecanismo de Video-vigilancia IP aportará con un amplio nivel de confianza para el personal, respecto al monitoreo y control de sucesos ocurridos en el Gobierno Municipal.
- La red del Gobierno Autónomo Descentralizado Municipal de Tulcán esta conformada por 162 puntos de red en uso y acceso a internet mediante fibra óptica con un ancho de banda de 8 Mbps suministrados por la CNT.

- De acuerdo al análisis realizado el tráfico de la red LAN y WLAN de la Institución es bajo por lo que su desempeño es óptimo, con tiempos de respuestas favorables y un bajo índice de problemas potenciales.

5.2 RECOMENDACIONES

- Se sugiere realizar el diseño de una Red de video-vigilancia IP tomando en cuenta los requerimientos, necesidades de vigilancia y seguridad del Gobierno Autónomo Descentralizado Municipal de Tulcán.
- Los fines a alcanzarse con el presente proyecto deben ser llevados a cabo conjuntamente con la Unidad Operacional de Sistemas Informáticos y Redes, la cual es la responsable del impulso y desarrollo tecnológico de la Institución.
- Se deberá realizar un análisis acerca de los requerimientos de red, ancho de banda y equipos a utilizarse, los cuales deberán cumplir con ciertas características específicas para proporcionar un servicio de calidad.
- Informar a los servidores municipales acerca del objetivo que se persigue con el sistema de vigilancia IP y los alcances que tendrá el mismo, para de este modo despejar las dudas que el advenimiento de una nueva tecnología ocasiona.
- Por motivos de seguridad y rendimiento es aconsejable configurar una VLAN, de este modo sólo los usuarios de un grupo específico podrán acceder a la administración de la red de vigilancia, para lo cual es recomendable llevar un registro o documentación de la misma.

CAPÍTULO VI

PROPUESTA

6.1 DATOS INFORMATIVOS

- **Tema**

Red de Video-vigilancia mediante tecnología IP para el acceso remoto de las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán.

- **Institución Ejecutora:**

Universidad Técnica de Ambato (Facultad de Ingeniería en Sistemas, Electrónica e Industrial)

- **Beneficiarios:**

Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán.

- **Ubicación:**

Provincia del Carchi, Cantón Tulcán.

- **Equipo Técnico responsable:**

Investigador: Jessica Ramos

Tutor: Ing. Julio Cuji

Entidad: Universidad Técnica de Ambato, en la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

6.2 ANTECEDENTES

El Gobierno Autónomo Descentralizado Municipal de Tulcán requiere de un sistema de vigilancia que se adapte e interactúe con su red actual, es por ello que el pilar del presente proyecto se fundamenta en una red de seguridad basada en tecnología IP, ya que presenta grandes prestaciones, como la convergencia de voz, vídeo y datos, capacidad de procesamiento y almacenamiento, acceso a sitios remotos, lo cual confiere al administrador de red y al personal encargado la capacidad para tomar de decisiones de una forma rápida y certera.

En apartados anteriores se detallaron las necesidades fundamentales de la municipalidad debido a la carencia de un sistema que garantice accesibilidad y seguridad permanente, por lo que resulta de gran beneficio el desarrollo del diseño propuesto en el presente capítulo.

6.3 JUSTIFICACIÓN

La realización del diseño de una Red de Video-vigilancia mediante tecnología IP para el acceso remoto de las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán, se encuentra fundamentada en las nuevas herramientas y posibilidades para optimizar la prevención de pérdidas y el desempeño de la institución. Permitiendo capturar vídeo como información digital y acceder a él desde cualquier parte a través de una red basada en IP, facultando la visualización, análisis y gestión de las grabaciones.

Por tal motivo, examinando los resultados, requerimientos y necesidades obtenidos en capítulos anteriores, se plantea un proyecto de diseño que aportará al desarrollo e impulso tecnológico de la Municipalidad.

La inteligencia integrada en las nuevas tecnologías permite el aprovechamiento de la infraestructura existente, escalabilidad, estándares abiertos, administración de software, instalación sencilla, posibilidad de aumentar la capacidad y rendimiento.

El uso de las cámaras digitales ofrece vídeo con mejor nitidez, una mayor cobertura y mejores capacidades de zoom. Además, su instalación es menos costosa, los nuevos modelos no necesitan toma de corriente. Mediante la tecnología de Alimentación eléctrica a través de Ethernet (PoE) puede alimentar una cámara con el mismo cable que se utiliza para conectarla a la red. PoE también facilita la aplicación de sistemas de alimentación ininterrumpida (SAI) para garantizar el funcionamiento las 24 horas del día y los 7 días de la semana.

6.4 OBJETIVOS

6.4.1 OBJETIVO GENERAL

Diseño de una red de Video-vigilancia mediante tecnología IP para el acceso remoto de las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán.

6.4.2 OBJETIVOS ESPECÍFICOS

- Analizar los sitios estratégicos del edificio municipal para el diseño de la red de vigilancia.
- Diseñar una VLAN que permita proporcionar seguridad y rendimiento a la red.
- Establecer la factibilidad técnica y económica para una futura implementación de la red de Video-vigilancia mediante tecnología IP.

6.5 ANÁLISIS DE FACTIBILIDAD

6.5.1 FACTIBILIDAD TÉCNICA

La factibilidad técnica se fundamentó en la evaluación de la tecnología existente en el Gobierno Autónomo Descentralizado Municipal de Tulcán, obteniendo como consecuencia de la investigación una amplia documentación técnica de los equipos de red e informáticos existentes, así como la distribución de puntos de red, el estado de tráfico y servicios brindados.

Mediante la información extraída se pudieron determinar los parámetros del diseño para una propuesta que se ajuste a los requerimientos y necesidades de la municipalidad, puntualizando la factibilidad en cuanto al aspecto técnico del proyecto, ya que mediante estos antecedentes se logró situar la mejor opción en cuanto a nuevas e idóneas técnicas de video-vigilancia existentes en el mercado actual.

6.5.2 FACTIBILIDAD OPERATIVA

A través del sondeo realizado en cuanto a requerimientos, peticiones de empleados, personal administrativo y directivos del GADMT se ratifica la necesidad de contar con un sistema de vigilancia que proporcione seguridad las 24 horas del día a la institución. Se cuenta con resultados favorables de entrevistas y una encuesta realizada a la Directora de la Unidad de Informática, los mismos que respaldan los juicios mencionados y establecen la factibilidad operativa, demostrándose que no se presenta oposición al cambio y a la implementación de nuevas tecnologías.

6.5.3 FACTIBILIDAD ECONÓMICA

La unidad de Informática anualmente presenta planes de trabajo en beneficio del Gobierno Autónomo Descentralizado Municipal de Tulcán, los costos de los mismos son atribuidos a la partida presupuestaria de equipos informáticos y entregados a la dirección de dicha unidad.

El presente proyecto cuenta con el apoyo de la directora de sistemas informáticos, quien es consiente de la importancia del desarrollo y diseño de la red ip de video-vigilancia, por lo que el proyecto es viable económicamente.

6.6 FUNDAMENTACIÓN CIENTÍFICO – TÉCNICA

6.6.1 VIDEO EN RED

6.6.1.1 Visión general de un sistema de video en red

El vídeo en red, utiliza una red IP inalámbrica o con cable como red troncal para transportar vídeo y audio digital, y otros datos. Cuando se aplica la tecnología de alimentación a través de Ethernet (PoE), la red también se puede utilizar para transportar alimentación a los productos de vídeo en red.

Un sistema de vídeo en red permite supervisar vídeo y grabarlo desde cualquier lugar de la red, tanto si se trata por ejemplo de una red de área local (LAN) o de una red de área extensa (WAN) como Internet.

En la figura N° 6.1 se observa un sistema de video en red que esta integrado de diferentes componentes, como las cámaras de red, los codificadores de vídeo y el software de gestión de vídeo. Los demás dispositivos, incluidos la red, el almacenamiento y los servidores, forman parte del equipo de tecnología IP estándar.



Figura N° 6. 1 Sistema de video en red

Fuente: http://www.axis.com/es/products/video/about_networkvideo/network_video.htm

Los elementos básicos de un sistema de vídeo en red son la cámara de red, el codificador de vídeo (que se utiliza para la conexión a cámaras analógicas), la red, el servidor y el almacenamiento, así como el software de gestión de vídeo, dichos elementos pueden ser apreciados en la figura .Como la cámara de red y el codificador

de vídeo son equipos basados en ordenadores, cuentan con capacidades que no pueden compararse con las de una cámara CCTV analógica.

Los componentes de red, servidor y almacenamiento forman parte del equipo de tecnología IP estándar. La posibilidad de utilizar un equipo listo para su uso común constituye una de las ventajas principales del vídeo en red.

6.6.1.2 Ventajas de un sistema de video-vigilancia de red digital

El sistema de video-vigilancia de red digital ofrece toda una serie de ventajas y funcionalidades avanzadas:

- *Accesibilidad remota:* acceder de forma remota a cámaras de red, permite a diferentes usuarios autorizados visualizar vídeo en vivo y grabado en cualquier momento y desde prácticamente cualquier ubicación en red del mundo.
- *Alta calidad de imagen:* En una aplicación de video-vigilancia, es esencial una alta calidad de imagen para poder capturar con claridad un incidente en curso e identificar a las personas u objetos implicados.
- *Gestión de eventos y vídeo inteligente:* Las cámaras de red avanzadas con inteligencia integrada pueden reducir la cantidad de grabaciones sin interés y permitir respuestas programadas. Las cámaras de red incluyen funciones integradas como la detección de movimiento por vídeo, alarma de detección de audio, conexiones de entrada y salida (E/S) y funcionalidades de gestión de alarmas y eventos.
- *Integración sencilla y preparada para el futuro:* Los productos de vídeo en red basados en estándares abiertos se pueden integrar fácilmente con sistemas de información basados en ordenadores y Ethernet, sistemas de audio o de seguridad y otros dispositivos digitales.
- *Escalabilidad y flexibilidad:* se puede añadir al sistema cualquier cantidad de productos de vídeo en red sin que ello suponga cambios significativos o costosos para la infraestructura de red.
- *Rentabilidad de la inversión:* Un sistema de vigilancia IP tiene normalmente un coste total de propiedad inferior al de un sistema CCTV analógico tradicional.

Una infraestructura de red IP a menudo ya está implementada y se utiliza para otras aplicaciones dentro de una organización, por lo que una aplicación de vídeo en red puede aprovechar la infraestructura existente. Las redes basadas en IP y las opciones inalámbricas constituyen además alternativas mucho menos caras que el cableado coaxial y de fibra tradicionales utilizados por un sistema CCTV analógico.

6.6.1.3 Directrices para seleccionar una cámara de red

Dada la variedad de cámaras de red disponibles, resulta útil disponer de algunas directrices para seleccionar el tipo que mejor se adapte a sus necesidades.

- Definir el objetivo de video-vigilancia
- Zona de cobertura
- Entorno interior o exterior
- Vigilancia visible u oculta
- Calidad de imagen
- Resolución
- Compresión
- Audio
- Gestión de eventos y vídeo inteligente
- Funcionalidades de red
- Interfaz abierta y aplicaciones de software

6.6.2 TECNOLOGÍAS DE RED

6.6.2.1 Red de área local y Ethernet

La tecnología LAN más utilizada es la Ethernet y está especificada en una norma llamada IEEE 802.3. Ethernet utiliza una topología en estrella en la que los nodos individuales (dispositivos) están conectados unos con otros a través de un equipo de red activo como un conmutador.

El medio de transmisión físico para una LAN por cable implica cables, principalmente de par trenzado, o bien, fibra óptica. En función del tipo de cables que se utilicen, actualmente las velocidades de datos pueden oscilar entre 100 Mbit/s y 10.000 Mbit/s.

Por regla general, las redes siempre deben tener más capacidad de la que se necesita. Para preparar una red para el futuro es una buena idea diseñar una red que solamente utilice el 30% de su capacidad.

6.6.2.2 Tipos de redes Ethernet

a. Fast Ethernet

Fast Ethernet hace referencia a una red Ethernet que puede transferir datos a una velocidad de 100 Mbit/s. Se puede basar en cable de par trenzado o de fibra óptica. (La antigua Ethernet de 10 Mbit/s todavía se instala y se usa, pero este tipo de redes no proporcionan el ancho de banda necesario para algunas aplicaciones de vídeo en red).

La mayoría de dispositivos que se conectan a una red, están equipados con una interfaz Ethernet 100BASE-TX/10BASE-T. El tipo de cable de par trenzado compatible con Fast Ethernet se denomina Cat-5.

b. Gigabit Ethernet

Gigabit Ethernet, que también se puede basar en cable de par trenzado o de fibra óptica, proporciona una velocidad de transferencia de datos de 1.000 Mbit/s (1 Gbit/s) y es cada vez más frecuente. El tipo de cable de par trenzado compatible con Gigabit Ethernet es el Cat-5e, en el que los cuatro pares de cables trenzados se utilizan para alcanzar la alta velocidad de transferencia de datos. Para los sistemas de vídeo en red se recomienda Cat-5e u otras categorías de cable superiores. La mayoría de interfaces son compatibles con las versiones anteriores de Ethernet 10 Mbit/s y 100 Mbit/s y se conocen como interfaces 10/100/1000.

c. 10 Gigabit Ethernet

10 Gigabit Ethernet es la última generación, proporciona una velocidad de transferencia de datos de 10 Gbit/s (10.000 Mbit/s) y se puede utilizar con fibra óptica o cable de par

trenzado. Con una solución de par trenzado se requiere un cable de altísima calidad, Cat-6a o Cat-7. La Ethernet de 10 Gbit/s se utiliza principalmente como red troncal en aplicaciones de gama alta que requieren una velocidad de transferencia de datos muy alta.

6.6.2.3 Alimentación a través de Ethernet

La Alimentación a través de Ethernet (PoE) permite proveer de energía a los dispositivos conectados a una red Ethernet usando el mismo cable que para la comunicación de datos.

La principal ventaja de PoE es el ahorro de costes que conlleva. No es necesario contratar a un electricista ni instalar una línea de alimentación separada. Esto supone una ventaja, sobre todo en zonas de difícil acceso. El hecho de que no sea necesario instalar otro cable de alimentación puede suponer un ahorro de varios centenares de dólares, dependiendo de la ubicación de la cámara. PoE también facilita el hecho de cambiar la ubicación de la cámara o añadir otras cámaras al sistema de videovigilancia.

Además, aumenta la seguridad del sistema de vídeo. Un sistema de videovigilancia con PoE se puede alimentar desde una sala de servidores, que a menudo está protegida con un Sistema de alimentación ininterrumpida. Esto significa que el sistema de videovigilancia puede funcionar incluso durante un apagón. Por las ventajas que tiene PoE, se recomienda usarla en tantos dispositivos como sea posible.

a. Norma 802.3af y High PoE

Hoy en día, la mayoría de dispositivos PoE cumplen con la norma IEEE 802.3af, que se publicó en 2003. Esta norma utiliza cables estándares Cat-5 o superiores y asegura que la transferencia de datos no se vea afectada. En dicha norma, al dispositivo que proporciona la energía se le llama equipo de suministro eléctrico (PSE). Éste puede ser un conmutador o midspan habilitado para PoE. El dispositivo que recibe la energía se conoce como dispositivo alimentado (PD).

Según la IEEE 802.3af, un PSE proporciona un voltaje de 48 V CC con una potencia máxima de 15,4 W por puerto. Pero, teniendo en cuenta que en un cable de par

trenzado hay pérdida de potencia, un PD sólo garantiza 12,95 W. La norma IEEE 802.3 especifica varias categorías de rendimiento para los PD. En la tabla N° 6.1 se establecen las clasificaciones de potencia según IEEE 802.3af.

Clase	Nivel de potencia mínimo en PSE	Nivel de potencia máximo de un PD	Uso
0	15.4 W	0.44 W - 12.95 W	predeterminado
1	4.0 W	0.44 W - 3.84 W	opcional
2	7.0 W	3.84 W - 6.49 W	opcional
3	15.4 W	6.49 W - 12.95 W	opcional
4	Tratado como clase 0		Reservado para usos futuros

Tabla N° 6. 1 Clasificaciones de potencia según IEEE 802.3af

Fuente: http://www.axis.com/es/products/video/about_networkvideo/network_video.htm

6.6.3 SISTEMAS DE GESTIÓN DE VÍDEO

6.6.3.1 Plataformas de hardware

Existen dos tipos diferentes de plataformas de hardware para un sistema de gestión de vídeo en red:

a. Plataforma de servidor de PC

Una solución de gestión de vídeo basada en una plataforma de servidor de PC incluye servidores de PC y equipos de almacenamiento que se pueden seleccionar directamente con el fin de obtener un rendimiento superior para el diseño específico del sistema. Una plataforma abierta de estas características facilita la opción de añadir funcionalidades al sistema, como un almacenamiento incrementado o externo, cortafuegos, protección contra virus y algoritmos de vídeo inteligentes, en paralelo con un programa de software de gestión de vídeo.

Una plataforma de servidor de PC también se puede ampliar, permitiendo añadir cuantos productos de vídeo en red sean necesarios. El hardware del sistema se puede ampliar o actualizar para satisfacer nuevas necesidades de rendimiento. Esto permite

a los usuarios gestionar vídeo y otros controles de edificios mediante un simple programa e interfaz de usuario. En la figura N° 6.2 se muestra un sistema de video-vigilancia en red basado en una plataforma abierta de servidor de PC



Figura N° 6. 2 Sistema de video-vigilancia en red basado en una plataforma abierta de servidor de PC

Fuente: http://www.axis.com/es/products/video/about_networkvideo/platforms.htm

b. Plataforma NVR

Un grabador de vídeo en red se presenta como una caja de hardware con funcionalidades de gestión de vídeo preinstaladas. En este sentido, un NVR es parecido a un DVR. Algunos DVR, también incluyen una función NVR, es decir, la capacidad también de grabar vídeo basado en red.

En la figura N° 6.3 se indica un sistema de video-vigilancia en red que utiliza un NVR, el cual normalmente está patentado y diseñado específicamente para gestión de vídeo. Está dedicado a sus tareas específicas de grabación, análisis y reproducción de vídeo en red y normalmente no permite que ninguna otra aplicación se conecte a éste. El sistema operativo puede ser Windows, UNIX/Linux o patentado.

Un NVR está diseñado para ofrecer un rendimiento óptimo para un conjunto de cámaras y normalmente es menos escalable que un sistema basado en servidor de PC. Esto permite que la unidad resulte más adecuada para sistemas más pequeños donde

el número de cámaras se encuentra dentro de los límites de la capacidad de diseño de un NVR. Normalmente, un NVR es más fácil de instalar que un sistema basado en una plataforma de servidor de PC.



Figura N° 6. 3 Sistema de video-vigilancia en red que utiliza un NVR
Fuente: http://www.axis.com/es/products/video/about_networkvideo/platforms.htm

6.6.4 CONSIDERACIONES SOBRE ANCHO DE BANDA Y ALMACENAMIENTO

Los requisitos de ancho de banda y almacenamiento de red son aspectos importantes en el diseño de sistemas de video-vigilancia. Entre los factores se incluyen el número de cámaras, la resolución de imagen utilizada, el tipo y relación de compresión, frecuencias de imagen y complejidad de escenas. Este capítulo ofrece algunas pautas en el diseño de un sistema, junto con información sobre soluciones de almacenamiento y varias configuraciones de sistema.

Los productos de vídeo en red utilizan el ancho de banda de red y el espacio de almacenamiento basándose en sus configuraciones. Esto depende de lo siguiente:

- Número de cámaras
- Si la grabación será continua o basada en eventos
- Número de horas al día que la cámara estará grabando
- Imágenes por segundo
- Resolución de imagen
- Tipo de compresión de vídeo: Motion JPEG, MPEG-4, H.264

- Escena: Complejidad de imagen (p. ej. pared gris o un bosque), condiciones de luz y cantidad de movimiento (entorno de oficina o estaciones de tren con mucha gente)
- Cuanto tiempo deben almacenarse los datos

6.6.4.1 Requerimiento del sistema

La velocidad requerida por el conjunto de cámaras no se puede calcular de manera determinística, esto debido a que el tráfico de datos generado por cada cámara varía de acuerdo a una serie de factores como se registra en los listados de la tabla N° 6.2.

Factor	Descripción	Ejemplo
Método de compresión de Video	Típica temporal o compresión espacial	MPEG-4, M-JPEG, Wavelet, y MPEG-2
Rata de Imágenes	Imágenes por seg.	1-30 IPS
Resolución de Imágenes	Número de píxeles horizontales y verticales	QCIF, CIF, 2CIF, 4CIF (conocido como full D1)
Actividad en la escena	Cantidad de actividad en el campo de visión de la cámara	Baja, media y alta
Tiempo muerto	Fracción de tiempo en la que no hay movimiento (es importante para los algoritmos de compresión temporal como MPEG-4, ya que se puede consumir ancho de banda durante este tiempo)	8:00 p.m. – 6:00 a.m. Lunes - Viernes, todo el Sábado y Domingo, llega a cerca del 50% del tiempo muerto

Tabla N° 6. 2 Factores que varían la tasa de bits

Fuente: http://www.boschsecurity.com.mx/_archivos_productos_sitios_la/boletines_informativos/ebrief/2006/Estimando_Ancho_de_Banda.pdf

De todos los factores descritos en la tabla anterior, solo la Actividad en la Escena es impredecible y no la podemos configurar de acuerdo a nuestra conveniencia, como es el caso de los factores restantes. Adicionalmente, la actividad en escena afecta en gran medida al método de compresión MPEG-4 utilizado en las cámaras, de tal

forma, cuando la actividad en escena es grande, MPEG-4 genera un tráfico mayor comparado al generado cuando la actividad de la escena es nula.

Es importante conocer cuál es el requerimiento de velocidad de cada cámara en distintas circunstancias y horas, de esta manera se podrá calcular de forma aproximada el consumo máximo y mínimo del sistema en su totalidad, con el fin de no sobrepasar el recurso limitado de ancho de banda que nos ofrece la red. Si la capacidad de la red se ocupa en su totalidad, el sistema puede presentar:

Pérdida de imágenes, ocasionando un video entrecortado.

La resolución del video puede caer a niveles en que la imagen sea poco clara.

El video se puede congelar completamente y se puede perder la conexión.

6.6.4.2 Requisitos de ancho de banda

En un sistema de vigilancia reducido compuesto de 8 a 10 cámaras, se puede utilizar un conmutador de red básico de 100 Megabits (Mbit) sin tener que considerar limitaciones de ancho de banda. La mayoría de las empresas pueden implementar un sistema de vigilancia de este tamaño utilizando la red que ya tienen.

Cuando se implementan 10 o más cámaras, la carga de red se puede calcular con algunas reglas generales:

- Una cámara configurada para ofrecer imágenes de alta calidad a altas frecuencias de imagen utilizará aproximadamente de 2 a 3 Mbit/s del ancho de banda disponible de la red.
- De 12 a 15 cámaras, considere el uso de un conmutador con una red troncal de un gigabit. Si se utiliza un conmutador compatible con un gigabit, el servidor que ejecuta el software de gestión de vídeo debería tener un adaptador para redes de un gigabit instalado.

Las tecnologías que permiten la gestión del consumo de ancho de banda incluyen el uso de VLAN en una red conmutada, Calidad de Servicio y grabaciones basadas en eventos.

6.6.4.3 Determinación aproximada del Ancho de Banda requerido

Para obtener una determinación aproximada del ancho de banda requerido por el sistema en su totalidad, se analizará el tráfico generado por una de las cámaras con restricción en fps (frames per second) y resolución, con un nivel de actividad en escena Medio. De esta manera, se multiplicará este requerimiento por el total de las cámaras, obteniendo así una aproximación del ancho de banda generado por el sistema.

La reconocida empresa BOSCH en un Documento de Referencia titulado “Estimando el Ancho de Banda” muestra una tabla de valores estimados de las tasas de bits generadas en el formato de compresión MPEG-4 . Los valores mostrados en la tabla N° 6.3 son estimados y fueron obtenidos de una gran cantidad de proyectos previos realizados; es decir son el resultado de la experiencia.

Resolución	IPS	Nivel de Actividad	Rata de Bits (Kbps)
CIF	3	Medio	160
CIF	7	Medio	185
CIF	15	Medio	200
CIF	30	Medio	500
2 CIF	3	Medio	320
2 CIF	7	Medio	370
2 CIF	15	Medio	400
2 CIF	30	Medio	1,000
4 CIF	3	Medio	640
4 CIF	7	Medio	740
4 CIF	15	Medio	800
4 CIF	30	Medio	2,000

Tabla N° 6. 3 Tasas de bits estimadas para una cámara IP

Fuente:http://www.boschsecurity.com.mx/_archivos_productos_sitios_la/boletines_informativos/ebrief/2006/Estimando_Ancho_de_Banda.pdf

6.6.4.4 Calcular requisitos de almacenamiento

El tipo de compresión de vídeo utilizado es uno de los factores que afectan a los requisitos de almacenamiento. El formato de compresión H.264 es de lejos la técnica de compresión de vídeo más eficiente que existe actualmente. Sin asegurar calidad de imagen, un codificador H.264 puede reducir el tamaño de un archivo de vídeo digital en más de un 80% comparado con el formato Motion JPEG y en más de un 50% con el estándar MPEG-4 (Parte 2). Esto significa que se necesita mucho menos ancho de banda de red y espacio de almacenamiento para un archivo de vídeo H.264. En la siguiente tabla, se proporcionan los cálculos de almacenamiento de muestra del formato de compresión MPEG-4.

a. Cálculo en MPEG-4

Un salón necesita que se graben 3 cámaras por un período de un mes (30 días) a 15 fps, con resoluciones CIF, 2CIF y 4CIF, con tiempos de 24, 12 y 8 horas diarias respectivamente.

Para lo cuál la tabla N° 6.3 sugiere rata de bits de 200 Kbps, 400 Kbps y 800 Kbps.

$$KB/hora = \frac{\text{Velocidad binaria aprox.}}{8} \times 3600s$$

$$MB/hora = \frac{KB/hora}{1000}$$

$$GB/día = \frac{MB/hora \times \text{horas de funcionamiento diarias}}{1000}$$

$$\text{Capacidad de Almacenamiento} = GB/día \times \text{período de almacenamiento}$$

Cámara	Resolución	Velocidad binaria aproximada (Kbps)	Imágenes por segundo	MB/hora	Horas de funcionamiento	GB/día
N°1	CIF	200	15	90	24	2,2
N°2	2 CIF	400	15	180	12	2,2
N°3	4 CIF	800	15	360	8	2,9

Tabla N° 6. 4 Cálculo de la capacidad de almacenamiento de un sistema
Elaborado por: El Investigador

Al realizar los cálculos respectivos como se observa en la tabla N° 6.4, se tiene que la capacidad total de almacenamiento para las 3 cámaras en un mes de almacenamiento es de 219 GB.

6.6.5 VIRTUAL LOCAL AREA NETWORKS (VLANs)

Al diseñar un sistema de vídeo en red, a menudo existe la intención de mantener la red sin contacto con otras redes por motivos tanto de seguridad como de rendimiento. A primera vista, la elección obvia sería construir una red independiente. Aunque esto simplificaría el diseño, los costes de adquisición, instalación y mantenimiento probablemente serían más elevados que si se utilizara una tecnología de red virtual de área local (VLAN).

VLAN es una tecnología que segmenta las redes de forma virtual, una funcionalidad que admiten la mayoría de conmutadores de red. Esto se consigue dividiendo los usuarios de la red en grupos lógicos. Sólo los usuarios de un grupo específico pueden intercambiar datos o acceder a determinados recursos en la red. Si un sistema de vídeo en red se segmenta en una VLAN, sólo los servidores ubicados en dicha LAN podrán acceder a las cámaras de red. Normalmente, las VLAN conforman una solución mejor y más rentable que una red independiente. El protocolo que se utiliza principalmente al configurar VLAN es IEEE 802.1Q, que etiqueta cada marco o paquete con bytes adicionales para indicar a qué red virtual pertenece.

En la figura N° 6.4 las VLAN se configuran en varios conmutadores. Cada LAN se segmenta en VLAN 20 y VLAN 30. Los vínculos entre los conmutadores transportan los datos de las distintas VLAN. Sólo los miembros de la misma VLAN pueden intercambiar datos, ya sea dentro de la misma red o a través de redes distintas. Las VLAN se pueden utilizar para separar una red de vídeo de una red de oficina.

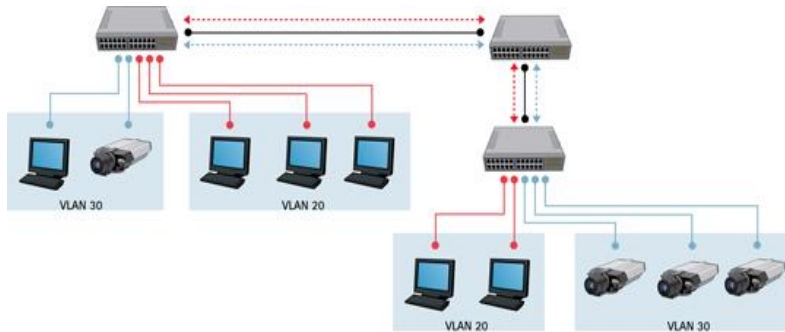


Figura N° 6. 4 Red virtual de área local (VLAN)

Fuente: http://www.axis.com/es/products/video/about_networkvideo/vlan.htm

El acceso a las VLAN está dividido en un rango normal o un rango extendido, las VLAN de rango normal se utilizan en redes de pequeñas y medianas empresas, se identifican por un ID de VLAN entre el 1 y 1005 y las de rango extendido posibilita a los proveedores de servicios que amplien sus infraestructuras a una cantidad de clientes mayor y se identifican mediante un ID de VLAN entre 1006 y 4094.

6.6.5.1 Tipos de VLAN

De acuerdo con la terminología común de las VLAN se clasifican en:

- *VLAN de Datos.*- es la que está configurada sólo para enviar tráfico de datos generado por el usuario, a una VLAN de datos también se le denomina VLAN de usuario.
- *VLAN Predeterminada.*- Es la VLAN a la cual todos los puertos del Switch se asignan cuando el dispositivo inicia, en el caso de los switches cisco por defecto es la VLAN1, otra manera de referirse a la VLAN de predeterminada es aquella que el administrador haya definido como la VLAN a la que se asignan todos los puertos cuando no están en uso.
- *VLAN Nativa.*- En un enlace de trunk 802.1Q existe una VLAN para la que no se emplea el encapsulado 802.1Q sino que las tramas se envían con encapsulado normal Ethernet (sin etiqueta de VLAN). Por defecto en los switches Cisco la VLAN nativa de un puerto en trunk es la VLAN 1, la VLAN nativa sirve como un identificador común en extremos opuestos de un enlace troncal, es aconsejable no utilizar la VLAN1 como la VLAN Nativa.

- *VLAN de administración.*- Es cualquier vlan que el administrador configura para acceder a la administración de un switch, la VLAN1 sirve por defecto como la VLAN de administración si es que no se define otra VLAN para que funcione como tal.

6.6.5.2 Modos de puertos del Switch

- *VLAN estática.*- Los puertos de un switch se asignan manualmente a una VLAN.
- *VLAN dinámica.*- La membresía de una VLAN de puerto dinámico se configura utilizando un servidor especial denominado Servidor de Política de Membresía de VLAN (VMPS).
- *VLAN de voz.*- El puerto se configura para que esté en modo de voz a fin de que pueda admitir un teléfono IP conectado al mismo tiempo de enviar datos.

6.6.5.3 Tipos de puertos

Un switch que utiliza VLANs puede tener dos tipos de puertos: puertos de acceso y puertos de trunk.

- *Puertos de acceso:* este tipo de puertos son los que conectan hosts finales. Trabajan con las tramas clásicas de Ethernet, sin el agregado de las etiquetas de VLAN.
- *Puertos de trunk:* los puertos de trunk tienen una función especial que es la de conectar switches entre sí o un switch con un router. Cuando llega tráfico a un puerto de trunk proveniente desde el propio switch, éste es etiquetado con el identificador de VLAN y enviado por el puerto. El equipo que lo recibe, desencapsula la trama Ethernet (quitándole la etiqueta) y lo envía al puerto que corresponda.

6.6.5.4 Etiquetado de trama

La identificación VLAN es el mecanismo que utilizan los switches para identificar cuál trama pertenece a cierta VLAN y tomar la decisión de envío por la red. Existen dos métodos de etiquetado de trama:

- a **Inter-Switch Link (ISL)**. Este es un protocolo propietario de Cisco y es usado solamente para conexiones Fast Ethernet y Gigabit Ethernet. El enrutamiento ISL puede ser usado sobre puertos de switch, interfaces de routers y tarjetas de interfaz para un servicio troncal.
- b **IEEE 802.1Q**. Creado por el IEEE como un método estándar para el etiquetado de trama. La figura N° 6.5 muestra el formato de trama establecido por el IEEE, en la cual se inserta un campo para identificar la VLAN. Si realiza un enlace troncal entre un switch cisco y un switch de otro fabricante, puede utilizar este método de etiquetado. Características:
 - Soporta hasta 4096 VLANs.
 - Inserta un campo de 4 bytes sin encapsulación
 - El tamaño de la trama final es más pequeña en comparación con ISL.

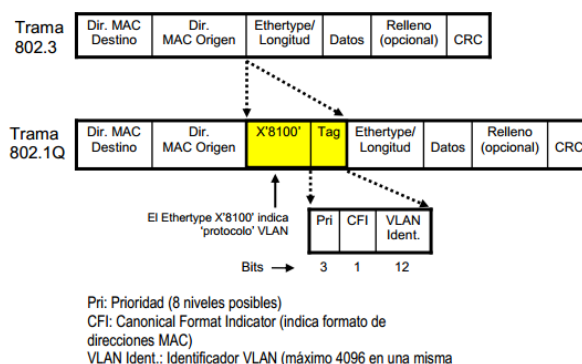


Figura N° 6. 5 Formato de trama 802.1Q

Fuente: <http://cdigital.uv.mx/bitstream/123456789/29518/1/DeiviCesareo.pdf>

6.6.5.5 Configurar un Enlace Troncal

Un enlace troncal es un enlace punto a punto entre dos dispositivos de red, el cual transporta más de una VLAN, como se aprecia en la figura N° 6.6.. Un enlace troncal de VLAN no pertenece a una VLAN específica, sino que es un conducto para las VLAN entre switches y routers.

Existen diferentes modos de enlaces troncales como el 802.1Q y el ISL, en la actualidad sólo se usa el 802.1Q, dado que el ISL es utilizado por las redes antiguas, un puerto de enlace troncal IEEE 802.1Q admite tráfico etiquetado y sin etiquetar, el enlace troncal dinámico DTP es un protocolo propiedad de cisco, DTP administra la negociación del enlace troncal sólo si el puerto en el otro switch se configura en modo de enlace troncal que admita DTP.

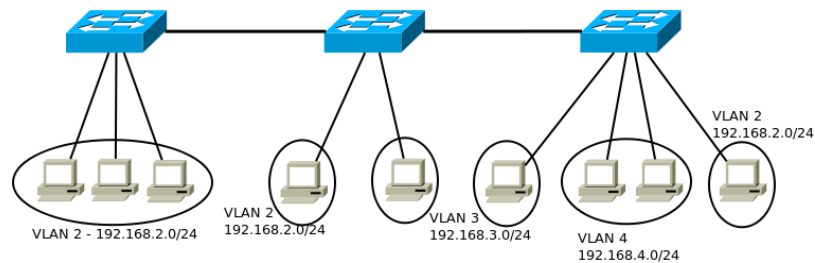


Figura N° 6. 6 Enlace Troncal entre switch

Fuente: <http://www.netstorming.com.ar/2010/01/18/introduccion-a-las-vlan/>

6.6.5.6 Enrutamiento entre VLAN

El enrutamiento entre vlans o inter vlan routing, resulta necesario una vez que se posee una infraestructura de red con vlan implementadas, debido a que los usuarios necesitaran intercambiar información de una red a otra.

El enrutamiento entre VLAN es un proceso que permite reenviar el tráfico de la red desde una VLAN a otra mediante un enrutador. Las VLAN están asociadas a subredes IP únicas en la red.

Por si sólo, un switch de capa 2 no tiene la capacidad de enrutar paquetes entre vlan diferentes, si ya tenemos creadas las vlan y hemos asignado más de una computadora a cada vlan, el proceso de enrutamiento lo lleva acabo un dispositivo de capa 3.

a. Router sin trunk (ruteo tradicional)

El enrutamiento tradicional requiere de enrutadores que tengan interfaces físicas múltiples para facilitar el enrutamiento entre VLAN. En la figura N° 6.7 el enrutador realiza el enrutamiento al conectar cada una de sus interfaces físicas a una VLAN única. Además, cada interfaz está configurada con una dirección IP para la subred asociada con la VLAN conectada a ésta. Al configurar las direcciones IP en las interfaces físicas, los dispositivos de red conectados a cada una de las VLAN pueden comunicarse con el enrutador mediante la interfaz física conectada a la misma VLAN. En esta configuración los dispositivos de red pueden utilizar el enrutador como un gateway para acceder a los dispositivos conectados a las otras VLAN.

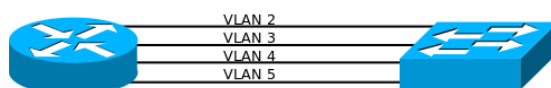


Figura N° 6. 7 Router sin trunk

Fuente: <http://www.netstorming.com.ar/2009/12/20/ruteo-entre-vlans/>

b. Router con trunk (router on-a-stick)

Una interfaz de un router se puede dividir en subinterfaces lógicas, por ejemplo de la interfaz FastEthernet 0/0 podemos derivar varias subinterfaces como: FastEthernet 0/0.10, FastEthernet 0/0.50, FastEthernet 0/0.30

La configuración de las subinterfaces del router es similar a la configuración de las interfaces físicas sólo que al final agregamos un punto y un número (.20), por lo regular este número es el mismo con el número de vlan a utilizar, todo esto para una mejor administración.

Una ventaja de utilizar un enlace troncal es que se reduce la cantidad de puertos del switch y del enrutador. Esto no sólo permite un ahorro de dinero sino también reduce la complejidad de la configuración. Como consecuencia, el enfoque de la subinterfaz del enrutador puede ampliarse hasta un número mucho más alto de VLAN que una

configuración con una interfaz física por diseño de VLAN. En la figura N° 6.8 se exhibe un enlace troncal mediante la configuración de subinterfaces.

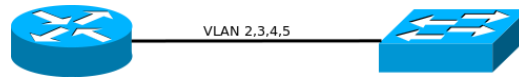


Figura N° 6. 8 Router con trunk (router on-a-stick)

Fuente: <http://www.netstorming.com.ar/2009/12/20/ruteo-entre-vlans/>

6.6.6 Comunicación a través de Internet

Para enviar datos entre un dispositivo conectado a una red de área local a otro conectado a otra LAN se requiere una vía de comunicación estándar, ya que es posible que las redes de área local utilicen distintos tipos de tecnologías. Esta necesidad lleva al desarrollo de un sistema de direcciones IP y protocolos basados en IP para comunicarse a través de Internet, que conforma un sistema global de redes informáticas interconectadas.

6.6.6.1 Conexiones a Internet

Para conectar una LAN a Internet se debe establecer una conexión de red a través de un proveedor de servicios de Internet (ISP). En una conexión a Internet se utilizan términos como velocidad de subida y velocidad de bajada. La velocidad de subida describe la velocidad de transferencia con la que se pueden subir datos del dispositivo a Internet: por ejemplo, cuando se envía un vídeo desde una cámara de red. La velocidad de bajada es la velocidad de transferencia con la que se bajan archivos: por ejemplo, cuando un monitor de ordenador recibe un vídeo

6.6.6.2 Puertos

Un número de puerto define un servicio o aplicación concretos para que el servidor receptor sepa cómo procesar los datos entrantes. Cuando un ordenador envía datos vinculados a una aplicación concreta, normalmente añade el número de puerto a una dirección IP sin que el usuario lo sepa. Los números de puerto pueden ir del 0 al

65535. Por ejemplo, un servicio web vía http se suele asignar al puerto 80 de una cámara de red.

6.6.6.3 Configuración de las direcciones IPv4

Para que una cámara de red o codificador de vídeo funcione en una red IP, se le debe asignar una dirección IP. Hay básicamente dos formas de configurar una dirección IPv4 1) de forma automática con el DHCP (Protocolo de configuración dinámica de host), y 2) introduciendo manualmente una dirección IP estática en la interfaz del producto de vídeo en red, una máscara de subred y la dirección IP del enrutador predeterminado.

El DHCP gestiona un conjunto de direcciones IP que puede asignar dinámicamente a una cámara de red/codificador de vídeo. A menudo la función DHCP la realiza un enrutador de banda ancha, que sucesivamente recibe sus direcciones IP de un proveedor de servicios de Internet. Una dirección IP dinámica significa que la dirección IP para un dispositivo de red puede cambiar de un día para otro. Para usar direcciones IP dinámicas se recomienda que los usuarios registren un nombre de dominio (por ejemplo, www.mycamera.com) para el producto de vídeo en red en un servidor de DNS (Sistema de nombres de dominio) dinámico, el cual siempre puede vincular el nombre de dominio del producto a cualquier dirección IP que tenga asignada.

6.6.6.4 NAT (Network address translation – Traducción de dirección de red)

Para que un dispositivo de red con una dirección IP privada pueda enviar información a través de Internet, debe utilizar un enrutador compatible con NAT. Con esta técnica, el enrutador puede traducir una dirección IP privada en una pública sin el conocimiento del host que realiza el envío. Las variantes de dispositivos NAT comparten las siguientes características:

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones (reenvío de paquetes).

a. Habilitación de puertos

La conversión de direcciones de red sólo permite solicitudes provenientes de la red interna hacia la red externa, con lo cual es imposible que un equipo externo envíe un paquete a un equipo de la red interna. En otras palabras, los equipos de la red interna no pueden funcionar como un servidor con respecto a la red externa.

Por esta razón, existe una extensión NAT llamada "habilitación de puertos" o mapeo de puertos que consiste en configurar la pasarela para enviar todos los paquetes recibidos en un puerto particular a un equipo específico de la red interna. Por lo tanto, si la red externa necesita acceder a un servidor Web (puerto 80) que funciona en un equipo 192.168.1.2, será necesario definir una regla de habilitación de puertos en la pasarela, con lo cual se redirigirán todos los paquetes TCP recibidos en el puerto 80 al equipo 192.168.1.2.

b. Activación de puertos

La mayoría de las aplicaciones cliente-servidor realiza una solicitud a través de un host remoto en un puerto determinado y a su vez abre un puerto para recuperar los datos. Sin embargo, ciertas aplicaciones utilizan más de un puerto para intercambiar datos con el servidor. Éste es el caso, por ejemplo, del FTP, para el que se establece una conexión por el puerto 21, pero los datos se transfieren por el puerto 20. Por lo tanto, con NAT, después de una solicitud de conexión en el puerto 21 de un servidor FTP remoto, la pasarela espera una conexión en un solo puerto y rechazará la solicitud de conexión en el puerto 20 del cliente.

Existe un mecanismo derivado de la NAT llamado "activación de puertos" que permite autorizar la conexión con determinados puertos (habilitación de puertos) si se completa una condición (solicitud). Por lo tanto, se trata de una habilitación de puertos condicional que permite que un puerto se abra sólo cuando una aplicación lo solicita. De esta manera, el puerto no permanece permanentemente abierto.

6.7 METODOLOGIA

El presente proyecto de video-vigilancia IP para el Gobierno Autónomo Descentralizado Municipal de Tulcán, al ser considerado substancial para empleados y directivos de la entidad, tomó inicio con la obtención de información, realizada mediante significativas técnicas investigativas como lo son la entrevista, la encuesta y la observación. También se procedió a la documentación de la situación actual de la red del edificio Municipal mediante un análisis de puntos de red y tráfico mediante el software CommView versión 6.0 para el monitoreo de tramas ethernet y CommView for WiFi versión 6.3 para el análisis de tramas 802.11.

A partir de la información obtenida se procedió a realizar el análisis e interpretación de resultados en donde se elaboró un registro definitivo de toda la información obtenida y se definió el tipo de tecnología para la solución al conflicto existente, dando paso al diseño del sistema de video-vigilancia IP, el mismo que empezó determinando los lugares más idóneos para la ubicación de las cámaras IP logrando así la cobertura deseada, seguido del estudio de equipos, en donde se realizó la comparación técnica de características y especificaciones en cuanto a software y hardware.

Para optimizar recursos de red se llegó a la determinación de que la creación de VLAN's era la mejor opción, para ello se realizó un modelo de direccionamiento IP y se procedió a la simulación en el software Packet Tracer de Cisco. El siguiente paso a efectuarse fue el de acceder remotamente a las cámaras desde internet, para lo cual se utilizó NAT para el redireccionamiento de puertos permitiendo la traducción de direcciones y en consecuencia la comunicación remota.

En la figura N° 6.9 se describe la metodología utilizada.

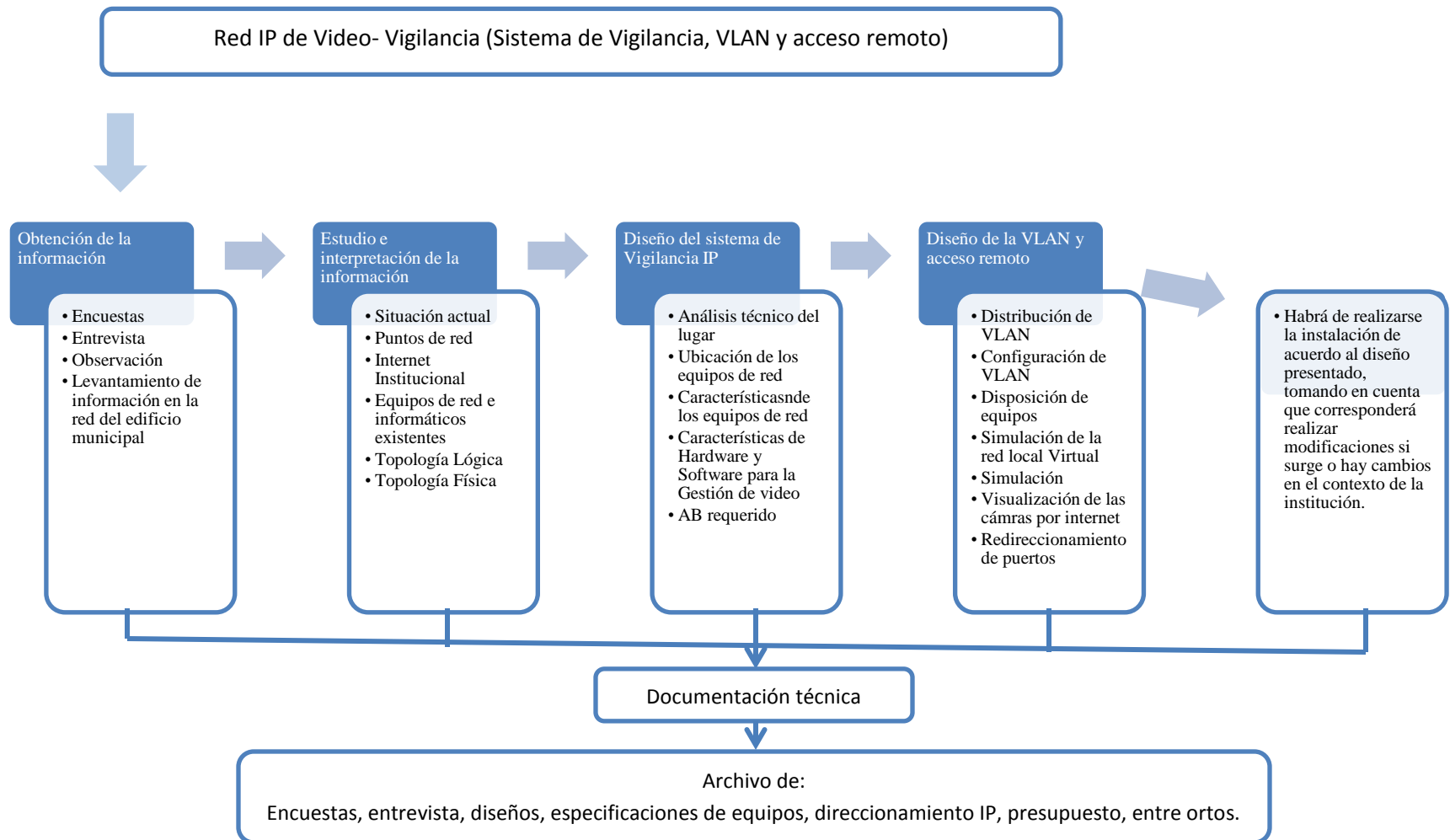


Figura N° 6. 9 Esquema de Trabajo
Elaborado por: El Investigador

6.8 SITUACIÓN ACTUAL DE LA RED DE COMUNICACIONES DEL GADMT

6.8.1 GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN

El Edificio del Gobierno Autónomo Descentralizado Municipal de Tulcán mostrado en la figura N° 6.10, se encuentra ubicado en el centro de la ciudad en las calles 10 de Agosto y José Joaquín Olmedo, frente al parque de la Independencia.



Figura N° 6. 10 Edificio del Gobierno Autónomo Descentralizado Municipal de Tulcán
Fuente: El Investigador

6.8.1.1 Niveles de organización y divisiones de trabajo por procesos del GADMT

La estructura organizacional del Municipio se basa en la Gestión de Procesos, compatibles con la demanda y la satisfacción de los ciudadanos/as y organizaciones sociales.

a. Procesos gobernantes

PROCESO NORMATIVO, que determina las políticas en las que se sustentarán los demás procesos institucionales para el logro de objetivos. Está integrado por: el Concejo Municipal.

PROCESO EJECUTIVO, que orienta y ejecuta la política trazada por el proceso normativo; le compete tomar las decisiones, impartir las instrucciones para que los demás procesos bajo su cargo se cumplan. Es el encargado de coordinar y supervisar el cumplimiento eficiente y oportuno de las diferentes acciones y productos. Está integrado por: Alcaldía.

b. Procesos habilitantes de apoyo y asesoría

Es el que presta asistencia técnica y administrativa de tipo complementario a los demás Procesos, además que corresponde al consultivo, de ayuda o de consejo a los demás procesos.

c. Procesos operativos; generadores de valor

Que es el encargado de la ejecución directa de las acciones que entregan productos y servicios a la comunidad o cliente; encargado de cumplir directamente con los objetivos y finalidades de la municipalidad, ejecuta los planes, programas, proyectos y demás políticas y decisiones del Proceso Gobernante. Los Productos y servicios que entrega al cliente, lo perfeccionan con el uso eficiente de recursos y al más bajo costo, y forma parte del proceso agregado de valor.

En la tabla N°6.1 Se establece la siguiente división de procesos y subprocesos, que componen el conjunto de equipos de trabajo:

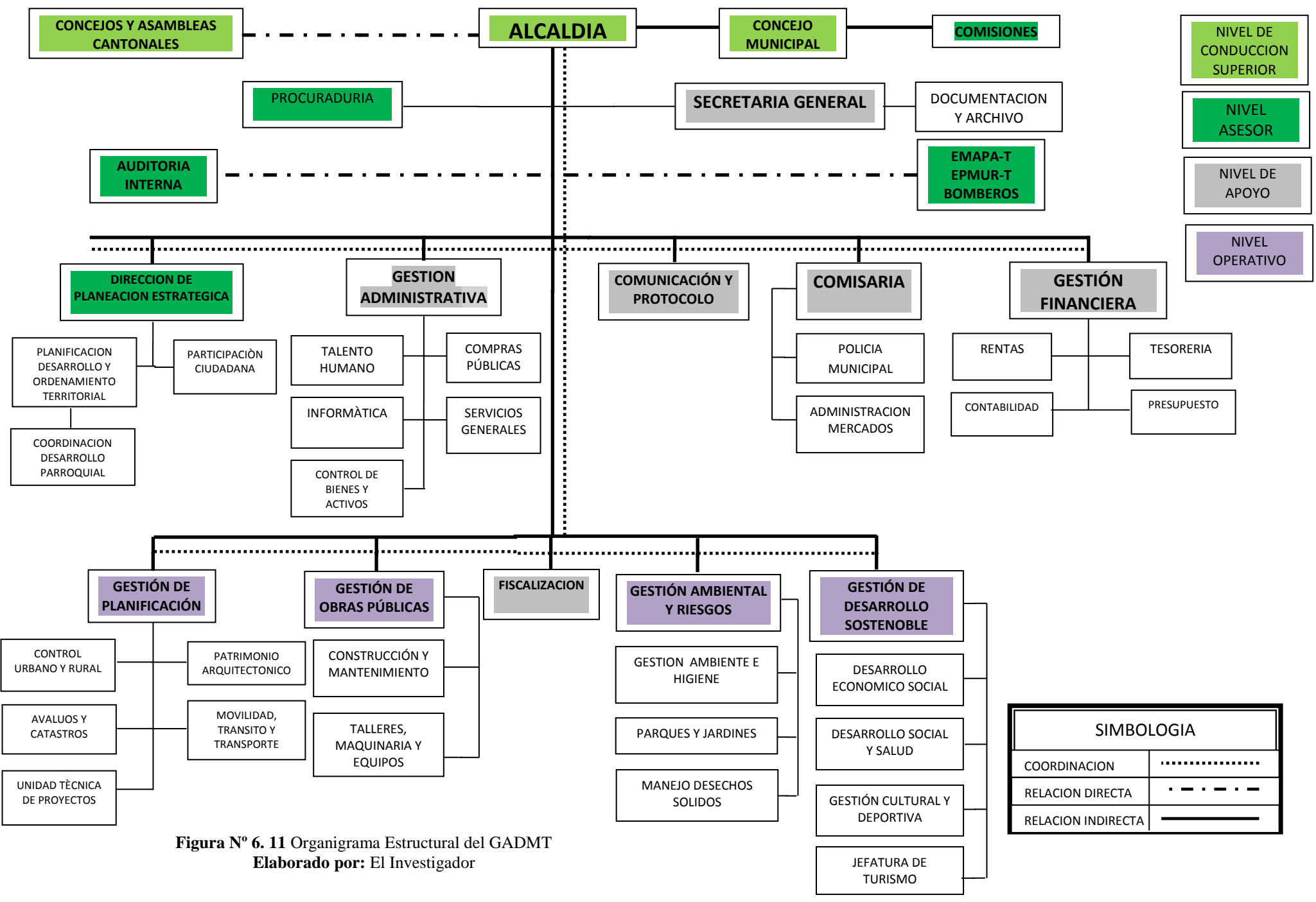
MACRO PROCESOS	PROCESOS	SUB PROCESOS
GOBERNADORES	GESTIÓN NORMATIVA	CONCEJO, COMISIONES PERMANENTES Y ESPECIALES
	GESTIÓN EJECUTIVA	ALCALDÍA
	GESTIÓN PARTICIPATIVA	PARTICIPACIÓN CIUDADANA
OPERATIVOS	GESTIÓN DE PLANIFICACIÓN	CONTROL URBANO Y RURAL
		TRANSPORTE
		AVALUOS Y CATASTROS
		CEMENTERIO
	GESTIÓN OBRAS PUBLICAS	CONSTRUCCIÓN Y MANTENIMEINTO:
		TALLERES Y EQUIPOS
	GESTIÓN AMBIENTAL Y RIEGOS	GESTIÓN AMBIENTAL HIGIENE Y SALUBRIDAD
MANEJO DE DESECHOS		
PARQUES Y JARDINES		
SEVICIOS PÚBLICOS		
GESTIÓN DE DESARROLLO SOSTENIBLE	CAMAL Y MERCADO	
	EDUCACIÓN Y RECREACIÓN	
	DESARROLLO SOCIAL Y SALUD	
HABILITANTES DE APOYO Y ASESORIA	GESTIÓN DE ASESORIA LEGAL	PROCURADOR SÍNDICO
		DESARROLLO LOCAL ESTUDIOS Y PROYECTOS
	GESTIÓN DE DESALLORRO LOCAL Y PARTICIPACIÓN SOCIAL	TURISMO
		AUDITORÍA
	GESTIÓN ADMINISTRATIVA	TALENTO HUMANO, INFORMÁTICA
		COMPRAS PÚBLICAS, PROVEEDURIAS
		SERVICIOS GENERALES, IMPRENTA
	GESTIÓN DE FISCALIZACIÓN DE OBRAS	FISCALIZACIÓN
	GESTIÓN DE SECRETARÍA GENENERAL	SECRETARÍA GENERAL
	GESTIÓN DE COMUNICACIÓN	COMUNICACIÓN SOCIAL
GESTIÓN DE CONTROL NORMATIVO	COMISARÍA	
	CONTABILIDAD, RENTAS, BODEGA	
GESTIÓN FINANCIERA	PRESUPUESTO, TESORERÍA	

Tabla N° 6. 5 Niveles de organización y divisiones de trabajo por procesos del GADMT
Elaborado por: El Investigador

6.8.1.2 Organigrama y descripción de los procesos

Se adopta el siguiente Organigrama Estructural como parte de la división de trabajo del Gobierno Municipal, a partir del cual se diseñarán los procesos y Subprocesos de la estructura organizacional.

El Organigrama Estructural del Gobierno Municipal de Tulcán expuesto en la figura N°6.11 considera cuatro niveles de actividades a ser desarrolladas en la gestión municipal: Nivel de Conducción Superior, Nivel Asesor, Nivel de Apoyo y Nivel Operativo.



NIVEL DE CONDUCCION SUPERIOR

NIVEL ASESOR

NIVEL DE APOYO

NIVEL OPERATIVO

SIMBOLOGIA	
COORDINACION
RELACION DIRECTA	-----
RELACION INDIRECTA	-----

Figura N° 6. 11 Organigrama Estructural del GADMT
 Elaborado por: El Investigador

6.8.1.3 Recurso humano del GADMT

En los niveles de organización y divisiones de trabajo por procesos del GADMT se realizó una apreciación general de la distribución del personal según su actividad desempeñada. Siendo 533 el número total de servidores públicos de la entidad municipal según los datos obtenidos de la Unidad de Talento Humano, de los cuales 155 de ellos están situados en el edificio municipal.

6.8.1.4 Distribución de unidades /direcciones en el edificio municipal de Tulcán

El presente proyecto de investigación se desarrolla únicamente en el edificio Municipal, el cual consta de cinco pisos:

Planta Baja

- Café Net
- Rentas
- Ventanillas de Recaudación
- Control de Bienes y Activos
- Comisaría

Primer Piso

- Dirección de Planificación
- Proyectos
- Avalúos y Catastros
- Unidad Ambiental
- Tránsito
- Zonas Azules

Segundo Piso

- Departamento Financiero
- Tesorería

- Coactivas
- Contabilidad
- Secretaria General
- Comunicaciones y Protocolo
- Sala de Reuniones (concejales-alcalde)
- Alcaldía
- Planeación estratégica

Tercer Piso

- Dirección Administrativa
- Sistemas
- Fiscalización
- Sindicatura
- Obras Públicas
- Cultura
- Desarrollo Sostenible
- Auditoria Interna
- Compras Públicas

Cuarto Piso

- Biblioteca
- Salón de usos múltiples
- Oficina de la Asociación de Empleados

6.8.2 DESCRIPCIÓN ACTUAL DE LA RED DE COMUNICACIONES INTERNA DEL GADMT

A continuación se presentan todos los equipos, puntos de red y extensiones telefónicas que conforman el sistema de comunicaciones del GMT, divididos por departamentos y pisos, los cuales son resultado de un levantamiento de información llevado a cabo en la institución comprendido entre el 2 y 8 de mayo del 2012.

a. Planta Baja

En la tabla N° 6.6 se detallan las extensiones telefónicas, 25 ordenadores personales en la planta baja del edificio municipal, también se establece un total de 12 impresoras, de las cuales 10 están compartidas en red y 2 son locales. Para obtener el total de conexiones de red se toman encuentra los puntos correspondientes a las pc's y a las impresoras con punto de red, obteniéndose un total de 25.

DIRECCIÓN/UNIDAD	PC'S		IMPRESORAS				EXTENSIONES TELEFÓNICAS
	NUM	PUNTO DE RED	NUM	COMPARTIDA EN RED	LOCAL	PUNTO DE RED	
CAFE NET	4	4	1	1	0	0	
RENTAS	6	6	3	3	0	0	Extensión/105
RECAUDACIÓN	7	7	3	3	0	0	Extensión/102
BIENES Y ACTIVOS	4	4	2	2	0	0	Extensión/103 Subextensión
COMISARÍA	2	2	2	0	2	0	Extensión/106
ADMINISTRACIÓN DE MERCADOS	2	2	1	1	0	0	
TOTAL	25	25	12	10	2	0	
25 PUNTOS DE RED /PLANTA BAJA							

Tabla N° 6. 6 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en la planta baja del edificio municipal.

Elaborado por: El Investigador

b. Primer Piso

En la tabla N° 6.7 se describen las extensiones telefónicas, 42 ordenadores personales en el primer piso del edificio municipal, también se detalla un total de 10 impresoras, de las cuales 7 están compartidas en red, 2 son locales y 1 se encuentra con punto de red. Estableciéndose un total de 43 conexiones de red.

DIRECCIÓN/UNIDAD	PC'S		IMPRESORAS			EXTENSIONES TELEFÓNICAS	
	NUM	PUNTO DE RED	NUM	COMPARTIDA EN RED	LOCAL		PUNTO DE RED
GESTION AMBIENTAL Y RIESGOS	6	6	2	1	1	0	Extensión/107 Subextensión
PROYECTOS	7	7	1	0	0	1	
TRANSITO Y TRANSPORTE	2	2	0	0	0	0	
PLANIFICACION URBANA	9	9	1	0	1	0	Extensión/111 Subextensión
CONSTRUCCIONES	4	4	1	1	0	0	
ZONAS AZULES	4	4	2	2	0	0	Extensión/145
AVALÚOS Y CATASTROS	10	10	3	3	0	0	Extensión/129 Subextensión
TOTAL	42	42	10	7	2	1	
TOTAL = 43 PUNTOS DE RED /PRIMER PISO							

Tabla N° 6. 7 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el primer piso del edificio municipal.

Elaborado por: El Investigador

c. Segundo Piso

En la tabla N° 6.8 se especifican las extensiones telefónicas, 39 ordenadores personales en el segundo piso del edificio municipal, también se dispone un total de 19 impresoras, de las cuales 10 están compartidas en red, 5 son locales y 4 se encuentran con punto de red. Apreciándose un total de 43 conexiones de red.

DIRECCIÓN/UNIDAD	PC'S		IMPRESORAS			EXTENSIONES TELEFÓNICAS	
	NUM	PUNTO DE RED	NUM	COMPARTIDA EN RED	LOCAL		PUNTO DE RED
DIRECCIÓN FINANCIERA	5	5	3	1	1	1	Extensión/112 Subextensión Extensión/114
TESORERÍA	4	4	2	1	1	0	Extensión/109
COACTIVAS	3	3	2	1		1	Extensión/133 Subextensión
CONTABILIDAD	4	4	3	2	1	0	Extensión/115
PLANEACIÓN ESTRATEGICA	11	11	4	2	1	1	Extensión/140 Subextensión Extensión/142
COMUNICACION Y PROTOCOLO	6	6	3	2	0	1	Extensión/101 Extensión/118
ALCALDIA	4	4	1	1	0	0	Extensión/120 Extensión/122
SECRETARIA GENERAL	2	2	1	0	1	0	Subextensión Extensión/117
TOTAL	39	39	19	10	5	4	
TOTAL = 43 PUNTOS DE RED /SEGUNDO PISO							

Tabla N° 6. 8 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el segundo piso del edificio municipal

Elaborado por: El Investigador

d. Tercer Piso

En la tabla N° 6.9 se detallan las extensiones telefónicas, 46 ordenadores personales en el tercer piso del edificio municipal, también se fija un total de 21 impresoras, de las cuales 17 están compartidas en red y 4 son locales. Lo que nos da como resultado un total de 46 puntos de red.

DIRECCIÓN/UNIDAD	PC'S		IMPRESORAS			EXTENSIONES TELEFÓNICAS	
	NUM	PUNTO DE RED	NUM	COMPARTIDA EN RED	LOCAL		PUNTO DE RED
DIRECCIÓN ADMINISTRATIVA	2	2	1	1	0	0	Extensión/125 Extensión/123
SERVICIOS GENERALES	2	2	0	0	0	0	Extensión/116
TALENTO HUMANO	5	5	2	1	1	0	Extensión/104
FISCALIZACIÓN	7	7	4	3	1	0	Extensión/128 Extensión/127
OBRAS PÚBLICAS	6	6	2	2	0	0	Extensión/130
SINDICATURA	4	4	2	1	1	0	Extensión/132 Extensión/151
AUDITORIA INTERNA	2	2	2	2	0	0	Extensión/110
CULTURA	6	6	3	3	0	0	Extensión/134
DESARROLLO SOSTENIBLE	3	3	2	2	0	0	Extensión/136
INFORMÁTICA	7	7	2	1	1	0	Extensión/143 Extensión/126
COMPRAS PÚBLICAS	2	2	1	1	0	0	Extensión/139
TOTAL	46	46	21	17	4	0	
TOTAL = 46 PUNTOS DE RED /TERCER PISO							

Tabla N° 6. 9 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el tercer piso del edificio municipal.

Elaborado por: El Investigador

e. Cuarto Piso

En la tabla N° 6.10 se especifica una extensión telefónica existente en el cuarto piso del edificio municipal, 3 ordenadores personales, una impresora local y cinco puntos de red.

DIRECCIÓN/UNIDAD	PC'S		IMPRESORAS			EXTENSIONES TELEFÓNICAS	
	NUM	PUNTO DE RED	NUM	COMPARTIDA EN RED	LOCAL		PUNTO DE RED
BIBLIOTECA	3	3	1	0	1	0	Extensión/137
SALON MÚLTIPLE	0	1	0	0	0	0	
ASOCIACIÓN DE EMPLEADOS	0	1	0	0	0	0	
TOTAL	3	5	1	0	1	0	
TOTAL = 5 PUNTOS DE RED /CUARTO PISO							

Tabla N° 6. 10 Equipos de cómputo, impresoras, extensiones telefónicas y puntos de red existentes en el cuarto piso del edificio municipal.

Elaborado por: El Investigador

6.8.2.1 Equipos de red

En las tablas N° 6.11, 6.12, 6.13, 6.14, 6.15, se describen la ubicación, los modelos, puertos usados y la capacidad de administración de los equipos de red del GADMT.

a. Planta Baja

MARCA/ MODELO	VELOCIDAD	PUERTOS /USADOS	ADMINISTRABLE	UBICACIÓN
D-LINK DES- 1024R+	10/100 Mbps	24/20	NO	Rentas
D-LINK DES-3526	10/100 Mbps	24/12	NO	Ventanillas Recaudación
CNET CSH-1600	10/100 Mbps	16/8	NO	Comisaría

Tabla N° 6. 11 Equipos de red existentes en la planta baja del edificio municipal.
Elaborado por: El Investigador

b. Primer Piso

MARCA/ MODELO	VELOCIDAD	PUERTOS/ USADOS	ADMINISTRABLE	UBICACIÓN
D-LINK DES-1024R+	10/100 Mbps	24/23	NO	Planificación Urbana
D-LINK DES-1228	10/100 Mbps (4 puertos) 1000 Mbps	28/14	SI (Vía Web)	Proyectos
DELL 2724	10/100 Mbps	24/6	NO	Unidad Ambiental
TRENDNET TE100- S8	10/100 Mbps	8/4	NO	Zonas Azules

Tabla N° 6. 12 Equipos de red existentes en el primer piso del edificio municipal.
Elaborado por: El Investigador

c. Segundo Piso

MARCA/ MODELO	VELOCIDAD	PUERTOS /USADOS	ADMINISTRABLE	UBICACIÓN
D-LINK DES-1228	10/100 Mbps (4 puertos) 1000 Mbps	28/26	SI (Vía Web)	Contabilidad
D-LINK DES- 1024R+	10/100 Mbps	24/23	NO	Planeación Estratégica

Tabla N° 6. 13 Equipos de red existentes en el segundo piso del edificio municipal.
Elaborado por: El Investigador

d. Tercer Piso

MARCA/ MODELO	VELOCIDAD	PUERTOS /USADOS	ADMINISTRABLE	UBICACIÓN
CISCO CATALYST 3550	10/100 Mbps	48/44	SI (Vía CLI)	Data Center
D-LINK DES- 1024R+	10/100 Mbps	24/22	NO	Data Center
D-LINK DES-1008D	10/100 Mbps	8/7	NO	Dirección Administrativa
Cisco 800 Series Routers	10/100 Mbps	4/2	SI	Data Center

Tabla N° 6. 14 Equipos de red existentes en el tercer piso del edificio municipal.
Elaborado por: El Investigador

e. Cuarto Piso

MARCA/ MODELO	VELOCIDAD	PUERTOS /USADOS	ADMINISTRABLE	UBICACIÓN
C-NET CSH-1600	10/100 Mbps	16/7	NO	Biblioteca

Tabla N° 6. 15 Equipos de red existentes en el cuarto piso del edificio municipal.
Elaborado por: El Investigador

6.8.2.2 Servidores

La tabla N° 6.16 expone las características de los servidores de red del Gobierno Municipal que se encuentran en el tercer piso en el cuarto de comunicaciones, ubicado en la Unidad de Informática.

NOMBRE/ FUNCION	MARCA/ MODELO	SISTEMA OPERATIVO
SERVER 01 Proxy	HP PROLIANT ML-150 G2	LINUX/CentOS 5.5
SERVER 02 Correo Trámites Documentos	HP PROLIANT DL-380 G6	LINUX/openSUSE
SERVER 03 RR.HH	HP PROLIANT ML-150 G2	Windows Server 2003
SERVER 04 BBD 1	COMPAQ PROLIANT 800	Windows Server 2003
SERVER 05 BDD 2	HP PROLIANT ML-150 G2	Windows Server 2003

Tabla N° 6. 16 Características de los Servidores de red del GADMT
Elaborado por: El Investigador

6.8.2.3 Topología física de red del GADMT

La topología física de red del Gobierno Autónomo Descentralizado Municipal de Tulcán es de estrella extendida como se indica en la figura N° 6.12. Esta topología es igual a la de estrella, con la diferencia de que cada nodo que se conecta con el nodo central también es el centro de otra estrella.

La ventaja de esto es que el cableado es más corto y limita la cantidad de dispositivos que se deben interconectar con cualquier nodo central.

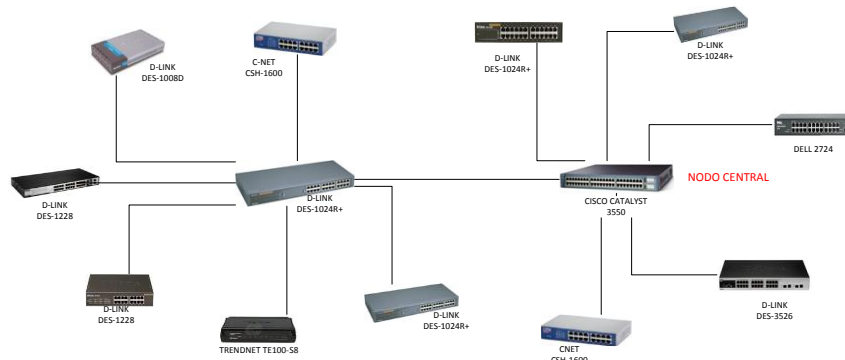


Figura N° 6. 12 Topología física de red del GADMT
Elaborado por: El Investigador

6.8.2.4 Topología lógica de red del GADMT

La topología lógica de red del Gobierno Autónomo Descentralizado Municipal de Tulcán es de Bus Ethernet ya que todos los dispositivos son conectados a un canal de comunicaciones de señales compartidas.

Cada dispositivo equipado con Ethernet opera en forma independiente del resto de los dispositivos de la red. Las señales Ethernet son transmitidas en serie, se transmite un bit a la vez. Las transmisiones se realizan a través del canal de señales compartidas donde todos los dispositivos conectados pueden escuchar la transmisión. Antes de comenzar una transmisión, un dispositivo escucha el canal de transmisión para ver si se encuentra libre de transmisiones. Si el canal se encuentra libre, el dispositivo puede transmitir sus datos en la forma de una trama Ethernet. Después de que es transmitida una trama, todos los dispositivos de la red compiten por la siguiente oportunidad de transmitir una trama. El acceso al canal de comunicaciones compartido es determinado por la subcapa MAC. Este control de acceso al medio es conocido como CSMA/CS.

6.8.2.5 Diagrama de comunicaciones del GADMT

En el siguiente diagrama de red de la figura N° 6.13 se muestra como esta estructurado el sistema de Comunicaciones del edificio municipal.

DIAGRAMA DE RED DEL GADMT

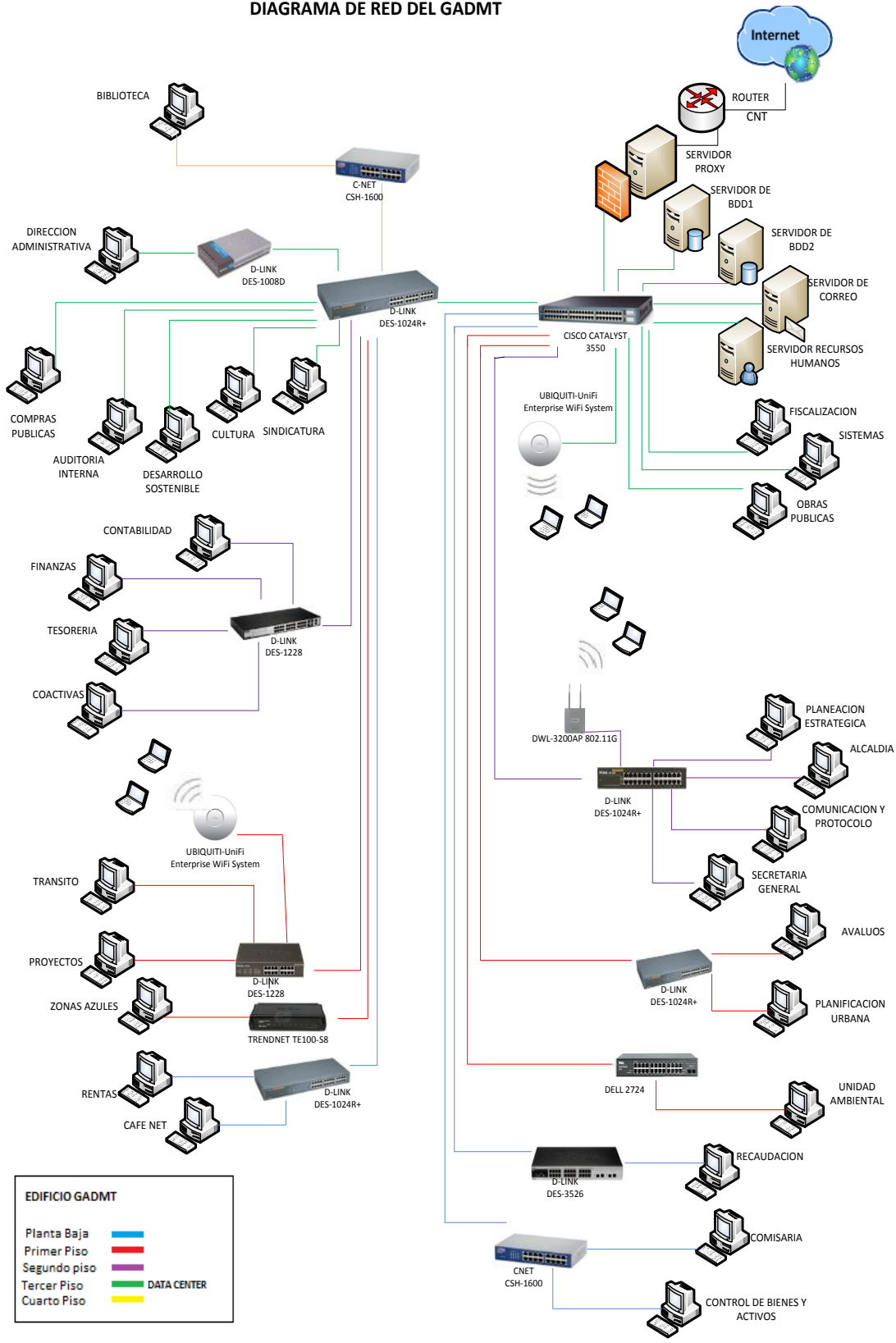


Figura N° 6. 13 Diagrama de red del GADMT
Elaborado por: El Investigador

6.8.2.6 Software utilizado en el sistema de comunicaciones

a. Base de datos

- MySQL para el almacenamiento de la información.
- PostgreSQL gestores de base de datos

b. Software de desarrollo

El software de desarrollo que se utiliza es Java para creación de aplicaciones pertenecientes al GMT.

c. Aplicaciones que ofrece la red actual

- Patentes
- Catastros: Urbano, Rural
- Impuesto vehicular
- Sistema Integrado Contabilidad (Plusvalía)
- Cementerio

d. Servicios proporcionados por la red.

- El sistema de comunicación ofrece los siguientes servicios:
- Servicio de Internet corporativo
- Internet público en la biblioteca y café Net
- Servicio de Proxy
- Servicio de intercambio de archivos.
- Servicio de impresión en red
- Alojamiento pagina Web del GMT
- Radio Municipal

6.9 MODELO OPERATIVO

6.9.1 DISEÑO DEL SISTEMA DE VIGILANCIA PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN

6.9.1.1 Análisis Técnico del Lugar

Luego del levantamiento de información y planos arquitectónicos realizado en el edificio Municipal se determinó las siguientes zonas a ser cubiertas por el sistema de cámaras digitales; que son las que se detallan en la tabla N° 6.17.

DIRECCIÓN/UNIDAD	ÁREA (m ²)
PLANTA BAJA	
RECAUDACIÓN	87,70
CAFE NET	25,25
COMISARÍA	49,55
BODEGA	48,80
BIENES Y ACTIVOS	23,40
HALL	112,60
PRIMER PISO	
PLANIFICACIÓN URBANA	80,25
PROYECTOS	37,78
ZONAS AZULES	70,62
AVALUOS Y CATASTROS	78,15
GESTIÓN AMBIENTAL Y RIESGOS	50,20
GRADAS E INGRESO AL 1º PISO	30,50
SEGUNDO PISO	
DIRECCIÓN FINANCIERA	55,20
COACTIVAS	52,40
CONTABILIDAD	26,15
PLANEACIÓN ESTRATÉGICA	113,95
COMUNICACIÓN Y PROTOCOLO	52,00
SALA DE ESPERA ALCALDÍA	19,50
GRADAS E INGRESO AL 2º PISO	30,50
TERCER PISO	
TALENTO HUMANO	59,15
INFORMÁTICA	51,00
FISCALIZACIÓN	60,00
OBRAS PÚBLICAS	43,70
SINDICATURA	66,15
COMPRAS PÚBLICAS	25,12
DESARROLLO SOSTENIBLE	51,80
GRADAS E INGRESO AL 3º PISO	30,50
CUARTO PISO	
SALÓN MÚLTIPLE	250,80
BIBLIOTECA	111,15
GRADAS E INGRESO AL 4º PISO	30,50

Tabla N° 6. 17 Zonas a ser cubiertas por el sistema de cámaras digitales

Elaborado por: El Investigador

6.9.1.2 Ubicación de las cámaras

En las figuras desde la N° 6.14 hasta la N° 6.18 y en las tablas desde la N° 6.18 hasta la N° 6.22, se definen las zonas de monitoreo establecidas así como la ubicación de las cámaras, con la finalidad de lograr la cobertura solicitada y cumplir con los requerimientos necesarios para la red de vigilancia.

a. Planta Baja

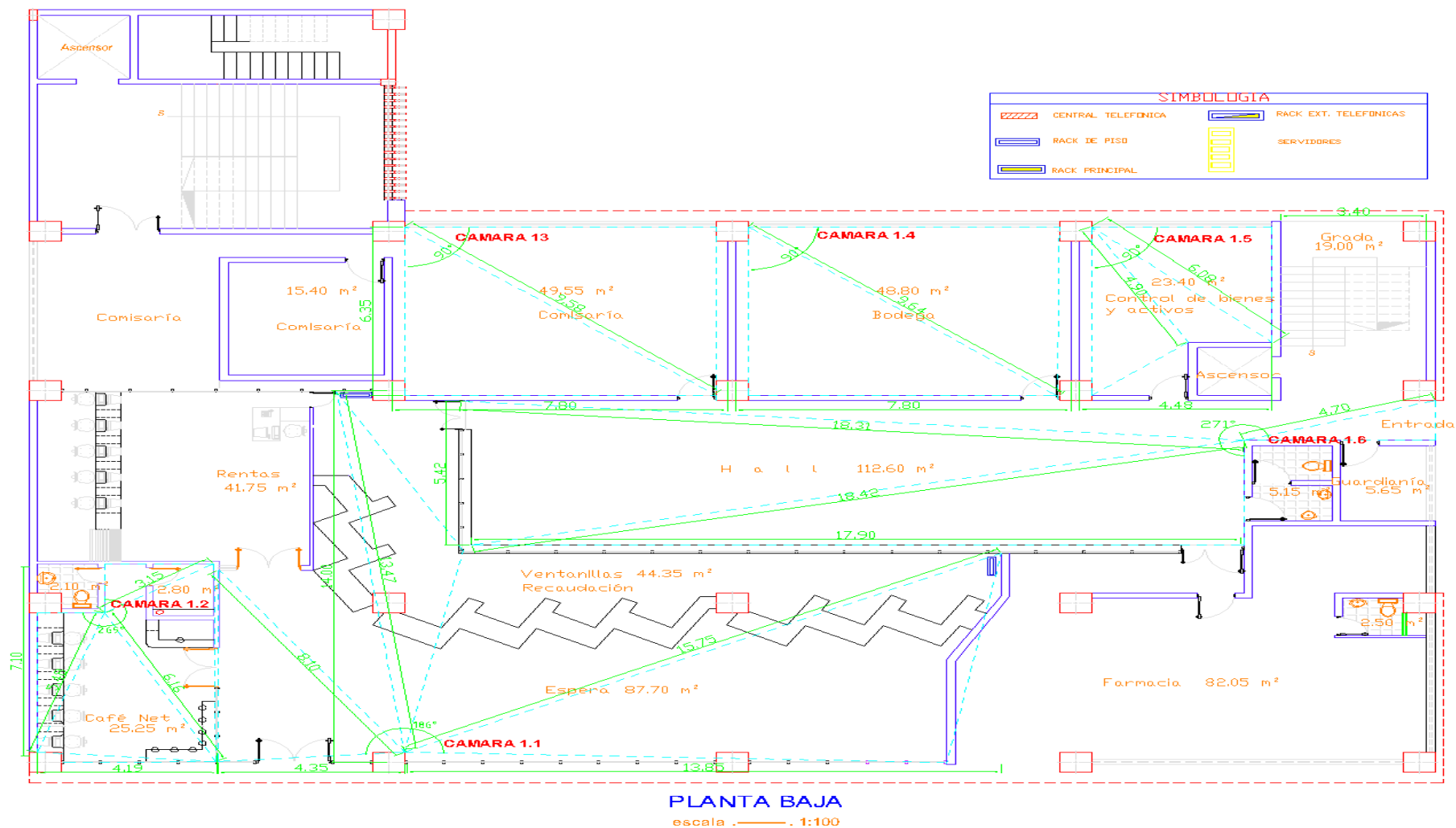


Figura N° 6. 14 Ubicación de las cámaras IP en la Planta baja del GADMT
 Elaborado por: El Investigador

N° DE CÁMARA	COBERTURA	DISTANCIA	DESCRIPCIÓN
CÁMARA 1.1	186°	16m	Cubre la puerta de ingreso principal, el área correspondiente a las Ventanillas de Recaudación y el ingreso a la Unidad de Rentas.
CÁMARA 1.2	269°	7m	Cubre la zona del Café Net y su puerta de acceso.
CÁMARA 1.3	90°	10m	Cubre la Unidad de Comisaría. Comprende secretaria de comisaría, administración de mercados y acceso a la oficina del comisario.
CÁMARA 1.4	90°	10m	Resguarda el área de bodega administrada por la Unidad de Control de Bienes y Activos.
CÁMARA 1.5	90°	6m	Cubre la Unidad de Control de Bienes y Activos.
CÁMARA 1.6	271°	19m	Abarca el Hall y la entrada del edificio Municipal.

Tabla N° 6. 18 Ubicación de las cámaras IP en la Planta baja del GADMT

Elaborado por: El Investigador

b. Primer Piso

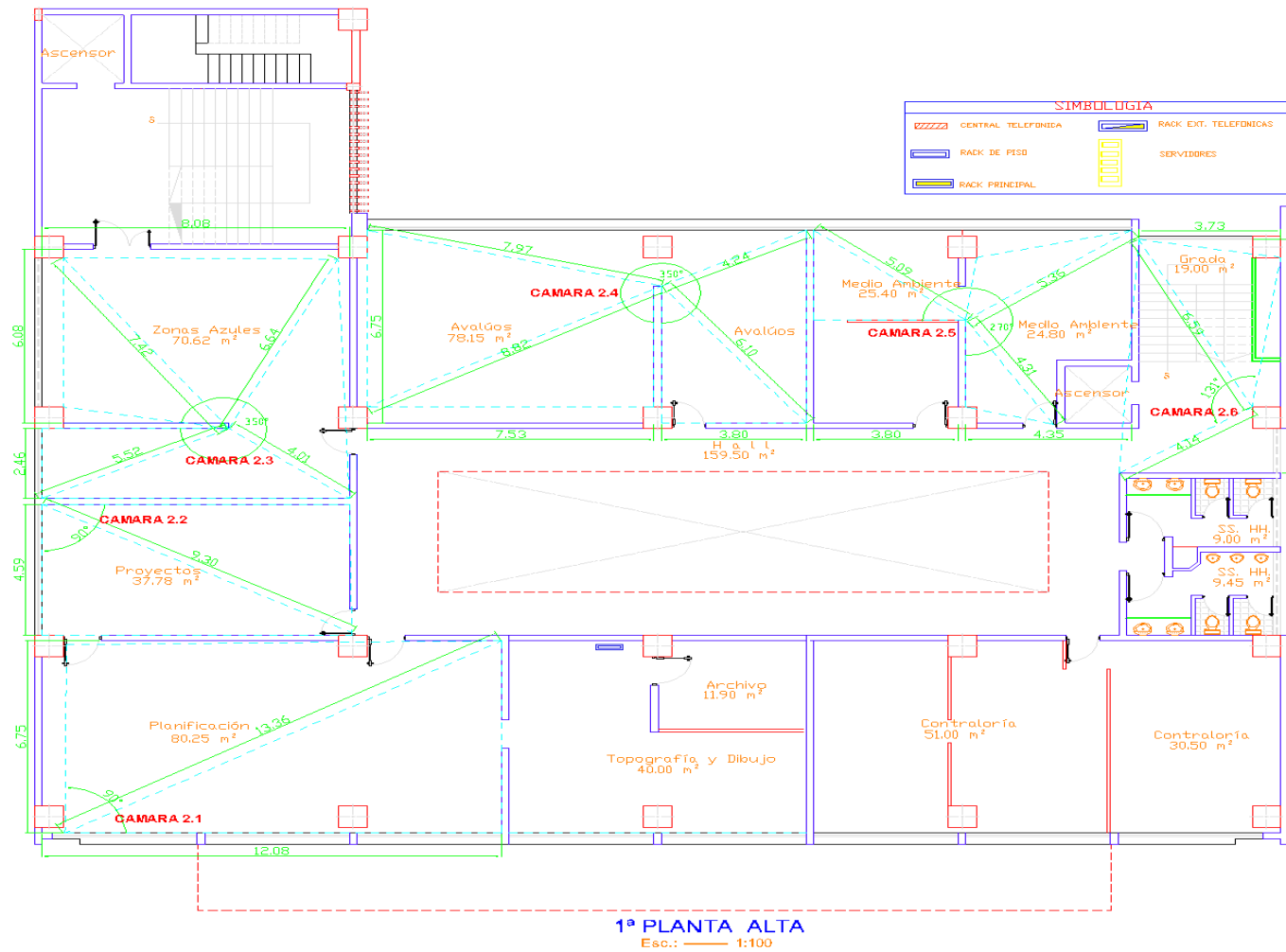


Figura N° 6.15 Ubicación de las cámaras IP en el Primer piso del GADMT
Elaborado por: El Investigador

N° DE CÁMARA	COBERTURA	DISTANCIA	DESCRIPCIÓN
CÁMARA 2.1	90°	14m	Cubre la Unidad de Planificación, el ingreso a la zona de topografía y dibujo, sus puertas de acceso.
CÁMARA 2.2	90°	10m	Cubre la Unidad de Proyectos y el ingreso a la misma.
CÁMARA 2.3	350°	8m	Cubre la Unidad de Zonas Azules y su puerta de acceso.
CÁMARA 2.4	350°	9m	Cubre la unidad de Avalúos y Catastros así como el ingreso de la misma.
CÁMARA 2.5	270°	6m	Cubre la Unidad de Medio Ambiente, su puerta de ingreso y la de acceso a la dirección.
CÁMARA 2.6	131°	7m	Cubre el área de las gradas y el acceso a la primera planta alta.

Tabla N° 6. 19 Ubicación de las cámaras IP en el Primer piso del GADMT
Elaborado por: El Investigador

c. Segundo Piso

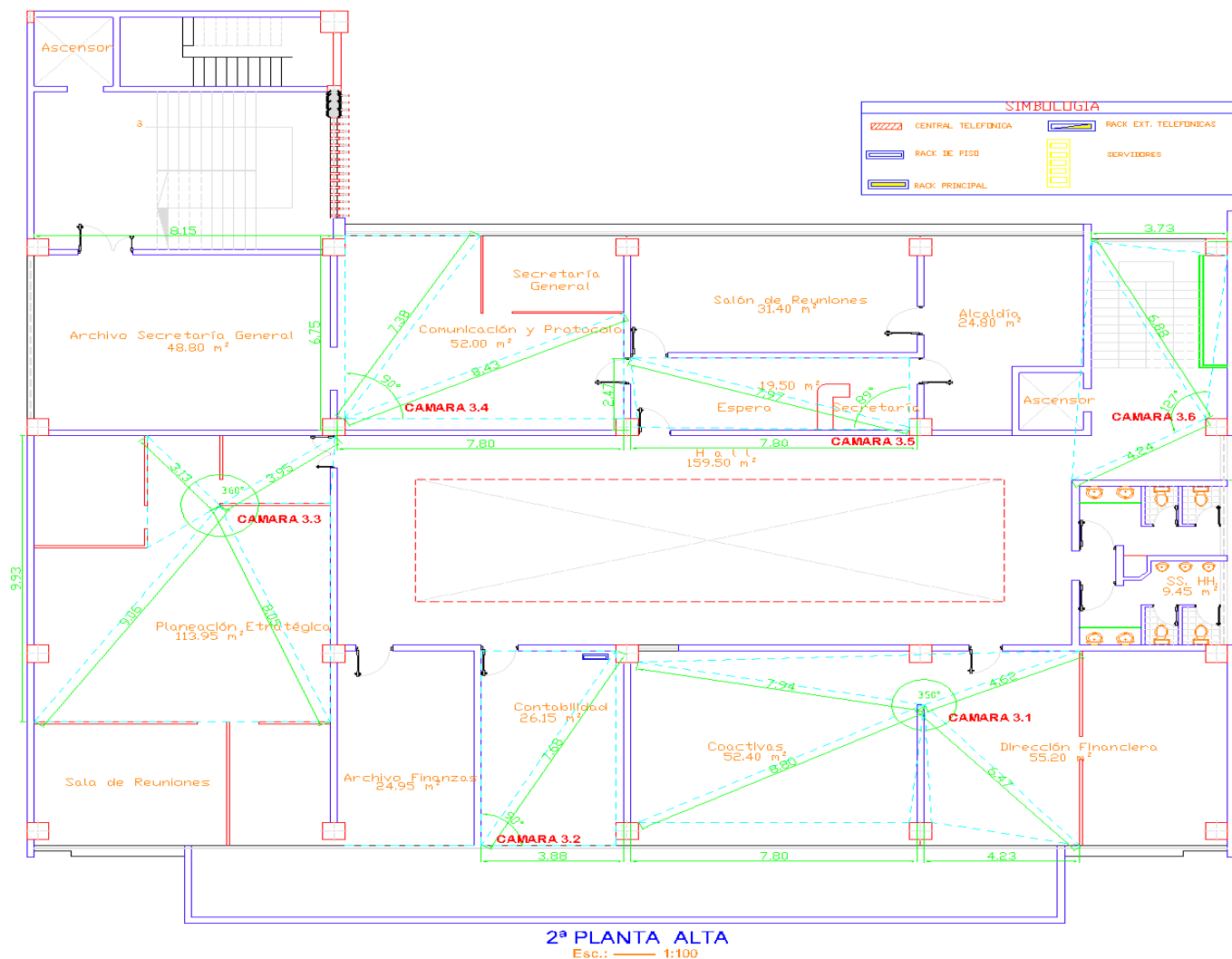


Figura N° 6. 16 Ubicación de las cámaras IP en el Segundo piso del GADMT
Elaborado por: El Investigador

N° DE CÁMARA	COBERTURA	DISTANCIA	DESCRIPCIÓN
CÁMARA 3.1	350°	9m	Cubre el área de Finanzas. Tesorería y Coactivas, además del ingreso a la dirección Financiera.
CÁMARA3.2	90°	8m	Cubre la Unidad de Contabilidad y su ingreso.
CÁMARA 3.3	360°	9m	Cubre la Unidad de Planeación Estratégica, su ingreso y el acceso a la sala de reuniones.
CÁMARA 3.4	90°	9m	Cubre la Unidad de Comunicación y Protocolo, su ingreso y las puertas de acceso a la oficina del Secretario General y Archivo de Secretaría.
CÁMARA 3.5	90°	8m	Cubre la Sala de espera y secretaría de Alcaldía, la puerta de acceso principal, el ingreso a la oficina del Alcalde y a la Sala de reuniones.
CÁMARA 3.6	127°	7m	Cubre el área de las gradas y el acceso a la segunda planta alta.

Tabla N° 6. 20 Ubicación de las cámaras IP en el Segundo piso del GADMT

Elaborado por: El Investigador

d. Tercer Piso

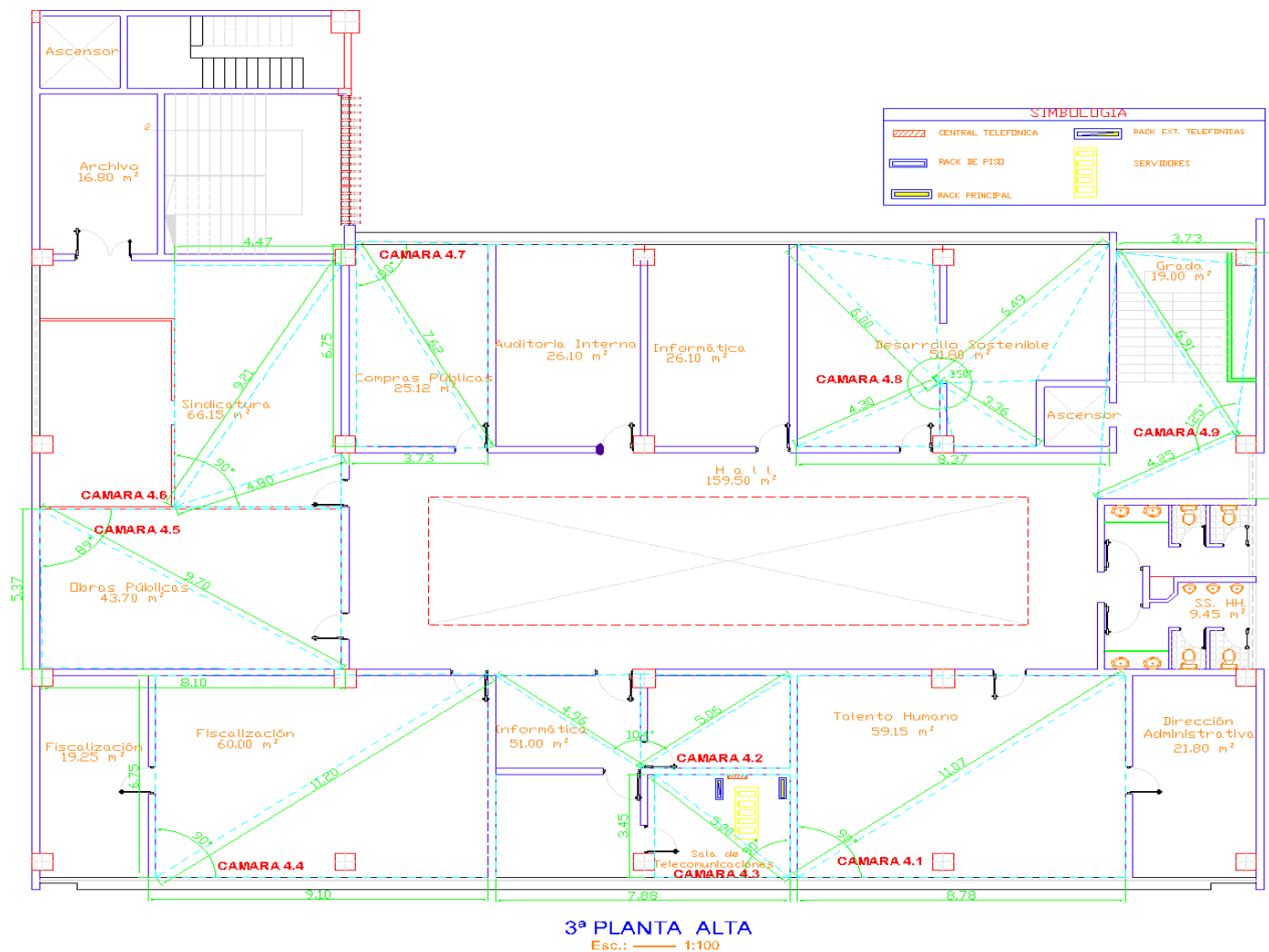


Figura N° 6. 17 Ubicación de las cámaras IP en el Tercer piso del GADMT
Elaborado por: El Investigador

Nº DE CÁMARA	COBERTURA	DISTANCIA	DESCRIPCIÓN
CÁMARA 4.1	90°	11m	Cubre la Unidad de Talento Humano, su ingreso y el acceso a la Dirección Administrativa.
CÁMARA 4.2	104°	6m	Cubre el área de Programadores, Servicio Técnico y puerta de ingreso.
CÁMARA 4.3	90°	5m	Cubre la Sala de Telecomunicaciones del GADMT.
CÁMARA 4.4	360°	12m	Cubre el área de Fiscalización, su puerta de ingreso y el acceso a la oficina del director de la Unidad.
CÁMARA 4.5	90°	10m	Cubre la Unidad de Obras Públicas y su puerta de acceso.
CÁMARA 4.6	90°	10m	Cubre el área de Sindicatura, su puerta de ingreso y el acceso a la oficina del director de la Unidad.
CÁMARA 4.7	90°	8m	Cubre la Unidad de Compras Públicas y su puerta de acceso.
CÁMARA 4.8	350°	7m	Cubre el área de Desarrollo Sostenible y su puerta de acceso.
CÁMARA 4.9	125°	7m	Cubre el área de las gradas y el acceso a la tercera planta alta.

Tabla N° 6. 21 Ubicación de las cámaras IP en el Tercer piso del GADMT

Elaborado por: El Investigador

e. Cuarto Piso

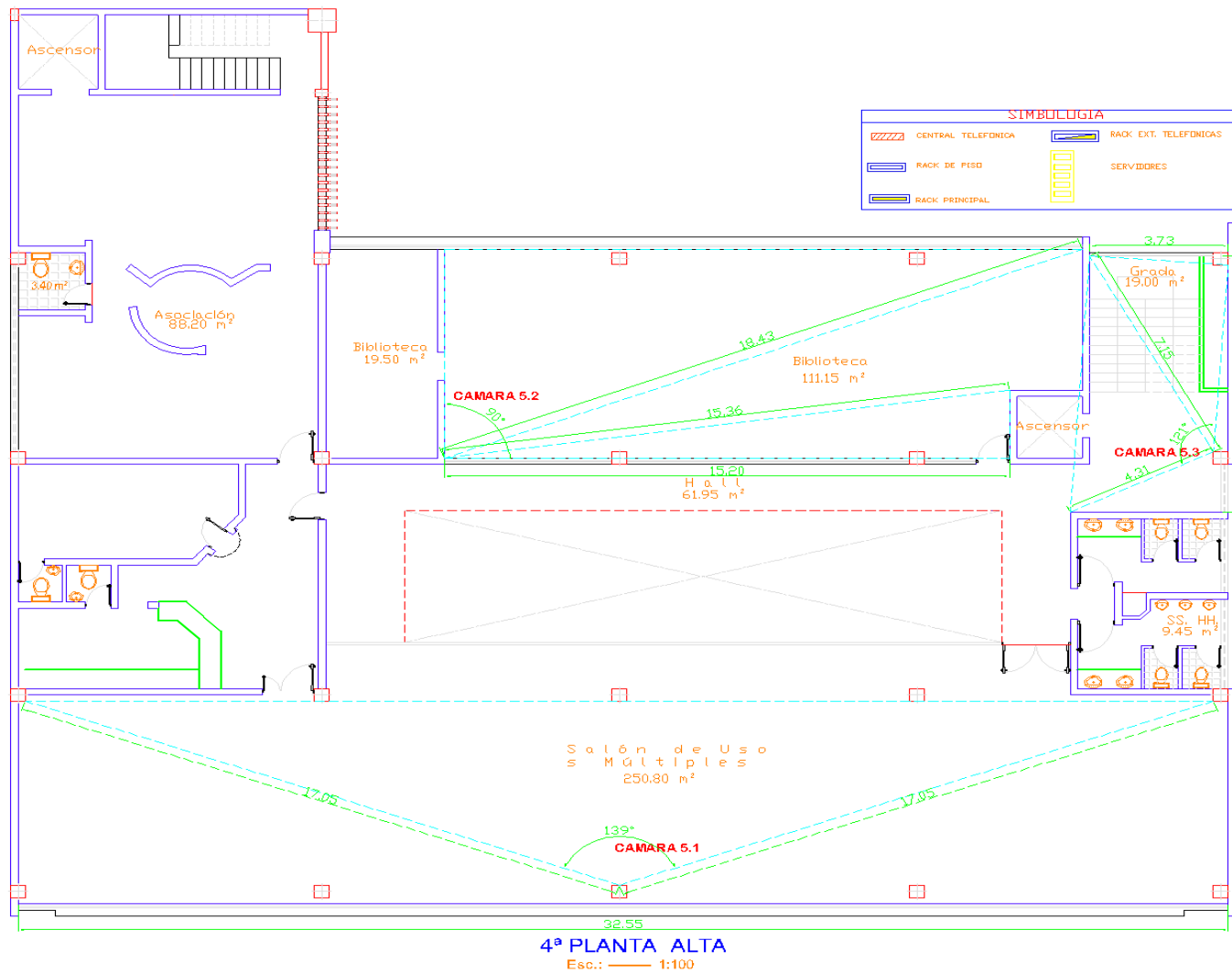


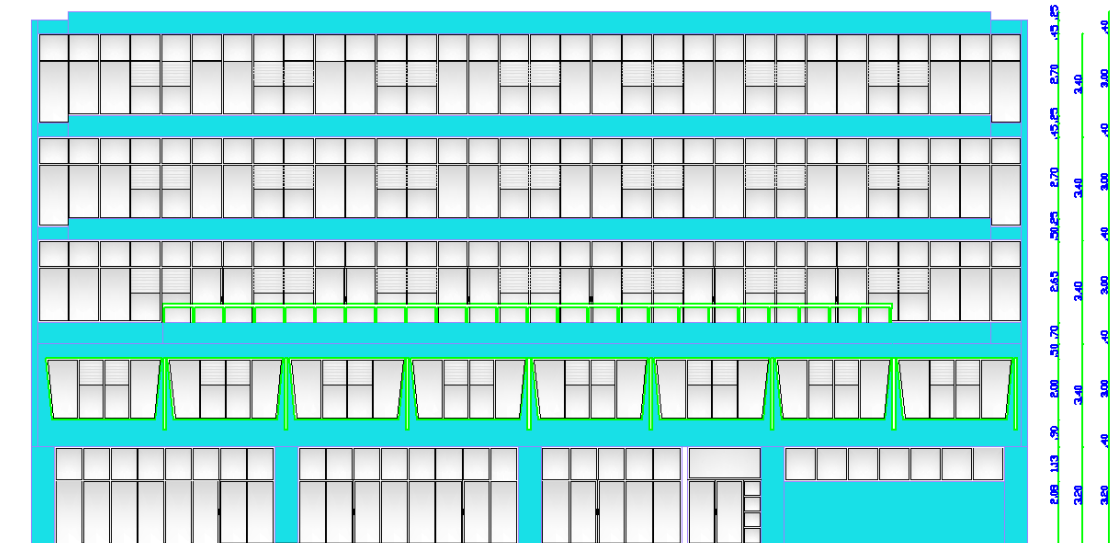
Figura N° 6. 18 Ubicación de las cámaras IP en el Cuarto piso del GADMT
Elaborado por: El Investigador

Nº DE CÁMARA	COBERTURA	DISTANCIA	DESCRIPCIÓN
CÁMARA 5.1	139°	17m	Cubre el Salón de Usos Múltiples, la entrada principal y la entrada proveniente de la cocina.
CÁMARA 5.2	90°	18m	Cubre la Biblioteca y su puerta de acceso.
CÁMARA 5.3	121°	7m	Cubre el área de las gradas y el acceso a la cuarta planta alta.

Tabla N° 6. 22 Ubicación de las cámaras IP en el Cuarto piso del GADMT
Elaborado por: El Investigador

6.9.1.3 Fachada frontal del GADMT

La altura del edificio Municipal es de 17 metros divididos en cinco pisos de aproximadamente 3.40 metros. En la figura N° 6.19 se observa la Fachada frontal del edificio del GADMT.



CORTE FACHADA CALLE OLMEDO
Esc.: 1:100

Figura N° 6. 19 Fachada Frontal del GADMT
Elaborado por: El Investigador

6.9.1.4 Características de las cámaras requeridas

En la tabla N° 6.23, se registran las características principales que deben poseer las cámaras para las zonas determinadas, de acuerdo a las necesidades de la institución.

ZONA	TIPO DE CÁMARA	# DE CÁMARA	CARACTERÍSTICAS
OFICINAS Y LA BIBLIOTECA	FIJA (cobertura<90)	1.3 - 1.4 - 1.5 - 2.1 - 2.2 - 3.2 - 3.4 - 3.5 - 4.1 - 4.3 - 4.5 - 4.6 - 4.7 - 5.2	Cámara para interiores Visibilidad nocturna Grabación de video de alta calidad Excelente resolución de hasta 30 fotogramas por segundo Detección de movimiento o señal de entrada digital, envía en tiempo real grabaciones de video vía FTP o correo electrónico Tipo de grabación basado en eventos, continuo y programado IEEE 802.3af Alimentación por Ethernet (PoE)
OFICINAS Y EL SALÓN DE USOS MÚLTIPLES	PTZ (cobertura>90)	1.1 - 1.2 - 2.3 - 2.4 - 2.5 - 3.1 - 3.3 - 4.2 - 4.4 - 4.8 - 5.1	Cámara para interiores Visión nocturna Grabación de video de alta calidad Excelente resolución de hasta 30 fotogramas por segundo Disparador de eventos: detección de movimiento o señal de entrada digital Envía en tiempo real grabaciones de video vía FTP o correo electrónico. IEEE 802.3af Alimentación por Ethernet(PoE)
HALL Y ACCESO PRINCIPAL A CADA PLANTA DEL GADMT	PTZ Inalámbrica (estéticamente factible)	1.6 - 2.6 - 3.6 - 4.9 - 5.3	Cámara para interiores Wi-Fi compatible con redes IEEE 802.11b/g/n Grabación de video de alta calidad Excelente resolución de hasta 30 fotogramas por segundo Visión nocturna Alertas por correo electrónico y subida de imágenes vía FTP accionadas por detección de movimientos Tipo de grabación: continua, programada o por detección de movimiento con software

Tabla N° 6. 23 Características de las cámaras IP para las zonas determinadas
Elaborado por: El Investigador

6.9.1.5 Análisis de equipos vigentes en el mercado

Existen numerosas alternativas de productos para la implementación del sistema de video-vigilancia a través de cámaras IP. Por lo que a continuación se realiza un análisis para determinar la mejor solución en el diseño de la red, para este propósito se ha escogido tres marcas de productos de vigilancia reconocidas como son: VIVOTEK, TRENDnet y Vstarcam.

Esta elección se efectúa teniendo en cuenta las funcionalidades, características, utilidad, calidad de servicio y precios de las diversas gamas de productos elegidos.

A continuación se presentan las marcas y modelos de cámaras IP seleccionadas:

a. VIVOTEK FD8134



Figura N° 6. 20 VIVOTEK FD8134

Fuente: <http://www.vivotek.es/products/show/102/domo-ip-h-264-d%C3%ADa-noche-ir-10-m-resoluci%C3%B3n-1-mpixel>

Como se observa en la figura N° 6.20, la VIVOTEK FD8134 es una cámara IP, tipo domo fija, fácil de instalar y usar, diseñada específicamente para aplicaciones de seguridad en interiores, tiene un diseño compacto y estilizado. Está equipada con un sensor de 1MP, permitiendo la visualización en una resolución 1280x800 a 30 fps, iluminador IR con alcance 10 m.

La cámara es compatible con el estándar de tecnología de compresión H.264, reduciendo drásticamente los tamaños de archivo y permitiendo un ahorro en el ancho de banda de la red. También dispone de compresión MPEG4 y MJPEG, permitiendo la transmisión de los streams de vídeo en cualquiera de estos formatos para diferentes usos. Los usuarios pueden recibir varias secuencias de vídeo simultáneamente en diferentes resoluciones, velocidad, y calidades de imagen para ser vistas en diferentes plataformas.

También se incluyen una serie de características avanzadas que son estándar para las cámaras de VIVOTEK, incluyendo detección anti sabotaje, ranura para almacenamiento Micro SD/SDHC, PoE 802.3af, y el software de gestión y grabación de 32 canales de VIVOTEK. Con todas estas capacidades, la FD8134 es una herramienta ideal para aplicaciones de vigilancia IP en interiores, como oficinas, bancos, cajeros automáticos, y tiendas.

b. VIVOTEK FD7132



Figura N° 6. 21 VIVOTEK FD7132

Fuente: <http://www.vivotek.com/web/product/productdetail.aspx?model=fd7132>

La Domo FD7132 de Vivotek, es una cámara Día/Noche dotada de iluminador IR (alcance 15 metros) y con posicionamiento triaxial, diseñada para la vigilancia de interiores. Dispone de una lente varifocal de gran ángulo lo que permite disponer de una visión de gran cobertura. Mediante el sofisticado sistema mecánico de 3 ejes y diseño industrial, resulta muy fácil su instalación tanto en paredes como en techos.

En la figura N° 6.21 se muestra la VIVOTEK FD7132. Para prevenir falsas alarmas, está dotada de un detector PIR (Infrarrojo pasivo), que permite detectar movimientos por los cambios de temperatura y por la emisión infrarroja en los objetos circundantes. El Circuito integrado de VIVOTEK VVTK-1000 Soc, permite de forma simultanea entregar de forma dual streams de Video simultáneos de hasta 30 fps con diferentes resoluciones y calidades a través de diferentes dispositivos multimedia para una visualización en tiempo real.

De forma adicional, ofrece características avanzadas tales como la vigilancia a través de móviles 3GPP, PoE 802.3af integrado, Audio bidireccional, y mas cosas, la FD7132 permite a los usuarios, de forma sencilla, la construcción de un sistema de vigilancia potente.

c. VIVOTEK PZ7132



Figura N° 6. 22 VIVOTEK PZ7132

Fuente: <http://www.vivotek.com/web/product/productdetail.aspx?model=pz7132>

La Cámara Inalámbrica PZ7132 exhibida en la figura N° 6.22, es de alto rendimiento y está equipada con un sensor de imagen CMOS, es la mejor opción para crear una red altamente confiable de vigilancia en tiendas, oficinas o seguridad de bancos.

La VIVOTEK PZ7132, que está equipada con una antena integrada que soporta 802.11 b/g, es una solución rentable pan / tilt / zoom para aplicaciones de vigilancia en interiores, como las tiendas de autoservicio. Integra un motor paneo y zoom óptico de 2.6x, que puede acercar y alejar para ver objetos cercanos o distantes. Posee movimiento horizontal de 350° y movimiento vertical de 125°, lo cual ofrece a los usuarios una amplia zona de vista.

La cámara puede emitir simultáneamente dos flujos de vídeo de vigilancia (Dual Stream) en tiempo real en cualquiera de los dos formatos de resolución MJPEG o MPEG-4. La PZ7131 es compatible con la norma IEEE 802.3af PoE (Power-over-Ethernet), haciendo la instalación más fácil y más rentable. Viene con un poderoso sistema de grabación y monitoreo que soporta hasta 32 canales lo que ayuda a los usuarios a crear un poderoso sistema de vigilancia.

d. VIVOTEK SD8121



Figura N° 6. 23 VIVOTEK SD8121

Fuente: <http://www.vivotek.es/products/show/107/speed-domo-ip-h-264-zoom-12x-d%C3%ADa-noche-instalaci%C3%B3n-en-interiores>

El Speed Domo IP SD8121 de VIVOTEK está equipado con una lente con Zoom óptico 12 X, es un Speed Domo Día/Noche de altas prestaciones pensado para aplicaciones en vigilancia profesional, siendo otro elemento significativo dentro de la gama profesional H.264 de VIVOTEK.

Con sensor CCD EXView de tecnología SONY, da imágenes extremadamente nítidas sin bordes dentados de objetos en movimiento. Dispone de un sofisticado sistema de Pan-Tilt con 360° de giro "sinfin" en horizontal, y 90° en vertical.

Equipada con la tecnología WDR (Wide Dynamic Range) la SD8121 expuesta en la figura N° 6.23, puede afrontar cualquier condición de luz cambiante. Otras funciones adicionales avanzadas, incluidas la vigilancia desde móviles 3GPP, Audio bidireccional, E/S digital para sensores y alarma. Es ideal para cualquier nivel de proyecto en empresas, como aeropuertos, centros comerciales, donde son imprescindibles niveles altos de fiabilidad y precisión.

e. TRENDnet TV-IP572PI



Figura N° 6. 24 TV-IP572PI

Fuente: http://www.trendnet.com/langsp/products/proddetail.asp?prod=185_TV-IP572PI&cat=179

La Cámara de internet PoE Megapíxel para día y noche, modelo, TV-IP572PI, mostrada en la figura N° 6.24, transmite en tiempo real videos de resolución megapíxel por Internet. Grabación de video con nitidez en plena oscuridad para distancias de hasta 7.5 metros. No necesita instalar la cámara cerca de una fuente de alimentación, ya que tanto los datos como la corriente se transmiten a través de un mismo cable Ethernet gracias a la tecnología Alimentación por Ethernet (PoE).

Graba videos 1280 x 800 Megapíxel (WXGA) de hasta 30 fotogramas por segundo (fps). Administra hasta cuatro video-perfiles para grabar videos de alta definición al mismo tiempo que transmite en tiempo real videos de baja resolución a un teléfono inteligente compatible. Controle hasta 32 cámaras TRENDnet con el software complementario para gestión de cámara. Las características avanzadas incluyen zonas para la grabación por detección de movimientos, alertas por correo electrónico, grabaciones programadas, compresión de imagen H.264 / MPEG-4 / MJPEG, audio de dos vías, superposición de fecha y hora, ranura para tarjetas Micro-SD para el almacenamiento de copias de seguridad, audio de dos vías (no incluye altavoces), lentes ajustables y zoom digitales 4x. Viene con kit para montaje en pared o techo y la carcasa en blanco crema de la cámara combina a la perfección con la mayoría de los ambientes.

f. TRENDnet TV-IP672PI



Figura N° 6. 25 TV-IP672PI

Fuente: http://www.trendnet.com/langsp/products/proddetail.asp?prod=195_TV-IP672PI&cat=181

La Cámara de internet PoE Megapíxel PTZ para día / noche, modelo TV-IP672PI de TRENDnet indicada en figura N° 6.25, ofrece vigilancia de seguridad durante el día y la noche dentro de un área muy amplia. Permite el movimiento de la cámara de un lado a otro en un ángulo de 340° e inclinación hacia arriba o hacia abajo unos 115° desde cualquier conexión a Internet. Grabación de video con nitidez en plena oscuridad para distancias de hasta 7.5 metros. No necesita instalar la cámara cerca de una fuente de alimentación, ya que tanto los datos como la corriente se transmiten a través de un mismo cable Ethernet gracias a la tecnología Power over Ethernet (PoE).

Graba videos 1280 x 800 Megapixel (WXGA) de hasta 30 fotogramas por segundo (fps). Administra hasta cuatro video-perfiles para grabar videos de alta definición al mismo tiempo que transmite en tiempo real videos de baja resolución a un teléfono inteligente compatible. Controla hasta 32 cámaras TRENDnet con el software complementario para gestión de cámara. Las características avanzadas incluyen zonas para la grabación por detección de movimientos, alertas por correo electrónico, grabaciones programadas, vigilancia automática con movimiento vertical y horizontal (giro / inclinación), patrulla automática, compresión de imagen H.264 / MPEG-4 / MJPEG, audio de dos vías, superposición de fecha y hora, ranura para tarjetas Micro-SD para el almacenamiento de copias de seguridad, audio de dos vías (no incluye altavoces), lentes ajustables y zoom digitales 4x. Viene con kit para montaje en pared o techo y la carcasa en blanco crema de la cámara combina a la perfección con la mayoría de los ambientes.

g. TRENDnet TV-IP422WN



Figura N° 6. 26 TV-IP422WN

Fuente: http://www.trendnet.com/langsp/products/proddetail.asp?prod=190_TV-IP422WN&cat=181

La cámara de Internet inalámbrica denotada en la figura N° 6.26, con movimiento horizontal y vertical para día/noche SecurView, modelo TV-IP422WN, ofrece protección durante el día y la noche sobre un área extensa. Permite el movimiento de la cámara de un lado a otro en un ángulo de 330 grados e inclinación hacia arriba o hacia abajo unos 105 grados.

La tecnología inalámbrica N ofrece cobertura inalámbrica sin igual, así como una mejor calidad de video en tiempo real. Las bombillas de infrarrojos garantizan la visión nocturna en plena oscuridad a distancias de hasta 5 metros (16 pies). Un micrófono integrado y altavoces opcionales permiten la comunicación de audio de 2 vías. Controla hasta 32 cámaras SecurView con el software complementario para gestión de cámara. Las características avanzadas de la cámara incluyen grabación por detección de movimientos, alertas de correo electrónico, sesiones de grabación programadas, compresión de imágenes MPEG-4/MJPEG, soporte 3GPP, un puerto USB opcional, vigilancia automática predeterminada, puertos de entrada y salida, y zoom digital Viene con kit para montaje en pared o techo y la carcasa en blanco crema de la cámara combina a la perfección con la mayoría de los ambientes.

h. Vstarcam H6812I



Figura N° 6. 27 Vstarcam H6812I

Fuente: <http://www.vstarcam.com/Indoor-IR-Dome-IP-Camera-74.html/>

Cámara para interior, ideal para hogares, tiendas, oficinas. Soporta 10 idiomas. Formato de compresión H.264, Sensor CMOS de 1/4 de pulgada, iluminación Auto IR-LED para visión nocturna que alcanza los 20 metros.

La Vstarcam H6812I puede apreciarse en la figura N° 6.27, tiene soporte de monitoreo a través de dispositivos móviles en línea (como iOS, el sistema operativo Android, el sistema operativo Symbian, WindowsPhone7), Alarma telefónica y de mensaje de Skype.

Soporta detección de movimiento, salida externa a alarma, email, ftp cuando la alarma es activada.

i. Vstarcam F6836w



Figura N° 6. 28 Vstarcam F6836w

Fuente: <http://www.vstarcam.com/Indoor-PTZ-Dome-IP-Camera-20.html>

La Vstarcam F6836w exhibida en la figura N° 6.28, soporta 10 idiomas, 9-canales vía navegador web, 64-canales vía Super-Client software, Búsqueda automática de equipos, control remoto, mensaje de alarma vía E-mail, Alarma Skype, Interfaz amigable; compatible con los estándares Wi-Fi IEEE 802.11b/g.

La visión remota permite grabar y ver desde cualquier lugar a cualquier hora. Soporta rotación Pan/Tilt de diferentes ángulos (Pan: 270& Tilt:90); Audio de 2 vías.

Iluminación Auto IR-LED para visión nocturna (sobre los 10 metros); soporta detección de movimiento, salida externa a alarma, email, ftp cuando la alarma es activada.

6.9.1.6 Cuadros comparativos: especificaciones técnicas de las cámaras IP

En las tablas desde la N° 6.24, hasta la N° 6.27, se detallan las especificaciones técnicas más relevantes referentes a los tipos y modelos de cámaras IP elegidas para el análisis, teniendo en cuenta la zona de ubicación y cobertura requerida.

Estableciéndose así un marco comparativo; permitiendo definir el tipo de cámara que más se ajuste a los requerimientos de la red de video-vigilancia IP, para lo cual se realiza un análisis metódico de las características, aplicaciones y particularidades que posee cada marca.

ANÁLISIS TÉCNICO: CÁMARA FIJA REQUERIDA EN LAS OFICINAS DEL GADMT

ANÁLISIS TÉCNICO: CÁMARA FIJA REQUERIDA EN LAS OFICINAS DEL GADMT			
Marca y Modelo	VIVOTEK FD8134	TRENDnet TV-IP572PI	Vstarcam H6812I
Tipo	domo fija	Posición fija	Domo fija
Sensor de imagen	1/4" CMOS	Sensor CMOS de 1/4 de pulgada	Sensor CMOS de 1/4 de pulgada
Resolución máxima de video	1280 x 800 pixels	1280 x 800 píxeles	VGA (640×480): QVGA (320×240)
Lente	f = 3,6 mm F 1.8	Distancia focal: 4 mm F/No: 1.5	f= 6mm
Iluminación mínima	0 Lux , F1.8, (IR LED On)	0 lux	0.3Lux
Visión	56° (horizontal), 41° (vertical)	Horizontal: 51.8°, Vertical: 33.8°, Diagonal: 59.6°	
Día / Noche	Filtro de corte IR amovible para la función día y noche 8 Iluminadores IR LED Integrados Alcance 10 m.	Construido en ICR Visión nocturna (IR) de hasta 7.5 metros	Iluminación Auto IR-LED para visión nocturna(sobre los 20 metros)
Compresión	H.264, MPEG-4 y MJPEG	H.264 / MPEG-4/MJPEG	H.264
Tasa de Velocidad	H.264: hasta 25 fps a 1280x800 MPEG-4: hasta 25 fps a 1280x800 MJPEG: hasta 25 fps a 1280x800	30fps	30fps
Temperatura	0 ~ 50 °C (32 ~ 122 °F)	Funcionamiento: 0°C ~ 40°C (32°F ~ 104°F) Almacenaje: -25°C ~ 70°C (-13°F ~ 158°F)	-10~50°C
Acción de eventos	Triple-ventana de detección de movimiento - Entrada Digital para sensor externo de alarma - Notificación de eventos por HTTP, SMTP, o FTP - Grabación local en ficheros MP4 - Detección de sabotaje	Evento disparador: detección de movimiento o entrada de señal digital Acción: envía en tiempo real instantáneas o grabaciones de video vía FTP o correo electrónico Tipo de grabación: basado en eventos, continuo y programado	Soporta detección de movimiento Salida externa a alarma, email, ftp cuando la alarma es activada Alarma Skype Programación de eventos
Red	10/100 Mbps Ethernet, RJ-45 Soporta ONVIF	IEEE 802.3u 10/100 Mbps Auto-MDIX Fast Ethernet	Ethernet de RJ-45 10/100Mb
Alimentación	12V CC Potencia: Max. 3,5 W Integra PoE 802.3af (Clase 2)	Entrada: 120~240V AC, 50~60 Hz, 0.2A Salida: Adaptador de alimentación externo 1.2A y 5V IEEE 802.3af Alimentación por Ethernet (PoE)	DC 5V 6W
Garantía	24 meses	36 meses	12 meses

Tabla N° 6. 24 Análisis técnico: cámara fija requerida en las oficinas del GADMT

Elaborado por: El Investigador

ANÁLISIS TÉCNICO: CÁMARA FIJA REQUERIDA EN LA BIBLIOTECA DEL GADMT

ANÁLISIS TÉCNICO: CÁMARA FIJA REQUERIDA EN LA BIBLIOTECA DEL GADMT			
Marca y Modelo	VIVOTEK FD7132	TRENDnet TV-IP572PI	Vstarcam H6812I
Tipo	domo fija	Posición fija	Domo fija
Sensor de imagen	1/4" CMOS	Sensor CMOS de 1/4 de pulgada	Sensor CMOS de 1/4 de pulgada
Resolución máxima de video	VGA Resolución (640 x 480 píxeles)	1280 x 800 píxeles	VGA (640x480): QVGA (320x240)
Lente	f=3.3 ~ 12 mm F 1.4 (wide) F 2.9 (tele)	Distancia focal: 4 mm F/No: 1.5	f= 6mm
Iluminación mínima	0.56 Lux / F1.4 (typical) 0 Lux / F1.4 (IR LED on)	0 lux	0.3Lux
Visión	17.9° ~ 63.6° (horizontal) 13.5° ~ 46.5° (vertical)	Horizontal: 51.8° Vertical: 33.8° Diagonal: 59.6°	
Día / Noche	Filtro de corte IR amovible para la función día y noche. IR LED*12 (850 nm). Alcance 15 metros	Construido en ICR Visión nocturna (IR) de hasta 7.5 metros	Iluminación Auto IR-LED para visión nocturna(sobre los 20 metros)
Compresión	MJPEG & MPEG-4	H.264 / MPEG-4/MJPEG	H.264
Tasa de Velocidad	MPEG-4: Up to 30/25 fps at 640x480 MJPEG: Up to 30/25 fps at 640x480	30fps	30fps
Temperatura	Temperatura: 0 ~ 50 °C (32 ~ 122 °F)	Funcionamiento: 0°C ~ 40°C (32°F ~ 104°F) Almacenaje: -25°C ~ 70°C (-13°F ~ 158°F)	-10~50°C
Acción de eventos	Triple-ventana de detección de movimiento Entrada y salida Digital para sensor externo y alarma - Notificación de eventos por HTTP, SMTP, o FTP - Grabación local en ficheros MP4 PIR (Sensor infrarrojo pasivo) para detección humana	Evento disparador: detección de movimiento o entrada de señal digital Acción: envía en tiempo real instantáneas o grabaciones de video vía FTP o correo electrónico Tipo de grabación: basado en eventos, continuo y programado	Soporta detección de movimiento Salida externa a alarma, email, ftp cuando la alarma es activada Alarma Skype Programación de eventos
Red	10/100 Mbps Ethernet, RJ-45	IEEE 802.3u 10/100 Mbps Auto-MDIX Fast Ethernet	Ethernet de RJ-45 10/100Mb
Alimentación	12V DC Power consumption: Max. 11 W 802.3af Power-over-Ethernet (Class 1)	Entrada: 120~240V AC, 50~60 Hz, 0.2A Salida: Adaptador de alimentación externo 1.2A y 5V IEEE 802.3af Alimentación por Ethernet (PoE)	DC 5V 6W
Garantía	24 meses	36 meses	12 meses

Tabla N° 6. 25 Análisis técnico: cámara fija requerida en la biblioteca del GADMT
Elaborado por: El Investigador

ANÁLISIS TÉCNICO: CÁMARA PTZ REQUERIDA EN LAS OFICINAS Y EL SALÓN DE USOS MÚLTIPLES DEL GADMT

ANÁLISIS TÉCNICO: CÁMARA PTZ REQUERIDA EN LAS OFICINAS Y EL SALÓN DE USOS MÚLTIPLES DEL GADMT			
Marca y Modelo	VIVOTEK SD8111	TRENDnet TV-IP672PI	Vstarcam F6836W
Tipo	Domo PTZ	PTZ	PTZ inalámbrica
Sensor de imagen	CCD 1/4", WDR Sony EXview HAD	Sensor CMOS de 1/4 de pulgada	0.3MegaPixel Color CMOS
Resolución máxima de video	resolución D1 (720 x 480 píxeles (NTSC))	1280 x 800 píxeles	VGA (640x480) /QVGA(320x240)
Lente	f=3,8 mm~45,6mm Autoiris F1.6 (G. Angular), F 2.8(Tele)	Distancia focal: 4 mm F/No: 1.5	f=3.6mm
Iluminación mínima	0.1 Lux / F1.6 (Color), 0.01 Lux / F1.6 (B/W)	0 lux	0.3Lux
Visión	1.7° ~ 55.8° (Horizontal)	Horizontal: 51.8°, Vertical: 33.8°, Diagonal: 59.6°	
PTZ Giro / Inclinación	. Pan range: 360° rotación continua . Tilt range: -10° ~ 190° flip	Giro: -170° ~ +170° Inclinación: hacia arriba 90° y hacia abajo 25° Posiciones predeterminada: 10	Pan: 355° Tilt: 120°
Día / Noche	Filtro IR removible automático para función día/noche	Construido en ICR Visión nocturna (IR) de hasta 7.5 metros	Iluminación Auto IR-LED para visión nocturna(sobre los 10 metros)
Zoom	Zoom: Óptico 12 X	Zoom: Digital 4x	
Compresión	H.264, MJPEG y MPEG-4	H.264 / MPEG-4/MJPEG	Motion-JPEG
Tasa de Velocidad	H.264: 720x480 hasta 30/25 fps MPEG4: 720x480 hasta 30/25 fps MJPEG: 720x480 hasta 30/25 fps	30fps	25fps
Temperatura	Temperatura: 0°C ~ 40°C (32°F ~ 104°F)	Funcionamiento: 0°C ~ 40°C (32°F ~ 104°F) Almacenaje: -25°C ~ 70°C (-13°F ~ 158°F)	-10~50°C
Acción de eventos	- Triple ventana de detección de movimiento - Cuatro entradas digitales, y una salida digital para sensor externo y alarma - Notificación de eventos mediante HTTP, SMTP, o FTP - Grabación local de ficheros MP4.	Evento disparador: detección de movimiento o entrada de señal digital Acción: envía en tiempo real instantáneas o grabaciones de video vía FTP o correo electrónico.	Soporta detección de movimiento Salida externa a alarma, email, ftp cuando la alarma es activada Alarma Skype Programación de eventos
Red	- Ethernet 10/100 Mbps , RJ-45 -Soporta ONVIF	IEEE 802.3u 10/100 Mbps Auto-MDIX Fast Ethernet	Ethernet de RJ-45 10/100Mb WIFI 802.11 b/g/n
Alimentación	. 12V DC . Power consumption: Max. 11.4 W	Entrada: 120~240V AC, 50~60 Hz, 0.2ª Salida: Adaptador alimentación externa 1.25A y 12V IEEE 802.3af Alimentación por Ethernet(PoE)	DC 5V 6W
Garantía	24 meses	36 meses	12 meses

Tabla N° 6. 26 Análisis técnico: cámara PTZ requerida en las oficinas y el salón de usos múltiples del GADMT

Elaborado por: El Investigador

ANÁLISIS TÉCNICO: CÁMARA PTZ INALÁMBRICA REQUERIDA EN EL HALL Y ACCESOS PRINCIPALES

ANÁLISIS TÉCNICO: CÁMARA PTZ INALÁMBRICA REQUERIDA EN EL HALL Y ACCESO PRINCIPAL A CADA PLANTA DEL GADMT			
Marca y Modelo	VIVOTEK PZ7132	TRENDnet TV-IP422WN	Vstarcam F6836W
Tipo	PTZ inalámbrica	PTZ inalámbrica	PTZ inalámbrica
Sensor de imagen	1/4" CMOS sensor	Sensor CMOS a color de 1/2.5 de pulgada	0.3MegaPixel Color CMOS
Resolución máxima de video	VGA Resolución (640 x 480 píxeles)	640 x 480 píxeles	VGA (640x480) /QVGA(320x240)
Lente	f = 2.8 ~ 7.3 mm F1.9	Distancia focal: 4.0mm Abertura (F/No): F1.8	f=3.6mm
Iluminación mínima	1.25 Lux / F1.9	0.5 Lux	0.3Lux
Visión	28.7° ~ 73.4° (horizontal), 21.6° ~ 54.7° (vertical), 35.8° ~ 92.2° (diagonal)	Ángulo de visualización en diagonal: 64 °	
PTZ Giro / Inclinación	Pan range: 350° (-175° ~ +175°) Tilt range: 125° (-35° ~ +90°)	Giro: +165~-165 ° Inclinación: +90 ~ -15 ° Posiciones predeterminada: 20	Pan: 355° Tilt: 120°
Día / Noche		LED de luz infrarroja con control de sensor de luz visión nocturna a distancias de hasta 5 metros	Iluminación Auto IR-LED para visión nocturna(sobre los 10 metros)
Zoom	2.6x optical zoom	Zoom: Digital 3x	
Compresión	MJPEG & MPEG-4	MPEG-4/MJPEG	Motion-JPEG
Tasa de Velocidad	MPEG-4: Up to 30/25 fps at 640x480 MJPEG: Up to 30/25 fps at 640x480	1~ 30 fps	25fps
Temperatura	Temperature: 0 ~ 50 °C (32 ~ 122 °F)	Funcionamiento: 0°C ~ 45°C (32°F ~ 113°F) Almacenaje: -15°C ~ 60°C (5°F ~ 140°F)	-10~50°C
Acción de eventos	Triple-ventana de detección de movimiento Entrada y salida Digital para sensor externo y alarma - Notificación de eventos por HTTP, SMTP, o FTP - Grabación local en ficheros MP4	Tipo de grabación: continua, programada o por detección de movimiento con software Guardar/recuperar los archivos de configuración Alertas por correo electrónico con un software complementario Entrada Digital para sensor externo de alarma	Soporta detección de movimiento Salida externa a alarma, email, ftp cuando la alarma es activada Alarma Skype Programación de eventos
Red	. 10/100 Mbps Ethernet, RJ-45 . Built-in 802.11b/g WLAN	IEEE 802.3u 10/100Mbps Fast Ethernet, Auto- MDIX Basado en la tecnología IEEE 802.11n compatible con redes IEEE 802.11b/g	Ethernet de RJ-45 10/100Mb WIFI 802.11 b/g/n
Alimentación	. 12V DC . Power consumption: Max. 12 W	10 watts max. Adaptador de alimentación externo 1.5A y 12V (3.5 mm plug)	DC 5V 6W
Garantía	24 meses	36 meses	12 meses

Tabla Nº 6. 27 Análisis técnico: cámara PTZ inalámbrica requerida en el hall y accesos principales
Elaborado por: El Investigador

6.9.1.7 Análisis técnico de las cámaras IP elegidas para el diseño

Las tablas N° 6.24 y la N° 6.25, presentan cuadros comparativos de las cámaras fijas requeridas en las oficinas, el salón de usos múltiples y la biblioteca del GADMT, para lo cual se llega a la conclusión que la TRENDnet TV-IP572PI es la solución más idónea ya que presenta mayores beneficios en cuanto a sus características y a costos accesibles con una garantía de 36 meses. Entre las características más relevantes tenemos:

- Visibilidad nocturna en un rango de hasta 7.5 metros,
- Ángulo de visión horizontal: 51.8°, vertical: 33.8° y Diagonal: 59.6°,
- Zoom digital de hasta 4x,
- Grabación de video H.264, MPEG-4 y MJPEG de alta calidad,
- Admite resolución de hasta 1280 x 800 píxeles a 30 fotogramas por segundo,
- Detección de movimiento o señal de entrada digital, envía en tiempo real grabaciones de video vía FTP o correo electrónico,
- Tipo de grabación basado en eventos, continuo y programado,
- IEEE 802.3af Alimentación por Ethernet (PoE)

En la tabla N° 6.26, se puede observar que la cámara PTZ VIVOTEK posee semejantes características a la PTZ TRENDnet. En tal virtud, debido a su mayor flexibilidad en costos y al tiempo de 36 meses establecidos en la garantía, se elige la cámara TRENDnet TV-IP672PI como la mejor opción para ser ubicada en las oficinas que lo requieren. Con las siguientes especificaciones:

- Visión nocturna de hasta 7.5 metros en interiores
- Ángulo de visión horizontal: 51.8°, vertical: 33.8°, diagonal: 59.6°
- Audio de 2 vías: Micrófono integrado y puerto de salida de audio para altavoces de terceros
- Giro hacia la izquierda o la derecha de 170°, para un total de 340°

- La cámara se mueve hacia arriba en un ángulo de 90° y hacia abajo unos 25°, para un total de 115°
- Zoom digital de hasta 4x
- Admite resolución de hasta 1280 x 800 píxeles a 30 fotogramas por segundo
- Disparador de eventos: detección de movimiento o señal de entrada digital
- Envía en tiempo real grabaciones de video vía FTP o correo electrónico.
- IEEE 802.3af Alimentación por Ethernet(PoE)

En el Hall y accesos principales del edificio municipal se requiere una cámara PTZ inalámbrica para brindar un entorno estéticamente atractivo, libre de cableado y de este modo aprovechar también la red inalámbrica existente en la entidad. De este modo observando la tabla N° 6.27, se llega a la conclusión que la TRENDnet TV-IP422WN cumple con los requerimientos necesarios para el diseño del sistema de vigilancia IP en cuanto a características, precios y a 36 meses de garantía. Con las siguientes descripciones:

- Wi-Fi compatible con redes IEEE 802.11b/g/n
- Ángulo de visualización en diagonal: 64 °
- Pan: 330 grados, Tilt: 105 grados
- Zoom digital 3x
- Grabación de video MPEG-4 y MJPEG de alta calidad
- Resolución de hasta 640 x 480 píxeles
- Visión nocturna por infrarrojos hasta 5 metros (16 pies)
- Alertas por correo electrónico y subida de imágenes vía FTP accionadas por detección de movimientos
- Tipo de grabación: continua, programada o por detección de movimiento con software.

En la tabla N° 6.28 se define el modelo de cámara IP a utilizarse por cada Unidad del GADMT.

DIRECCIÓN/UNIDAD	CÁMARA	
	#	MODELO
PLANTA BAJA		
RECAUDACIÓN	1.1	TRENDnet TV-IP672PI
CAFE NET	1.2	TRENDnet TV-IP672PI
COMISARÍA	1.3	TRENDnet TV-IP572PI
BODEGA	1.4	TRENDnet TV-IP572PI
BIENES Y ACTIVOS	1.5	TRENDnet TV-IP572PI
HALL	1.6	TRENDnet TV-IP422WN
PRIMER PISO		
PLANIFICACIÓN URBANA	2.1	TRENDnet TV-IP572PI
PROYECTOS	2.2	TRENDnet TV-IP572PI
ZONAS AZULES	2.3	TRENDnet TV-IP672PI
AVALUOS Y CATASTROS	2.4	TRENDnet TV-IP672PI
GESTIÓN AMBIENTAL Y RIESGOS	2.5	TRENDnet TV-IP672PI
GRADAS E INGRESO AL 1º PISO	2.6	TRENDnet TV-IP422WN
SEGUNDO PISO		
DIRECCIÓN FINANCIERA Y COACTIVAS	3.1	TRENDnet TV-IP672PI
CONTABILIDAD	3.2	TRENDnet TV-IP572PI
PLANEACIÓN ESTRATÉGICA	3.3	TRENDnet TV-IP672PI
COMUNICACIÓN Y PROTOCOLO	3.4	TRENDnet TV-IP572PI
SALA DE ESPERA ALCALDÍA	3.5	TRENDnet TV-IP572PI
GRADAS E INGRESO AL 2º PISO	3.6	TRENDnet TV-IP422WN
TERCER PISO		
TALENTO HUMANO	4.1	TRENDnet TV-IP572PI
INFORMÁTICA	4.2	TRENDnet TV-IP672PI
SALA DE TELECOMUNICACIONES	4.3	TRENDnet TV-IP572PI
FISCALIZACIÓN	4.4	TRENDnet TV-IP672PI
OBRAS PÚBLICAS	4.5	TRENDnet TV-IP572PI
SINDICATURA	4.6	TRENDnet TV-IP572PI
COMPRAS PÚBLICAS	4.7	TRENDnet TV-IP572PI
DESARROLLO SOSTENIBLE	4.8	TRENDnet TV-IP672PI
GRADAS E INGRESO AL 3º PISO	4.9	TRENDnet TV-IP422WN
CUARTO PISO		
SALÓN MÚLTIPLE	5.1	TRENDnet TV-IP672PI
BIBLIOTECA	5.2	TRENDnet TV-IP572PI
GRADAS E INGRESO AL 4º PISO	5.3	TRENDnet TV-IP422WN

Tabla N° 6. 28 Modelo de cámara IP a utilizarse por cada Unidad del GADMT

Elaborado por: El Investigador

6.9.1.8 Características software y hardware para la gestión de video

a. Software administrador de cámaras

- **IP es SecurView Pro**

El nuevo software gratuito de TRENDnet para gestión de cámaras IP SecurView Pro establece un nuevo estándar de rendimiento y características.

Este software es compatible con todos los modelos de cámara IP de TRENDnet actuales y se introducirá gradualmente en todos los embalajes de cámaras IP existentes en los meses posteriores. SecurView Pro es compatible con Windows 7, Windows XP, Windows Vista, Microsoft Server 2003 y Microsoft Server 2008, además ofrece baja carga de la CPU y puede gestionar hasta 32 cámaras IP de TRENDnet.

Además ofrece a los usuarios amplias opciones de visualización de la cámara, tales como modos de visualización predeterminados, diseños de visualización personalizados y modo de pantalla completa. Barras de herramienta laterales, en la parte inferior y superior que se pueden ocultar para aumentar el campo visual del video. Los administradores pueden arrastrar y soltar imágenes en directo hacia una nueva ubicación; definir ciclos de visualización de la cámara y llevar el video con movimiento al frente de la pantalla de visualización.

Los usuarios pueden definir una combinación de programas de grabación semanales y grabación por detección de movimiento; programar áreas de detección de movimiento de cualquier forma; integrar disparadores de eventos al sistema de alarma de cámaras IP; establecer fecha, hora y superposiciones de texto por cámara; y definir la superposición de máscara para ocultar áreas sensibles.

Este software proporciona cero pérdidas de arquitectura con la capacidad para grabar una secuencia de vídeo única en varias ubicaciones al mismo tiempo. Gestiona archivos de grabación por hora de grabación o asignación de espacio. Las útiles estadísticas de grabación ayudan a gestionar los archivos y la característica de limpieza de disco condensa y optimiza los archivos antiguos.

La función de búsqueda y reproducción es muy avanzada. La secuencia de navegación proporciona una referencia visual rápida de contenido grabado mediante la visualización de video y movimiento grabados en un momento específico. Los usuarios pueden ahorrar mucho tiempo si utilizan la opción de búsqueda de grabaciones continuas de eventos de movimiento, dentro de un área definida del campo visual. El lapso de tiempo en la reproducción proporciona otra opción de búsqueda útil. La función de mapa permite a los usuarios asignar cámaras a una imagen como el plano de la planta de una oficina o en Google Maps™. En las figuras N° 6.29 y N° 6.30, se observan la Interfaz gráfica del software SecurView Pro y la captura de video gestionado por el mismo.

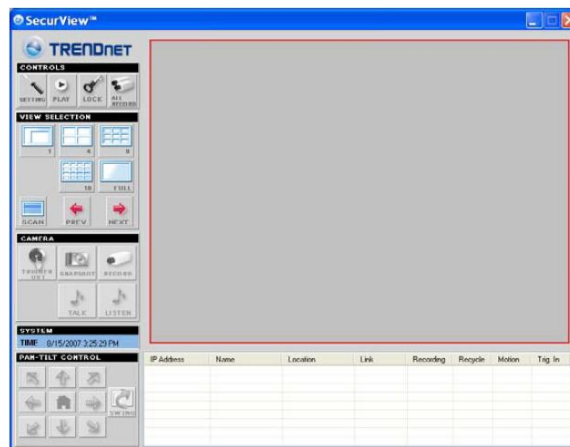


Figura N° 6. 29 Interfaz gráfica del software SecurView Pro
Fuente: Guía del usuario TRENDnet TV-IP422WN

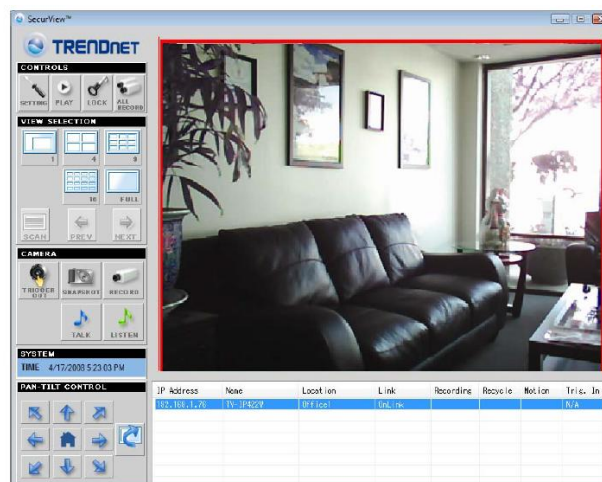


Figura N° 6. 30 Captura de video gestionado con el software SecurView Pro
Fuente: Guía del usuario TRENDnet TV-IP422WN

- **Características del software para cámara SecurView Pro**

1. Gestión de hasta 32 cámaras
2. Compatible con Windows y Microsoft Server 2003 y 2008
3. Soporte multilingüe
4. Visualización de la cámara
 - Modos de visualización predeterminados
 - Programación de modos de visualización personalizados
 - Vista de pantalla completa
 - Permite arrastrar y soltar imágenes en directo a una nueva ubicación
 - Programación de secuencia de visualización de ciclos de la cámara
 - Detección de movimiento que permite traer videos hacia adelante
 - Barras de herramientas laterales, en la parte superior e inferior que se pueden ocultar
 - Acceso basado en Web a través de tabletas y teléfonos inteligentes
5. Opciones de grabación
 - Programación de grabaciones semanales
 - Grabación por detección de movimiento: Define las áreas de detección de movimiento de cualquier forma y la sensibilidad de la detección de movimiento
 - Grabación mediante disparador de eventos
 - Fecha y hora de la toma
 - Superposición de mascara para ocultar áreas sensibles
 - Permite guardar una secuencia de video en múltiples ubicaciones al mismo tiempo
 - Definición de cuotas de grabación por tiempo de grabación o asignación de espacio
 - La característica de limpieza de disco condensa y optimiza archivos antiguos
 - Estadísticas de grabación en tiempo real para ayudar a administrar los archivos

6. Búsqueda y reproducción

- Barra de navegación que ofrece una rápida referencia visual del contenido grabado
- Búsqueda de grabaciones continuas por movimiento
- Búsqueda de grabaciones por movimiento dentro de un campo definido (una parte del área de visualización)
- Búsqueda de lapsos de tiempo en la reproducción

7. Ofrece un mapa de las cámaras en una imagen como una planta

8. Ofrece un mapa de las cámaras en Google Maps™

9. Software SecurView Pro gratis: gestiona hasta 32 cámaras

b. Hardware para la gestión de video

1. Requisitos mínimos del sistema

- Un PC con adaptador de red instalado de manera correcta
- Unidad de CD-ROM
- Resolución VGA: 800 x 600 o superior
- Navegador Web: Internet Explorer (6.0 ó superior), Firefox, Safari, y Chrome

2. Características del servidor de video

La tabla N° 6.29, presenta las características mínimas requeridas por el computador que actuará como servidor de video del sistema.

Compatible con sistemas operativos	1-8 cámaras		9-32 cámaras	
	CPU	Memoria	CPU	Memoria
Windows 7 (32/64-bit)	Intel Core 2 Duo	2GB RAM o superior	Intel Core 2 Quad	4GB RAM o superior
Windows Vista (32/64-bit)	Intel Core 2 Duo	2GB RAM o superior	Intel Core 2 Quad	4GB RAM o superior
Windows XP (32/64-bit)	Intel Core 2 Duo	2GB RAM o superior	Intel Core 2 Quad	4GB RAM o superior
Windows Server 2008	2GHz	2GB RAM o superior	2GHz	4GB RAM o superior
Windows Server 2003	2GHz	2GB RAM o superior	2GHz	4GB RAM o superior

Tabla N° 6. 29 Características del servidor de video
Elaborado por: El Investigador

2.1. Almacenamiento de video/estimación de la capacidad de disco duro

Las cámaras seleccionadas para la red de video-vigilancia IP del GADMT se configurarán por detección de movimiento, estableciéndose un promedio para cada cámara de 10 horas de grabación por día.

ZONA	ID CÁMARA	# CAM	GRABACIÓN	HORAS/DÍA (c/u)	HORAS/DÍA (total)
1. PLANTA BAJA	1.1 - 1.6	6	Detección de movimiento	10	60
2. PRIMER PISO	2.1 - 2.6	6	Detección de movimiento	10	60
3. SEGUNDO PISO	3.1 - 3.6	6	Detección de movimiento	10	60
4. TERCER PISO	4.1 - 4.9	9	Detección de movimiento	10	90
5. CUARTO PISO	5.1 - 5.3	3	Detección de movimiento	10	30
TOTAL CÁMARAS		30	TOTAL HORAS/DÍA DEL SISTEMA		300

Tabla N° 6. 30 Almacenamiento de video

Elaborado por: El Investigador

De los datos presentados en la tabla N° 6.30, se indica que para un total de 30 cámaras, diariamente se almacenarán aproximadamente 300 horas de grabación.

Para determinar el espacio del disco duro requerido para el almacenamiento de video, se toma de referencia la Tabla N° 6.3, la cual muestra valores estimados de las ratas de bits generadas en el formato de compresión MPEG-4, debido a que la mayoría de los gestores de video lo poseen. Se toma de punto de partida el nivel de actividad medio, el tamaño de resolución es CIF, la velocidad binaria aproximada de 200 Kbps, las imágenes por segundo de 15, y 10 horas de funcionamiento. A continuación se presentan los cálculos a realizarse con la información extraída.

$$KB/hora = \frac{Velocidad\ binaria\ aprox.}{8} \times 3600s$$

$$KB/hora = \frac{200Kb}{8} \times 3600s = 90000KB/hora$$

$$MB/hora = \frac{KB/hora}{1000}$$

$$MB/hora = \frac{90000KB/hora}{1000} = 90MB/hora$$

$$GB/día = \frac{MB/hora \times horas\ de\ funcionamiento\ diarias}{1000}$$

$$GB/día = \frac{90MB/hora \times 10horas}{1000} = 0,9GB/día$$

#Cámara	Resolución	Velocidad binaria aproximada (Kbps)	Imágenes por segundo	MB/hora	Horas de funcionamiento	GB/día
1	CIF	200	15	90	10	0,9

Tabla N° 6. 31 Almacenamiento por día
Elaborado por: El Investigador

La tabla N° 6.31, plantea que se requiere 0.9 GB/día por cada cámara, el número de cámaras IP que se requiere para el edificio Municipal es de 30, en consecuencia el total de espacio requerido para el sistema será de 27 GB/día, si se almacena durante un período de un mes (30días), el espacio que se requiere será de 810 GB.

Se establece un espacio de disco adicional de 190 GB en caso de requerirse mayor resolución en ciertas zonas, por lo tanto el disco duro deberá tener una capacidad mayor o igual a 1 TB.

3. Características de la estación remota

La tabla N° 6.32, presenta las características mínimas requeridas por los computadores que actuarán como estación remota del sistema.

Sistemas operativos	Estación Remota		
	Procesador	Memoria	Capacidad de disco
Windows 7 (32/64-bit)	Intel Pentium 4 o superior	512MB RAM o superior	60GB o superior
Windows Vista (32/64-bit)			
Windows XP (32/64-bit)			

Tabla N° 6. 32 Características de la estación remota
Elaborado por: El Investigador

6.9.1.9 Determinación aproximada del ancho de banda requerido

a Estimación del Ancho de Banda por cámara

Los valores de la tabla N° 6.3 permiten obtener una determinación aproximada del ancho de banda requerido por el sistema, los mismos que se detallan a continuación en la tabla N° 6.33.

Cuadros por segundo (fps)	15
Resolución	CIF
Nivel de actividad	Medio
Tasa de bits estimada/cámara	200 Kbps

Tabla N° 6. 33 Estimación del Ancho de Banda por cámara
Elaborado por: El Investigador

Se estima una tasa de bits de 200 Kbps por cada cámara.

b Estimación del Ancho de Banda del sistema completo

La red en su totalidad consta de un total de 30 cámaras IP a una tasa de bits de 200 Kbps y configuradas con los parámetros antes mencionados, lo cual nos permite obtener la tasa de bits estimada del sistema, la misma que corresponde a 6Mbps.

6.9.1.10 Diagrama de la red LAN con cámaras IP

En la figura N° 6.31 se puede apreciar el diagrama de la red que se propone para el Sistema de Video-Vigilancia. La red de datos que se utilizará para las cámaras IP son:

Para el cableado vertical se utilizará el mismo cableado existente, para el cableado horizontal se utilizará el cable UTP categoría 6 ya que es un estándar para Gigabit Ethernet y otros protocolos de redes compatible con versiones anteriores con los estándares de categoría 5/5e. Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1Gbps.

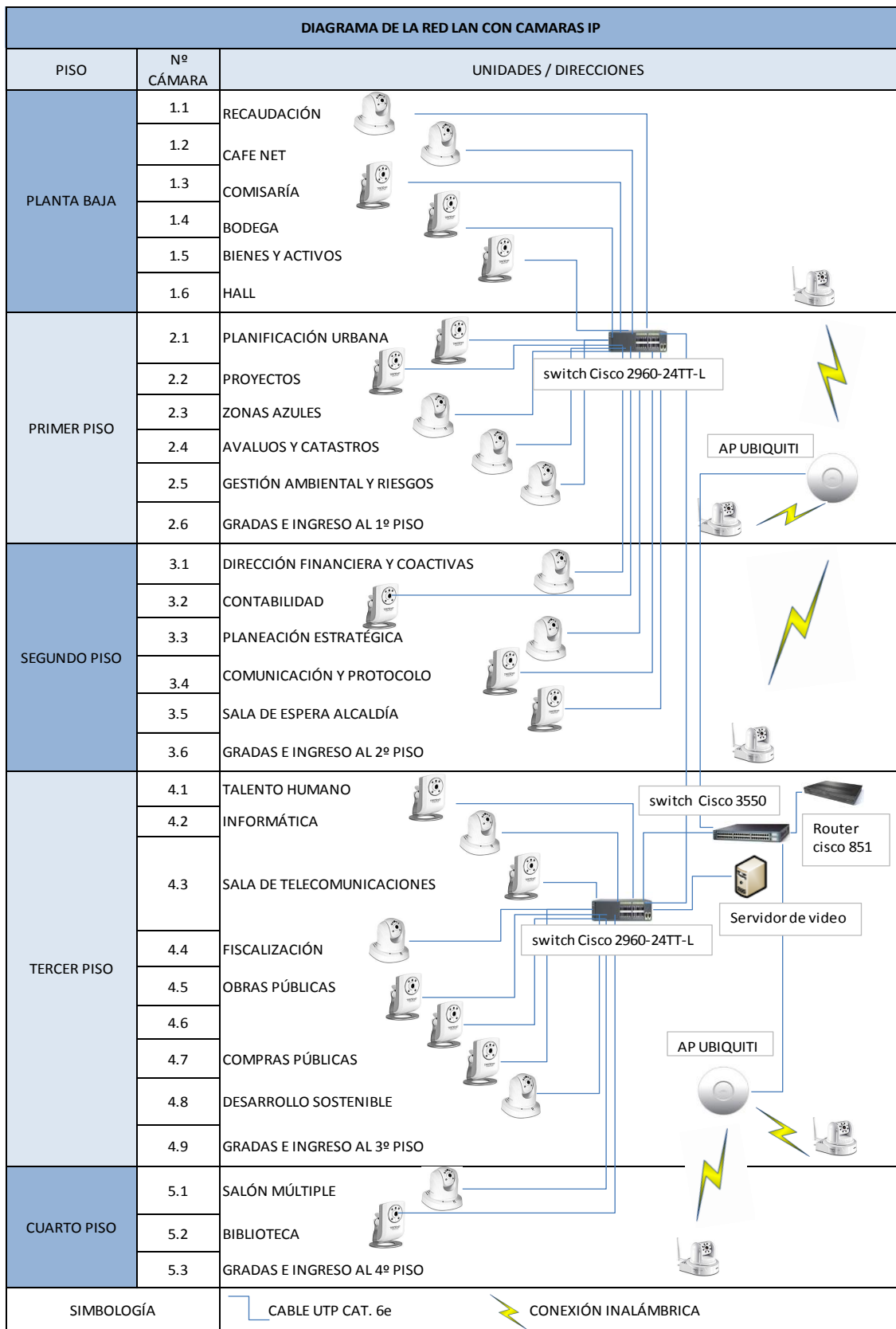


Figura Nº 6. 31 Diagrama de la red LAN con cámaras IP

Elaborado por: El Investigador

6.9.2 DISEÑO DE LA RED VIRTUAL DE ÁREA LOCAL (VLAN) PARA EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE TULCÁN

6.9.2.1 Análisis previo al diseño de VLAN

Con la creación de las VLAN se puede limitar el tráfico de difusión al interior de una red, creando dominios más pequeños en el interior de la misma y formando grupos para manejar las redes virtuales según su función. Para la red del Gobierno Autónomo Descentralizado Municipal de Tulcán se establecen 4 VLAN:

- VLAN1: Red de uso General (VLAN por default)
- VLAN2: Vigilancia IP (Red de video)
- VLAN3: Administrador1 (Red de gestión 1 – switch 1)
- VLAN4: Administrador2 (Red de gestión 2 – switch 2)

En la figura N° 6.32 se observan las 4 VLAN's definidas:

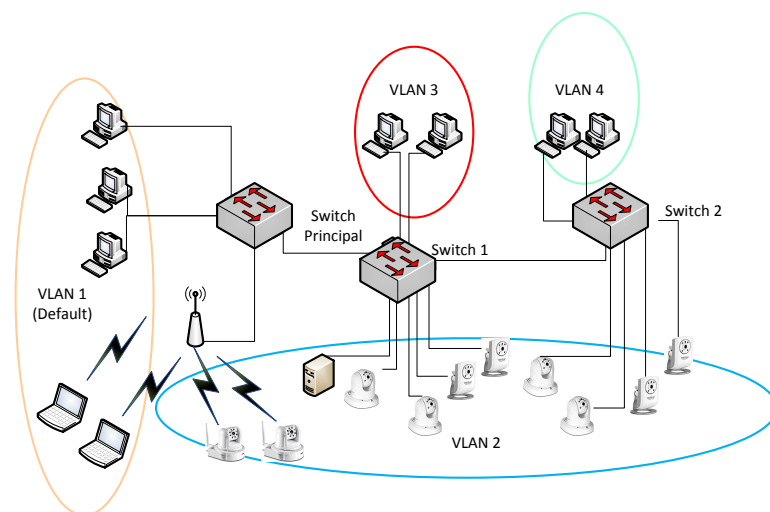


Figura N° 6. 32 Creación de VLAN's para el GADMT
Elaborado por: El Investigador

6.9.2.2 Distribución de VLAN

Las VLAN han sido diseñadas para unir dependencias que manejen la misma información. A continuación se muestra como están distribuidas las VLAN:

La VLAN1 es la VLAN por defecto a la cual todos los puertos del switch se asignan cuando el dispositivo inicia, esta designada para la red de uso General: computadoras, servidores e impresoras con punto de red de las Unidades y Direcciones del GADMT. La cual tiene asignada por el administrador de red la dirección 192.168.100.0/24.

Las VLAN2, VLAN3 y VLAN4 son las LAN virtuales destinadas a la conformación y administración de la red de video que van a ser configuradas en los switch, para lo cual se destina la dirección de red 192.168.101.0/24, la misma que debe ser dividida en subredes para la creación de las distintas redes virtuales. Para este proceso se realiza VLSM (Variable Length Subnet Mask o máscara de subred de longitud variable), en el que se toma una dirección de red o subred y la divide en subredes más pequeñas adaptando las máscaras según las necesidades de hosts de cada subred, generando una máscara diferente para las distintas subredes de una red. Esto permite no desaprovechar un gran número de direcciones, a diferencia del subneteo (subnetting) que genera una máscara común (fija) y cantidad de hosts iguales a todas las subredes. Con estos antecedentes procedemos a la conformación de las VLAN's:

a. La VLAN2 esta dedicada para la red de video-vigilancia IP: cámaras IP alámbricas e inalámbricas y servidor de video. Esta LAN virtual es la mas extensa, como se observa en la tabla N° 6.34 se especifican 34 direcciones para la creación de la subred.

LAN VIRTUAL DE VIDEO-VIGILANCIA IP	PUNTOS DE RED
CÁMARAS	30
SERVIDOR DE VIDEO	1
PC MONITOREO LOCAL DE LA RED IP DE VIDEO-VIGILANCIA	2
PUERTA DE ENLACE	1
TOTAL	34

Tabla N° 6. 34 Hosts requeridos para la creación de la subred de la VLAN2
Elaborado por: El Investigador

Requerimiento de hosts:

Se aplica la siguiente fórmula para calcular la cantidad de hosts:

$$\text{Hosts utilizables} = 2^n - 2$$

Se utiliza 6 como valor para n ya que es la primera potencia de 2 superior a 34. Al pedir prestado 6 bits para la porción de host se produce este cálculo:

$$2^6 = 64$$

$$64 - 2 = 62 \text{ direcciones de host utilizables}$$

Este cálculo cumple con el requisito actual para 34 direcciones, dando lugar a la disponibilidad de 28 direcciones libres que podrán ser dispuestas para la ampliación de la red IP.

Se destina el bloque de direcciones 192.168.101.0/26.

Dirección de subred de video-vigilancia IP: 192.168.101.0 con máscara 255.255.255.192, la dirección de host incluye un rango de 192.168.101.1 a 192.168.101.62 y la dirección de broadcast de 192.168.101.63. Ya que estas direcciones han sido asignadas para la LAN virtual 2, no se encuentran disponibles para la asignación de las subredes restantes.

b. La VLAN3 está reservada para la administración, acceso remoto y configuración del switch 1. En la tabla N° 6.35 se definen 4 direcciones de red necesarias para la subred de administrador1.

LAN VIRTUAL DE ADMINISTRADOR 1	PUNTOS DE RED
PC ADMINISTRACIÓN SWITCH 1	2
SWITCH 1	1
PUERTA DE ENLACE	1
TOTAL	4

Tabla N° 6. 35 Hosts requeridos para la creación de la subred de la VLAN3
Elaborado por: El Investigador

c. La **VLAN4** está reservada para la administración, acceso remoto y configuración del switch 2. Se detallan 4 direcciones de requerimiento de hosts para la subred de administrador2 en la tabla N° 6.36.

LAN VIRTUAL DE ADMINISTRADOR 2	PUNTOS DE RED
PC ADMINISTRACIÓN SWITCH 2	2
SWITCH 2	1
PUERTA DE ENLACE	1
TOTAL	4

Tabla N° 6. 36 Hosts requeridos para la creación de la subred de la VLAN4
Elaborado por: El Investigador

La VLAN3 y VLAN4 tiene un requerimiento de 4 hosts. Se emplea la fórmula:

$$\text{Hosts utilizables} = 2^n - 2$$

Para los dos casos se piden prestados 3 bits a la porción de host y el cálculo es:

$$2^3 - 2 = 6 \text{ hosts utilizables}$$

Cumpléndose así con el requisito de dejar poco margen para el crecimiento.

En la VLAN3 se dispone del bloque de direcciones 192.168.101.64/29.

Dirección de subred de administrador1: 192.168.101.64 con máscara 255.255.255.248, la dirección de host incluye un rango de 192.168.101.65 a 192.168.101.70 y la dirección de broadcast de 192.168.101.71.

A continuación en la VLAN4 se adopta el bloque de direcciones 192.168.101.72/29.

Dirección de subred de administrador1: 192.168.101.72 con máscara 255.255.255.248, la dirección de host incluye un rango de 192.168.101.73 a 192.168.101.78 y la dirección de broadcast de 192.168.101.79.

Esto completa la asignación de direcciones utilizando VLSM, si es necesario realizar un ajuste para adoptar el crecimiento futuro, aún se encuentran

disponibles las direcciones en el rango de 192.168.101.80 a 192.168.101.255. En la tabla N° 6.37, se muestran los rangos de direcciones IP asignados y las que quedan sin asignar.

RED	DIRECCIÓN DE SUBRED	RANGO DE DIRECCIÓN DE HOST		DIRECCIÓN DE BROADCAST
VLAN2: Vigilancia IP	192.168.101.0/26	192.168.101.1	192.168.101.62	192.168.101.63
VLAN3: Administrador1	192.168.101.64/29	192.168.101.65	192.168.101.70	192.168.101.71
VLAN4: Administrador2	192.168.101.72/29	192.168.101.73	192.168.101.78	192.168.101.79
Sin utilizar	No asignado	192.168.101.81	192.168.101.254	No asignado

Tabla N° 6.37 Subredes destinadas para las VLAN''s
Elaborado por: El Investigador

6.9.2.3 Configuración de VLAN

a. Direccionamiento IP

En la tabla N° 6.38, se muestran los equipos de red que forman parte de las VLAN 2, 3 y 4, con sus respectivos identificativos y direccionamiento IP. Los cuales constituyen parámetros necesarios para la conformación de las redes virtuales.

DISTRIBUCIÓN DE PUNTOS DE RED		ID	VLAN	DIRECCIÓN IP
PUERTA DE ENLACE			2	192.168.101.1/26
CÁMARAS ALÁMBRICAS	RECAUDACIÓN	1.1	2	192.168.101.2/26
	CAFE NET	1.2	2	192.168.101.3/26
	COMISARÍA	1.3	2	192.168.101.4/26
	BODEGA	1.4	2	192.168.101.5/26
	BIENES Y ACTIVOS	1.5	2	192.168.101.6/26
	PLANIFICACIÓN URBANA	2.1	2	192.168.101.7/26
	PROYECTOS	2.2	2	192.168.101.8/26
	ZONAS AZULES	2.3	2	192.168.101.9/26
	AVALUOS Y CATASTROS	2.4	2	192.168.101.10/26
	GESTIÓN AMBIENTAL Y RIESGOS	2.5	2	192.168.101.11/26
	DIRECCIÓN FINANCIERA Y COACTIVAS	3.1	2	192.168.101.12/26
	CONTABILIDAD	3.2	2	192.168.101.13/26
	PLANEACIÓN ESTRATÉGICA	3.3	2	192.168.101.14/26
	COMUNICACIÓN Y PROTOCOLO	3.4	2	192.168.101.15/26
	SALA DE ESPERA ALCALDÍA	3.5	2	192.168.101.16/26
	TALENTO HUMANO	4.1	2	192.168.101.17/26
	INFORMÁTICA	4.2	2	192.168.101.18/26
	SALA DE TELECOMUNICACIONES	4.3	2	192.168.101.19/26
	FISCALIZACIÓN	4.4	2	192.168.101.20/26
	OBRAS PÚBLICAS	4.5	2	192.168.101.21/26
	SINDICATURA	4.6	2	192.168.101.22/26
	COMPRAS PÚBLICAS	4.7	2	192.168.101.23/26
	DESARROLLO SOSTENIBLE	4.8	2	192.168.101.24/26
SALÓN MÚLTIPLE	5.1	2	192.168.101.25/26	
BIBLIOTECA	5.2	2	192.168.101.26/26	
CAMARAS INALÁMBRICAS	HALL	1.6	2	192.168.101.27/26
	GRADAS E INGRESO AL 1º PISO	2.6	2	192.168.101.28/26
	GRADAS E INGRESO AL 2º PISO	3.6	2	192.168.101.29/26
	GRADAS E INGRESO AL 3º PISO	4.9	2	192.168.101.30/26
	GRADAS E INGRESO AL 4º PISO	5.3	2	192.168.101.31/26
PC MONITOREO DE LA RED IP DE VIDEO-VIGILANCIA	PC1		2	192.168.101.60/26
	PC2		2	192.168.101.61/26
SERVIDOR DE VIDEO			2	192.168.101.62/26
PUERTA DE ENLACE			3	192.168.101.65/29
PC ADMINISTRACIÓN SWITCH VIGILANCIA1	PC3		3	192.168.101.66/29
	PC4		3	192.168.101.67/29
SWITCH 1			3	192.168.101.70/29
PUERTA DE ENLACE			4	192.168.101.73/29
PC ADMINISTRACIÓN SWITCH VIGILANCIA2	PC5		4	192.168.101.74/29
	PC6		4	192.168.101.75/29
SWITCH 2			4	192.168.101.78/29

Tabla N° 6. 38 Direccionamiento IP para la red de vigilancia del GADMT

Elaborado por: El Investigador

En la figura N° 6.33, se indica el Direcccionamiento IP para la red de vigilancia del GADMT.

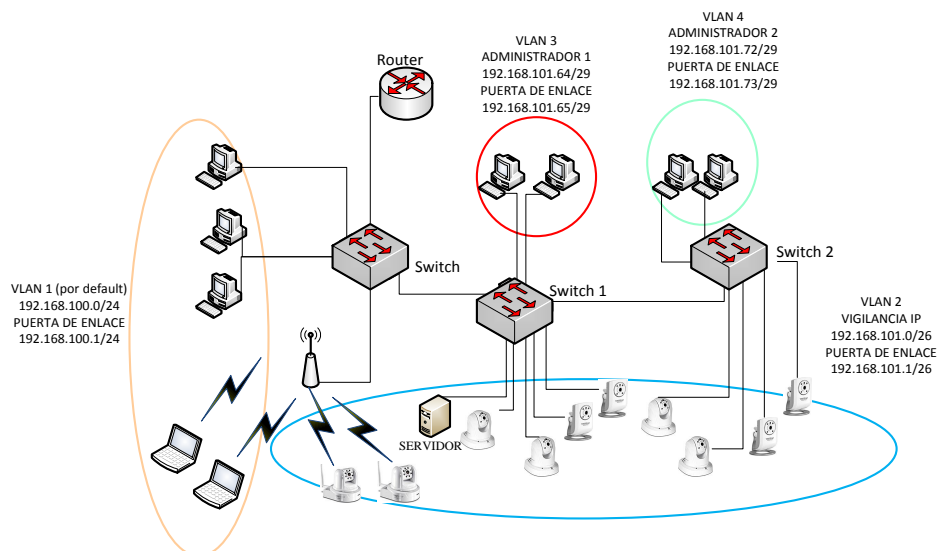


Figura N° 6. 33 Direcccionamiento IP para la red de vigilancia del GADMT
Elaborado por: El Investigador

6.9.2.4 Disposición de equipos

Como se detalla en capítulos anteriores, en el cuarto de equipos del GADMT se dispone de un router cisco de la serie 800, el mismo que permitirá interconectar las vlan's entre sí y a la vez permitirá su salida a internet. Además se cuenta con el switch CISCO CATALYST 3550 el cual funcionará como interfaz de comunicación entre las cámaras alámbricas e inalámbricas de la VLAN2 y a su vez conformará el enlace troncal.

Para el desarrollo del proyecto se requiere la compra de 2 switches, los mismos gestionaran la red de video IP, permitiendo las conexiones físicas y lógicas de los equipos para la vigilancia. La marca y modelo elegido es Cisco Catalyst 2960-24TT-L de 24 puertos.

- **Cisco Catalyst 2960-24TT-L**

Los Switches de Cisco Catalyst 2960 soportan voz, datos, vídeo y acceso seguro, ofreciendo una gestión escalable.



Figura N° 6. 34 Cisco Catalyst 2960-24TT-L

Fuente: http://www.almacen-informatico.com/CISCO_Catalyst-2960-24TT-WS-C2960-24TT-L_32140_p.htm

En la figura N° 6.34, se puede apreciar el switch Cisco Catalyst 2960-24TT-L, sus especificaciones técnicas más relevantes mostradas en la tabla N° 6.39 son las siguientes:

Tipo de dispositivo	Conmutador - 24 puertos - Gestionado
Tipo incluido	Montaje en rack - 1U
Puertos	24 x 10/100 + 2 x 10/100/1000
Rendimiento	Capacidad de conmutación : 32 Gbps Rendimiento de reenvío (tamaño de paquete de 64 bytes) : 6.5 Mpps
Tamaño de tabla de dirección MAC	8K de entradas
Protocolo de gestión remota	SNMP 1, SNMP 2, RMON 1, RMON 2, RMON 3, RMON 9, Telnet, SNMP 3, SNMP 2c, HTTP, HTTPS, TFTP, SSH
Algoritmo de cifrado	SSL
Método de autenticación	Secure Shell (SSH), RADIUS, TACACS+
Características	Conmutación Layer 2, auto-sensor por dispositivo, asignación dirección dinámica IP, negociación automática, soporte BOOTP, soporte ARP, equilibrio de carga, soporte VLAN, señal ascendente automática (MDI/MDI-X automático), snooping IGMP, soporte para Syslog, soporte DiffServ, Broadcast Storm Control, soporte IPv6, Multicast Storm Control, Unicast Storm Control, admite Rapid Spanning Tree Protocol (RSTP), admite Multiple Spanning Tree Protocol (MSTP), snooping DHCP, soporte de Dynamic Trunking Protocol (DTP), soporte de Port Aggregation Protocol (PAgP), soporte de Access Control List (ACL), Quality of Service (QoS), Protocolo de control de adición de enlaces (LACP), Port Security, MAC Address Notification, Remote Switch Port Analyzer (RSPAN)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x, IEEE 802.1s, IEEE 802.3ah, IEEE 802.1ab (LLDP)
Memoria RAM	64 MB
Memoria Flash	32 MB Flash
Indicadores de estado	Actividad de enlace, velocidad de transmisión del puerto, modo puerto duplex, alimentación, tinta OK, sistema
Dispositivo de alimentación	Fuente de alimentación - interna
Voltaje necesario	CA 120/230 V (50/60 Hz)
Consumo eléctrico en funcionamiento	28 vatios

Tabla N° 6. 39 Especificaciones Técnicas del switch Cisco Catalyst 2960-24TT-L

Fuente: http://www.almacen-informatico.com/CISCO_Catalyst-2960-24TT-WS-C2960-24TT-L_32140_p.htm

6.9.2.5 Simulación de las redes virtuales

Para simular las VLAN's se utilizó Packet Tracer, el cual es un simulador de entorno de redes de comunicaciones de fidelidad media, desarrollado por Cisco, permite crear topologías de red mediante la selección de los dispositivos y su respectiva ubicación en un área de trabajo, utilizando una interfaz gráfica. Permite realizar la configuración de dispositivos de red, así como la detección y corrección de errores en sistemas de comunicaciones. Ofrece como ventaja adicional el análisis de cada proceso que se ejecuta en el programa de acuerdo a la capa del modelo OSI que interviene en dicho proceso; razón por la cuál es una herramienta de gran ayuda en el aprendizaje del funcionamiento y configuración de redes de comunicaciones y aplicaciones.

En la figura N° 6.35 se exhibe el entorno para la simulación de las redes virtuales. Se observa las cuatro VLAN's precisadas, las cámaras IP alámbricas e inalámbricas requeridas en la VLAN2 se representan por medio de computadores personales y computadores portátiles, ya que el software no cuenta con cámaras de red en el menú de dispositivos finales, tomándose así la definición de una cámara IP, misma que puede describirse como una cámara y un ordenador combinados para formar una única unidad.

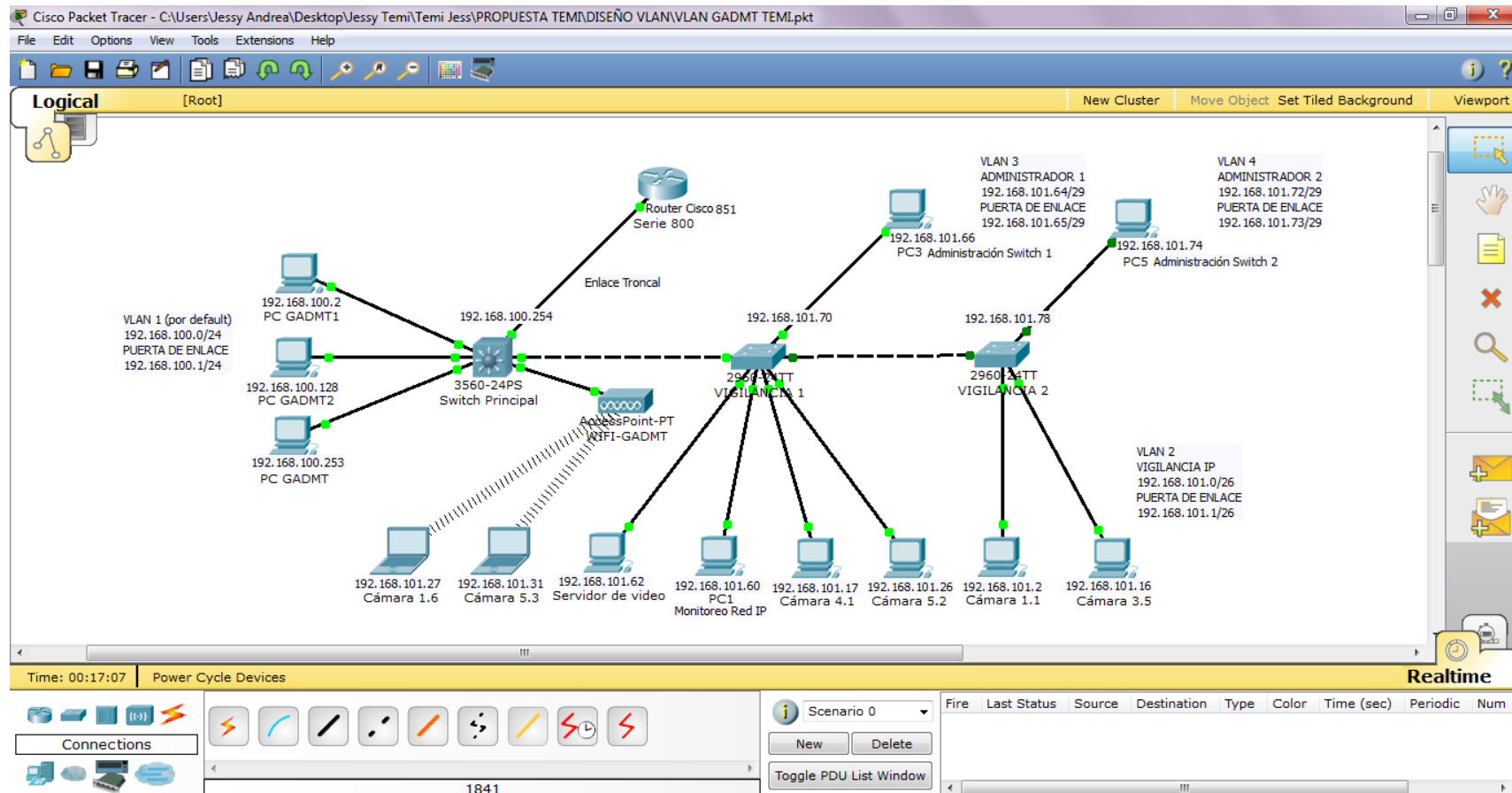


Figura N° 6. 35 Simulación de las VLAN's en Packet Tracer
Elaborado por: El Investigador

En las tablas N° 6.40 y N° 6.41, se detallan la asignación de puertos para las distintas VLAN y los puertos troncales en los switch Cisco Catalyst 2960-24TT-L de 24 puertos. En el Switch denominado VIGILANCIA1 se establecen puertos para el enlace troncal entre switches, cámaras alámbricas del tercer y cuarto piso del edificio municipal, PC's de monitoreo, servidor de video y PC 's de administrador del switch perteneciente a la VLAN 3. Para el Switch denominado VIGILANCIA2 se designan puertos al enlace troncal, cámaras alámbricas para la planta baja, primero y segundo piso, PC 's de administrador del switch perteneciente a la VLAN 4.

DETALLE	PUERTOS
ENLACE TRONCAL	1 al 2
CÁMARAS/VLAN2	3 al 12
MONITOREO/VLAN2	16 al 17
SERVIDOR DE VIDEO/VLAN2	18
VLAN 3	19 al 24

Tabla N° 6. 40 Asignación de puertos Switch VIGILANCIA1
Elaborado por: El Investigador

DETALLE	PUERTOS
ENLACE TRONCAL	1
CÁMARAS/VLAN2	2 al 16
VLAN 4	19 al 24

Tabla N° 6. 41 Asignación de puertos Switch VIGILANCIA2
Elaborado por: El Investigador

Una vez establecidos los parámetros del diseño se procede a las siguientes configuraciones.

- SWITCH VIGILANCIA1

Switch>**enable** (Ingresa al modo de configuración privilegiado)

Switch#**configure terminal** (Ingresa al modo de configuración global)

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#**hostname** Vigilancia1 (Asignación de nombre al switch1)

Vigilancia1(config)#vlan 2 (Añade la VLAN 2)

Vigilancia1(config-vlan)#name vigilanciaip (Asigna un nombre a la VLAN)

Vigilancia1(config-vlan)#exit (Sale del modo de configuración de la VLAN)

Vigilancia1(config)#vlan 3

Vigilancia1(config-vlan)#name administrador1

Vigilancia1(config-vlan)#exit

Vigilancia1(config)#exit (sale del modo de configuración global)

Vigilancia1#

%SYS-5-CONFIG_I: Configured from console by console

Vigilancia1#show vlan (Muestra las VLAN creadas. Figura N° 6.36)

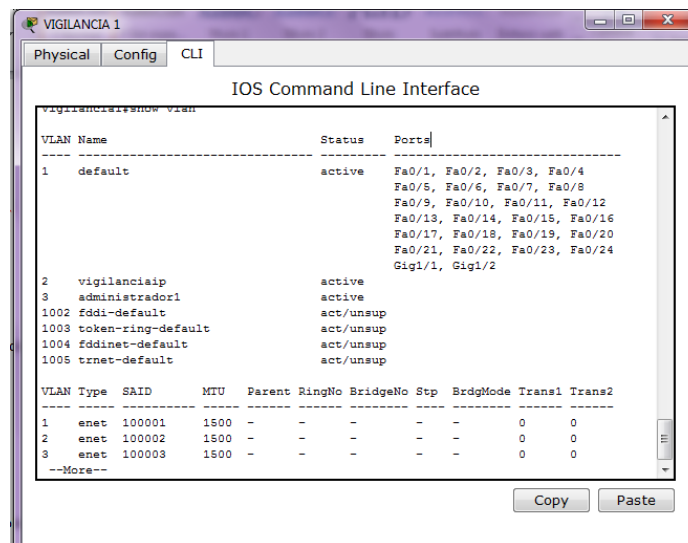


Figura N° 6. 36 VLAN creadas en el switch - Packet Tracer
Elaborado por: El Investigador

Vigilancia1(config)#interface fastEthernet 0/3 (Ingresa en la configuración del puerto fast Ethernet 0/3)

Vigilancia1(config-if)#switchport mode access (Define VLANS en modo estático)

Vigilancia1(config-if)#**switchport access vlan 2** (Asigna la VLAN al puerto)

Vigilancia1(config-if)#**exit** (Sale del modo de configuración de la interfaz)

Vigilancia1(config)#**interface range fa0/3 – 18** (Ingresa en la configuración de un rango de puertos fast Ethernet 0/3)

Vigilancia1(config-if-range)#**switchport mode access**

Vigilancia1(config-if-range)#**switchport access vlan 2**

Vigilancia1(config-if-range)#**exit**

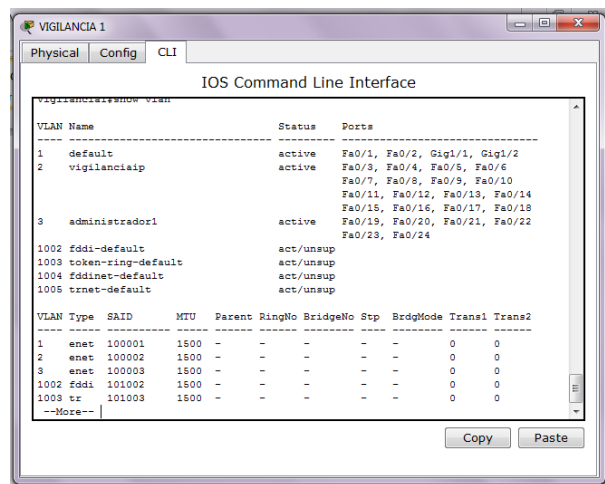
Vigilancia1(config)#**interface range fa0/19 – 24**

Vigilancia1(config-if-range)#**switchport mode access**

Vigilancia1(config-if-range)#**switchport access vlan 3**

Vigilancia1(config-if-range)#**exit**

La figura N° 6.37, muestra las VLAN creadas así como la asignación de puertos para cada una de ellas.



The screenshot shows the 'IOS Command Line Interface' window in Packet Tracer. It displays the configuration for three VLANs: 'default', 'vigilanciaip', and 'administrador1'. The 'default' VLAN is active and assigned to ports Fa0/1, Fa0/2, Gig1/1, and Gig1/2. The 'vigilanciaip' VLAN is active and assigned to ports Fa0/3 through Fa0/18. The 'administrador1' VLAN is active and assigned to ports Fa0/19 through Fa0/24. Below this, a table shows the details for each VLAN, including its type, SAID, MTU, and parent bridge.

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Gig1/1, Gig1/2
2 vigilanciaip	active	Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18
3 administrador1	active	Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Trans1	Trans2
1	enet	100001	1500	-	-	-	-	-	0	0
2	enet	100002	1500	-	-	-	-	-	0	0
3	enet	100003	1500	-	-	-	-	-	0	0
1002	fdci	101002	1500	-	-	-	-	-	0	0
1003	tr	101003	1500	-	-	-	-	-	0	0

Figura N° 6. 37 Asignación de puertos de las VLAN en el switch- Packet Tracer

Elaborado por: El Investigador

Vigilancia1(config)#**interface vlan 3** (Ingresamos a la interfaz virtual para crear la VLAN de administración)

%LINK-5-CHANGED: Interface Vlan3, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan3, changed state to up

Vigilancia1(config-if)#**ip address** 192.168.101.70 255.255.255.248
(Asignamos una dirección IP)

Vigilancia1(config-if)#**no shutdown** (Habilita el puerto)

Vigilancia1(config-if)#exit

Vigilancia1(config)#**vlan** 90 (Añadimos la VLAN nativa 90)

Vigilancia1(config-vlan)#**name native**

Vigilancia1(config-vlan)#exit

Vigilancia1(config)#**int** fa0/2

Vigilancia1(config-if)#**switchport mode trunk** (Setea al puerto de modo trunk, para permitir pasar más de una VLAN)

Vigilancia1(config-if)#**switchport trunk native vlan** 90 (Configurar la VLAN que va a enviar y recibir tráfico no etiquetado sobre el puerto troncal)

Vigilancia1(config-if)#exit

Vigilancia1(config)#exit

Vigilancia1#**show interface fa0/2 switchport** (Muestra información del puerto fa0/2. Figura N° 6.38)

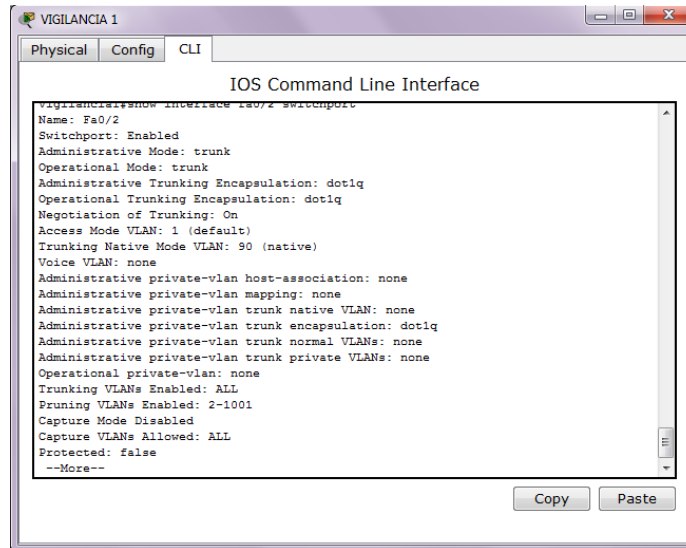


Figura N° 6. 38 Información del puerto fa0/2 del switch -Packet Tracer
Elaborado por: El Investigador

Vigilancia1(config)#vlan 91

Vigilancia1(config-vlan)#name native

Vigilancia1(config-vlan)#exit

Vigilancia1(config)#int fa0/1

Vigilancia1(config-if)#switchport mode trunk

Vigilancia1(config-if)#switchport trunk native vlan 91

Vigilancia1(config-if)#exit

Vigilancia1#**show interfaces trunk** (Muestra información del enlace troncal:
 VLAN's nativas y puertos permitidos para el enlace troncal. Figura N° 6.39)

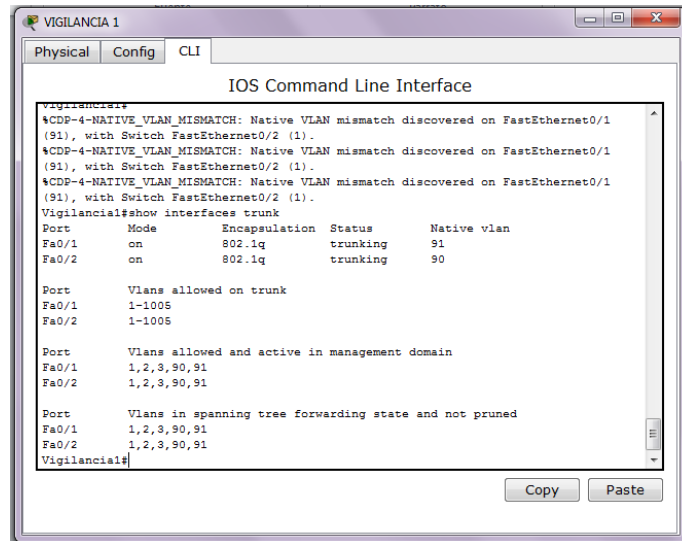


Figura N° 6. 39 Información del enlace troncal en el switch- Packet Tracer
Elaborado por: El Investigador

Vigilancia1#copy **running-config startup-config** (Guardar los cambios efectuados)

Destination filename [startup-config]?

Building configuration...

[OK]

- SWITCH VIGILANCIA2

Switch>enable

Switch#configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#hostname Vigilancia2

Vigilancia2(config)#vlan 2

Vigilancia2(config-vlan)#name vigilanciaip

Vigilancia2(config-vlan)#exit

Vigilancia2(config)#vlan 4

```
Vigilancia2(config-vlan)#name administardor2
Vigilancia2(config-vlan)#exit
Vigilancia2(config)#int range fa0/2 - 18
Vigilancia2(config-if-range)#switchport mode access
Vigilancia2(config-if-range)#switchport access vlan 2
Vigilancia2(config-if-range)#exit
Vigilancia2(config)#int range fa0/19 - 24
Vigilancia2(config-if-range)#switchport mode access
Vigilancia2(config-if-range)#switchport access vlan 4
Vigilancia2(config-if-range)#exit
Vigilancia2(config)#interface vlan 4
%LINK-5-CHANGED: Interface Vlan4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state
to up
Vigilancia2(config-if)#ip address 192.168.101.75 255.255.255.248
Vigilancia2(config-if)#no shut
Vigilancia2(config-if)#exit
Vigilancia2(config)#vlan 90
Vigilancia2(config-vlan)#name native
Vigilancia2(config-vlan)#exit
Vigilancia2(config)#int fa0/1
Vigilancia2(config-if)#switchport mode trunk
```


Vigilancia2(config-if)#switchport trunk native vlan 90

Vigilancia2(config-if)#exit

Vigilancia2(config)#exit

Vigilancia2#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

- SWITCH PRINCIPAL CISCO CATALYST 3550

Switch>enable

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#vlan 2

Switch(config-vlan)#name vigilanciaip

Switch(config-vlan)#exit

Switch(config)#vlan 3

Switch(config-vlan)#name administrador1

Switch(config-vlan)#exit

Switch(config)#vlan 4

Switch(config-vlan)#name administrador2

Switch(config-vlan)#exit

Switch(config)#int fa0/5

Switch(config-if)#switchport mode access

```
Switch(config-if)#switchport access vlan 2

Switch(config-if)#exit

Switch(config)#vlan 91

Switch(config-vlan)#name native

Switch(config-vlan)#exit

Switch(config)#int fa0/2

Switch(config-if)#switchport mode trunk

Switch(config-if)#switchport trunk native vlan 91

Switch(config-if)#exit

Switch#show interfaces trunk

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.100.254 255.255.255.0

Switch(config-if)#exit

Switch(config)#int fa0/1

Switch(config-if)#switchport mode trunk ( Enlace troncal con el router)

Switch(config-if)#switchport trunk native vlan 1

Switch(config-if)#exit

Switch(config)#exit

Switch#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]
```

- ROUTER SERIE 800

Router>enable

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#**int fa0/0.1** (serie de comandos para crear una subinterfaz para una vlan)

Router(config-subif)#**encapsulation dot1Q 1** (configurar la subinterfaz para que funcione en una VLAN específica)

Router(config-subif)#**ip address 192.168.100.1 255.255.255.0** (Asignar la dirección IP del puerto de enlace predeterminada para la subred de la VLAN)

Router(config-subif)#exit

Router(config)#int fa0/0.2

Router(config-subif)#encapsulation dot1Q 2

Router(config-subif)#ip address 192.168.101.1 255.255.255.192

Router(config-subif)#exit

Router(config)#int fa0/0.3

Router(config-subif)#encapsulation dot1Q 3

Router(config-subif)#ip address 192.168.101.65 255.255.255.248

Router(config-subif)#exit

Router(config)#int fa0/0.4

Router(config-subif)#encapsulation dot1Q 4

Router(config-subif)#ip address 192.168.101.73 255.255.255.248

Router(config-subif)#exit

Router(config)#int fa0/0

Router(config-if)#no shutdown (Habilitamos el puerto. La Figura N° 6.40 muestra que las subinterfaces de la interfaz fast ethernet0/0 están activadas)

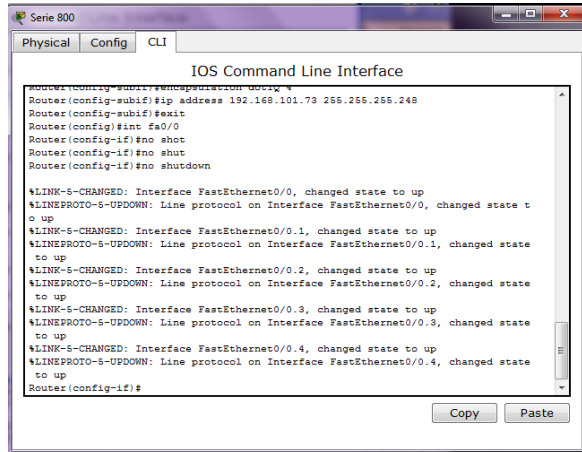


Figura N° 6. 40 Habilitación del puerto del Router - Packet Tracer
Elaborado por: El Investigador

Router#show ip route (Muestra las redes y subredes con su respectiva dirección IP configuradas como subinterfaces del router. Figura N° 6.41)

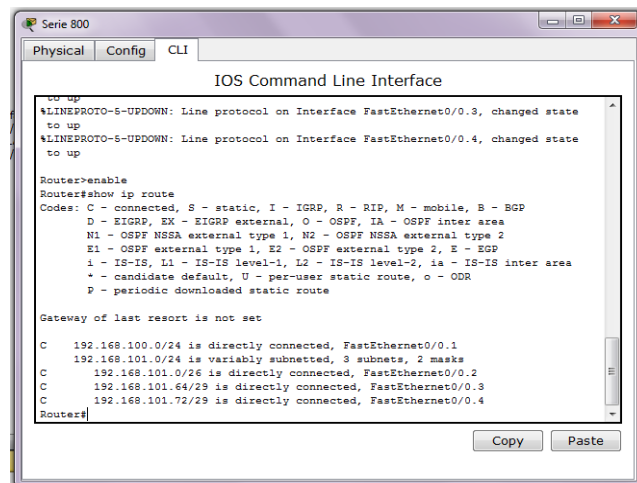


Figura N° 6. 41 Sub-interfaces del Router - Packet Tracer
Elaborado por: El Investigador

Router#copy running-config startup-config

Destination filename [startup-config]?

Building configuration...

[OK]

Una vez terminadas las configuraciones para crear e interconectar VLAN's se procede a enviar paquetes en tiempo real desde la VLAN1 a las demás, como se puede observar en la figura N° 6.42 la respuesta obtenida es exitosa.

Realtime							
Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic
	Successful	PC GADMT1	Cámara 1.6	ICMP		0.000	N
	Successful	PC GADMT1	PC3	ICMP		0.000	N
	Successful	PC GADMT1	PC5	ICMP		0.000	N

Figura N° 6. 42 Envío de paquetes en tiempo real - Packet Tracer
Elaborado por: El Investigador

6.9.3 ACCESO REMOTO

6.9.3.1 Visualización de las cámaras por internet

El Gobierno Autónomo Descentralizado Municipal de Tulcán posee una conexión a la WAN destinada para el internet institucional a través de la Corporación Nacional de Telecomunicaciones (CNT), de este modo para poder mirar las cámaras IP fuera de la red se debe configurar la traducción de direcciones (NAT) que permite el acceso a Internet mediante la IP pública de la conexión WAN.

En la figura N° 6.43 se puede apreciar la visualización de las cámaras del GADMT por internet, utilizando NAT.

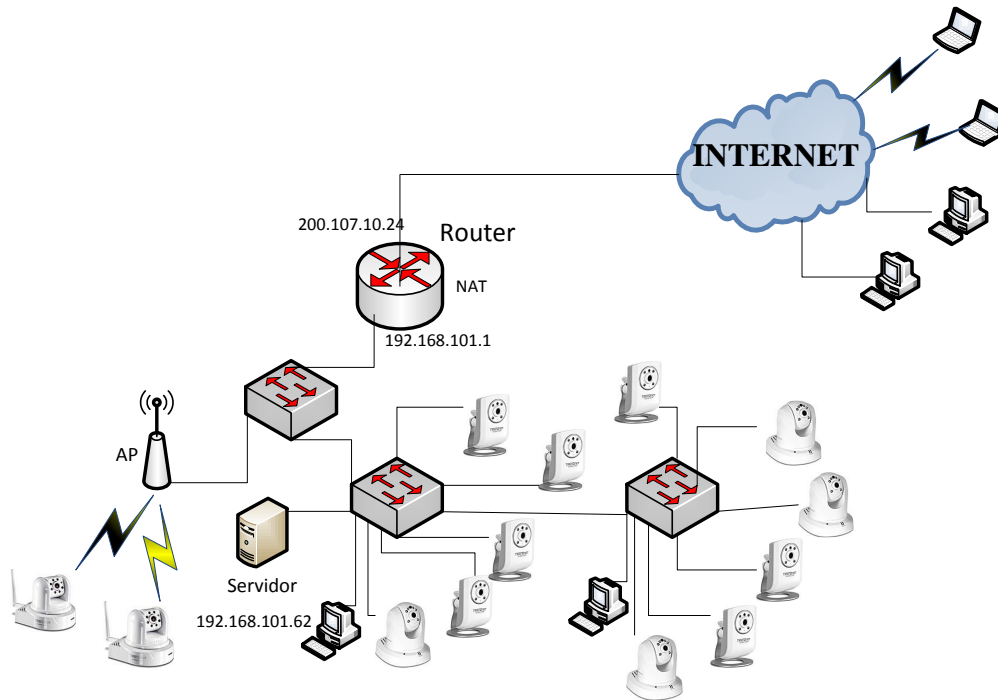


Figura N° 6. 43 Visualización de las cámaras del GADMT por internet
Elaborado por: El Investigador

6.9.3.2 Configuración del redireccionamiento de puertos mediante NAT para habilitar acceso remoto a la cámara IP

Es necesario realizar una configuración en el NAT del router que permita acceder remotamente a la cámara, puesto que las cámaras tendrán configurada una IP privada, que van desde la 192.168.101.2/26 a la 192.168.101.31/26. Para ello, se configura un puerto público en el router para el redireccionamiento a una dirección IP de la LAN interna y al puerto privado de la LAN, si se requiere. Un uso común de la virtualización es el acceso remoto a múltiples cámaras. Por cada cámara se debe crear un Servidor Virtual, con los datos especificados en la tabla N° 6.42.

Para habilitar el puerto HTTP se deben tomar en cuenta las siguientes observaciones:

- El puerto elegido no deberá ser alguno de los ya utilizados por servicios comunes de red, tal como el puerto 21 (FTP), 25 (POP), 80(Web), entre otros.
- Es recomendable que cada cámara cuente con un puerto diferente para no tener problemas de comunicación.

TIPO	DIRECCIÓN/UNIDAD	CÁMARA		PUERTO HTTP DEFINIDO
		#	DIRECCIÓN IP	
CÁMARA ALÁMBRICAS	RECAUDACIÓN	1.1	192.168.101.2/26	3001
	CAFE NET	1.2	192.168.101.3/26	3002
	COMISARÍA	1.3	192.168.101.4/26	3003
	BODEGA	1.4	192.168.101.5/26	3004
	BIENES Y ACTIVOS	1.5	192.168.101.6/26	3005
	PLANIFICACIÓN URBANA	2.1	192.168.101.7/26	3006
	PROYECTOS	2.2	192.168.101.8/26	3007
	ZONAS AZULES	2.3	192.168.101.9/26	3008
	AVALUOS Y CATASTROS	2.4	192.168.101.10/26	3009
	GESTIÓN AMBIENTAL Y RIESGOS	2.5	192.168.101.11/26	3010
	DIRECCIÓN FINANCIERA Y COACTIVAS	3.1	192.168.101.12/26	3011
	CONTABILIDAD	3.2	192.168.101.13/26	3012
	PLANEACIÓN ESTRATÉGICA	3.3	192.168.101.14/26	3013
	COMUNICACIÓN Y PROTOCOLO	3.4	192.168.101.15/26	3014
	SALA DE ESPERA ALCALDÍA	3.5	192.168.101.16/26	3015
	TALENTO HUMANO	4.1	192.168.101.17/26	3016
	INFORMÁTICA	4.2	192.168.101.18/26	3017
	SALA DE TELECOMUNICACIONES	4.3	192.168.101.19/26	3018
	FISCALIZACIÓN	4.4	192.168.101.20/26	3019
	OBRAS PÚBLICAS	4.5	192.168.101.21/26	3020
	SINDICATURA	4.6	192.168.101.22/26	3021
	COMPRAS PÚBLICAS	4.7	192.168.101.23/26	3022
DESARROLLO SOSTENIBLE	4.8	192.168.101.24/26	3023	
SALÓN MÚLTIPLE	5.1	192.168.101.25/26	3024	
BIBLIOTECA	5.2	192.168.101.26/26	3025	
CAMARAS INALÁMBRICAS	HALL	1.6	192.168.101.27/26	3026
	GRADAS E INGRESO AL 1º PISO	2.6	192.168.101.28/26	3027
	GRADAS E INGRESO AL 2º PISO	3.6	192.168.101.29/26	3028
	GRADAS E INGRESO AL 3º PISO	4.9	192.168.101.30/26	3029
	GRADAS E INGRESO AL 4º PISO	5.3	192.168.101.31/26	3030

Tabla N° 6. 42 Asignación de los puertos de cámaras IP

Elaborado por: El Investigador

Para acceder a cámaras ubicadas en la LAN privada a través de Internet, la dirección IP pública del enrutador se debe usar junto con el número de puerto correspondiente de la cámara de red en la red privada.

Al configurar un enrutador para asociar un único número de puerto HTTP al puerto HTTP predeterminado y a la dirección IP de un producto de vídeo en red concreto. Este proceso se denomina reenvío de puertos y funciona como se indica a continuación. Los paquetes de datos entrantes llegan al enrutador a través de su dirección IP pública (externa) y un número de puerto específico. El enrutador está configurado para reenviar los datos que entran por un número de puerto predefinido a un dispositivo específico de la parte del enrutador correspondiente a la red privada. A continuación, el enrutador sustituye la dirección del emisor por su propia dirección IP privada (interna). Para el cliente receptor, el enrutador es el origen de los paquetes. Con los paquetes de datos salientes ocurre lo contrario. El enrutador sustituye la dirección IP privada del dispositivo origen por la IP pública del propio enrutador antes de enviar los datos a través de Internet.

Gracias al reenvío de puertos del enrutador, es posible acceder a cámaras de red de una red local con direcciones IP privadas a través de Internet. En la figura, el enrutador reenvía los datos (solicitud) que recibe el puerto 3001 a una cámara de red con la dirección IP privada 192.168.101.2 a través del puerto interno.

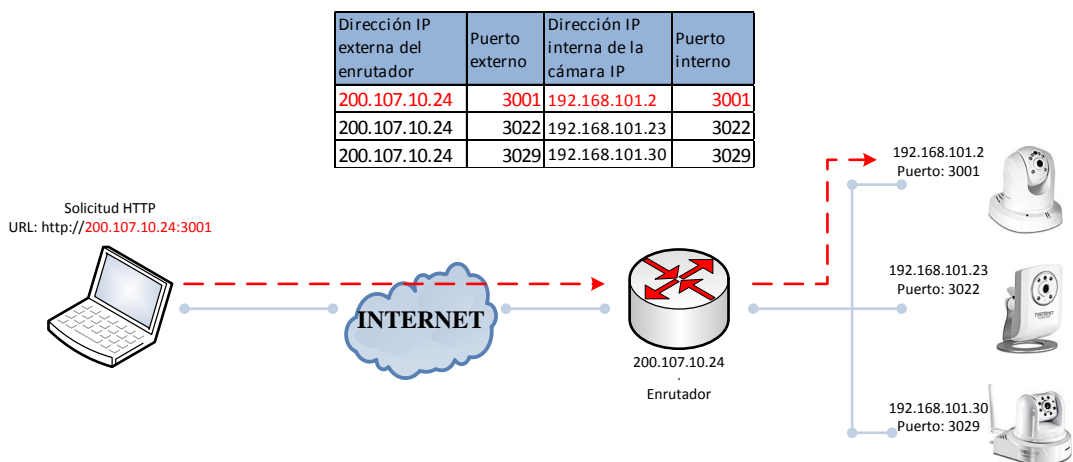


Figura N° 6. 44 Redireccionamiento de puertos
Elaborado por: El Investigador

Las cámaras IP tienen el puerto http:80 como parámetro de origen, cuando se lleva a cabo la modificación de ese puerto será necesario que para volver a entrar a la configuración Web desde la red local habrá que teclear la siguiente nomenclatura:

http:// + (IP Privada) + (:) + (Puerto http de la cámara)

Para ver la cámara desde internet, una vez configurado el reenvío de puertos en el router se deberá teclear en el navegador Web, siguiendo la siguiente nomenclatura:

http:// + (IP Pública) + (:) + (Puerto http de la cámara)

6.9.4 ANÁLISIS FINANCIERO

Para efectuar el análisis financiero del presente trabajo investigativo, se realiza el cálculo de la *inversión*, para ello se suman todos los valores correspondientes a:

- Valor de los equipos, detallado en la tabla N° 6.43.
- Costo de instalación que corresponde al valor de los equipos más el costo de ingeniería. La ingeniería es el 30% del valor de los equipos. En la tabla N°6.44 se especifican dichos valores.
- Y el valor de los 4 Mbps de ancho de banda adicionales que se requieren para dar operatividad al estudio. En la tabla N° 6.45 se establece el valor mensual a cancelarse por el servicio actual de internet, el requerimiento para un óptimo funcionamiento de la red IP es de 4 Mbps adicionales, el valor del incremento se registra en la tabla N° 6.46 y el valor total a pagar por el servicio de internet se determina en la tabla N° 6.47.

ÍTEM	DESCRIPCIÓN	UNIDAD	CANTIDAD	PRECIO	
				UNITARIO	TOTAL
1	Cámara TRENDnet TV-IP572PI	c/u	14	380,50	5327,00
2	Cámara TRENDnet TV-IP672PI	c/u	11	350,67	3857,37
3	Cámara TRENDnet TV-IP422WN	c/u	5	402,79	2013,95
4	Switch Cisco Catalyst 2960-24TT-L	c/u	2	700,00	1400,00
5	Computador Intel Core I7 3.4 Ghz+16gb+monitor Led 18.5	c/u	1	950,00	950,00
6	Rollo De 305 Metros De Cable Utp Categoria 6e	c/u	4	174,00	696,00
7	Conectores	c/u	90	0,20	18,00
SUBTOTAL					14262,32
12% IVA					1711,48
TOTAL					15973,80

Tabla N° 6. 43 Costo de los equipos del proyecto
Elaborado por: El Investigador

INSTALACIÓN	
EQUIPOS	15973,8
INGENIERIA (30% equipos)	4792,14
Total	20765,94

Tabla N° 6. 44 Costo de instalación
Elaborado por: El Investigador

ANCHO DE BANDA ACTUAL	
SERVICIO DE INTERNET	PAGO MENSUAL
8 Mbps	1832

Tabla N° 6. 45 AB actual
Elaborado por: El Investigador

ANCHO DE BANDA ADICIONAL	
SERVICIO DE INTERNET	PAGO MENSUAL
4 Mbps	916

Tabla N° 6. 46 AB adicional
Elaborado por: El Investigador

ANCHO DE BANDA REQUERIDO	
SERVICIO DE INTERNET	PAGO MENSUAL
8 Mbps	1832
4 Mbps	916
TOTAL(12Mbps)	2748

Tabla N° 6. 47 AB requerido en el proyecto
Elaborado por: El Investigador

En la tabla N° 6.48 se establece el valor de la inversión.

ÍTEM	VALOR
ESTUDIO	1000,00
4 Mbps ADICIONALES	11000,00
INSTALACIÓN	20765,94
TOTAL	32765,94

Tabla N° 6. 48 Inversión
Elaborado por: El Investigador

Una vez calculado los costos de la inversión inicial que corresponden al año 0, se estiman los ingresos y egresos del proyecto previsto a cinco años o periodos, que es el tiempo que dura la administración en los Gobiernos Autónomos Descentralizados.

Los egresos que se realizan durante los cinco años son los siguientes: el valor de \$11000 de 4 Mbps de ancho de banda adicionales que se cancelaran por cada año. Se prevé un costo de mantenimiento de equipos de \$1500 a partir del tercer año.. Un costo de depreciación de acuerdo al mercado, que corresponde a los 20% anuales, de todo el valor de equipos, es decir \$3194,76.

En la tabla N° 6.49 se muestran los egresos de manera detallada.

EGRESOS	1	2	3	4	5
4 Mbps adicionales	11000	11000	11000	11000	11000
Mantenimiento			1500	1500	1500
Depreciación	3194,76	3194,76	3194,76	3194,76	3194,76

Tabla N° 6. 49 Egresos
Elaborado por: El Investigador

Los ingresos especificados en la tabla N° 6.50, son los siguientes: en la actualidad el GADMT cuenta con doce guardias, que realizan 3 turnos, es decir en cada turno 4 guardias. La idea que se plantea es reducir tres guardias, lo que permitirá tener un ahorro para la municipalidad. El pago mensual por guardia es de \$400, por las doce personas al mes serian \$4800 y al año un valor de \$57600. Al dicho planteamiento, se cuenta con nueve guardias, al mes se pagará \$3600 y al año \$32400; al realizar la diferencia de pago anual entre los dos casos, tenemos un ahorro de \$25200.

INGRESOS	1	2	3	4	5
Ahorro (3 guardias)	25200	25200	25200	25200	25200

Tabla N° 6. 50 Ingresos
Elaborado por: El Investigador

Una vez calculados los valores de inversión inicial, egresos e ingresos, se procede a realizar el flujo neto de caja expuesto en la tabla N° 6.51. Primero se calcula el total de egresos e ingresos por año, luego se determina el flujo neto por año, restando el total de ingresos menos el total de egresos de cada año.

EGRESOS	0	1	2	3	4	5
Equipos	15973,8					
4 Mbps adicionales	11000	11000	11000	11000	11000	11000
Estudio e ingeniería	5792,14					
Mantenimiento				1500	1500	1500
Depreciación		3194,76	3194,76	3194,76	3194,76	3194,76
TOTAL EGRESOS	32765,94	14194,76	14194,76	15694,76	15694,76	15694,76
INGRESOS						
Ahorro (3 guardias)		25200	25200	25200	25200	25200
TOTAL INGRESOS	0	25200	25200	25200	25200	25200
FLUJO DE CAJA	-32765,94	11005,24	11005,24	9505,24	9505,24	9505,24

Tabla N° 6. 51 Flujo de caja
Elaborado por: El Investigador

Una vez presentado el flujo neto de caja y con sus respectivos valores, se realiza el cálculo de los indicadores financieros: Valor actual neto (VAN), Tasa interna de retorno (TIR) y Periodo de recuperación de la inversión (PRI).

Para el VAN, se utiliza la fórmula siguiente:

$$VAN = BNA - Inversión$$

BNA = beneficio neto actualizado de cada año

Para calcular el BNA se emplea la siguiente fórmula:

$$BNA = \frac{F}{(1+i)^n}$$

F = flujo de caja neto proyectado para cada año.

i = tasa de descuento o interés (17%).

n = número de años o periodos del proyecto.

Cálculo del VAN:

$$VAN = \frac{11005,24}{(1+0,17)^1} + \frac{11005,24}{(1+0,17)^2} + \frac{9505,24}{(1+0,17)^3} + \frac{9505,24}{(1+0,17)^4} + \frac{9505,24}{(1+0,17)^5} - 32765,94$$

$$VAN = 32788,37 - 32765,94$$

$$VAN = 22,43$$

El valor del VAN es mayor a 0, por lo tanto el proyecto es aceptado, para su ejecución.

Cálculo de la TIR:

$$TIR = 17,0308\%$$

La TIR es la tasa de interés (o la tasa de descuento) con la cual el valor actual neto o valor presente neto (VAN o VPN) es igual a cero. El VAN o VPN es calculado a partir del flujo de caja anual, trasladando todas las cantidades futuras al presente. Es el indicador de la rentabilidad del estudio proyecto, y en este caso a mayor TIR, mayor rentabilidad.

Cálculo del PRI:

El periodo de recuperación de la inversión esta entre el *tercero y cuarto año*, específicamente es *3, 33 periodos*. Se considera un buen grado de recuperación, tomando en cuenta que el proyecto tiene la duración de cinco años.

6.10 CONCLUSIONES

- En el presente proyecto se diseñó una red de Video-vigilancia mediante tecnología IP para el acceso remoto de las Unidades Operativas del Gobierno Autónomo Descentralizado Municipal de Tulcán, en el desarrollo del mismo se analizó la mejor opción en cuanto a la tecnología para ser utilizada. La propuesta planteada abre la posibilidad de montar un sistema de seguridad en todas las unidades del edificio municipal con el fin de supervisar continuamente las instalaciones del edificio municipal
- Por medio de los planos arquitectónicos del edificio del GADMT, se dispuso la ubicación de las cámaras con la finalidad de lograr la cobertura solicitada y cumplir con los requerimientos necesarios para la red de vigilancia, de manera que las áreas de interés sean cubiertas con el menor número de cámaras.
- Los sistemas de seguridad, basados en su totalidad en tecnología IP, ofrecen un gran nivel de escalabilidad a diferencia de los sistemas analógicos, dado que permite la convergencia con los diferentes servicios manejados actualmente, tal es el caso de voz sobre IP o redes de datos.
- Se planteó un sistema de video-vigilancia híbrido con cámaras IP alámbricas que incorporan tecnología Alimentación por Ethernet (PoE) e inalámbricas basadas en la tecnología IEEE 802.11n. Además las cámaras incorporan visión nocturna, ofreciendo accesibilidad y seguridad durante el día y la noche.

- El criterio de selección de los equipos y software de monitoreo se lo realizó en base a la interoperabilidad entre dispositivos, aplicaciones, calidad y costo. Las cámaras y el software de video son de la marca TRENDnet, y los equipos de comunicación son Cisco; de esta forma se preserva compatibilidad entre dispositivos y se facilita la administración y mantenimiento del sistema de vigilancia.
- La tecnología digital de las cámaras seleccionadas para el diseño facilita la grabación de imágenes sin el uso de equipos conversores de señal, disponiendo de su propio software que les permite actuar como un servidor web sin el uso de ningún dispositivo extra.
- En el diseño se optó por el software gratuito de video SecurView Pro debido al ahorro de costos que significa. Este software es compatible con todos los modelos de cámara IP de TRENDnet actuales, además ofrece baja carga de la CPU y puede gestionar hasta 32 cámaras.
- Para la grabación del video obtenido de las cámaras IP el parámetro más importante a dimensionar es la capacidad de almacenamiento de la PC que actuará como servidor, para ello se tomó en cuenta la cantidad de cámaras, el número de horas a grabarse por día, la resolución, cantidad de fotogramas por segundo y el formato de compresión. A través de los cálculos realizados se determina que el disco duro debe tener una capacidad mayor o igual a 1 TB.
- Las nuevas técnicas de compresión y digitalización del video hace que sea versátil al momento de la transmisión reduciendo el ancho de banda, incluyendo ventajas como nitidez de video, optimizando recursos y reduciendo espacio en el grabado.
- Se efectuó el diseño de una VLAN de video-vigilancia IP con el fin de que únicamente los usuarios de este grupo específico puedan intercambiar datos o acceder a determinados recursos. Cada VLAN utiliza un dominio de broadcast, por lo que el tráfico de todo este dominio es independiente, con esto se elimina el riesgo de que un enlace que no pertenece al dominio de una VLAN en particular afecte los enlaces de otras VLANs.

- El proyecto aportó también a la integración de un concepto de gran relevancia que es la capacidad de acceso remoto, de este modo se podrán mirar las cámaras IP fuera de la red del edificio municipal, debiéndose configurar en el router un servidor virtual por cada cámara, para que por medio de NAT (redireccionamiento de puertos) se pueda acceder directamente al servidor de cada cámara.
- El GADMT al contar con una estructura predefinida para el cableado estructurado facilita la elaboración del diseño de la red de vigilancia ya que pone en evidencia la factibilidad técnica y económica, al utilizar equipos y aprovechar el cableado existente, proporcionando un ahorro considerable a la municipalidad. Para corroborar lo mencionado al realizarse el análisis financiero se obtuvieron resultados ventajosos, constituyéndose en un proyecto rentable.

6.11 RECOMENDACIONES

- Se debe permitir el acceso a los equipos de la red IP únicamente a las personas autorizadas, para de esta manera salvaguardar la seguridad de los mismos y evitar daños en el sistema de video-vigilancia.
- Al ser la conexión remota a través de Internet se recomienda que este servicio sea utilizado por el menor número de personas desde el exterior, ya que al otorgar permiso a muchos usuarios, se podría provocar lentitud en las solicitudes realizadas.
- Para incrementar la seguridad del enlace local y remoto, se sugiere el uso de políticas y mecanismos de seguridad a configurarse en los equipos de comunicaciones.
- Es de gran utilidad contar con un servidor de respaldo, para que en caso de una falla que no se pueda corregir fácilmente, el sistema continúe monitoreando el lugar.

- Tener respaldos de los videos en alguna unidad externa, de esta manera se evitará saturar la capacidad de disco del servidor y permitirá contar con grabaciones para la conservación de evidencias.
- Se recomienda explotar las funciones de las cámaras, esto es la alarma, enviar mensajes a celulares, alertas por correo electrónico con un software complementario, entre otros.
- Se debe realizar el mantenimiento preventivo del sistema de seguridad para garantizar su pleno funcionamiento luego de la fase de instalación.
- Para la administración de la red de video-vigilancia IP, es necesario contar con una detallada documentación de los equipos, configuraciones y direccionamiento IP, con la finalidad de evitar errores en la gestión y manejo del sistema.

6.12 BIBLIOGRAFÍA

- TOMASI, Wayne. *Sistemas de Comunicaciones Electrónicas*. Primera Edición. España. Editorial Prentice Hall. 1996.
- ROLDÁN, David. *Comunicaciones Inalámbricas: Un Enfoque Aplicado*. Primera Edición. Alfaomega Grupo Editor. México, Mayo 2005.
- NICHOLS, Randall. *Seguridad para Comunicaciones Inalámbricas*. Primera Edición en Español por McGraw-Hill/Interamericana de España 2003.
- CRAIG ZACKER, *Manual de referencia Redes*. Primera Edición en Español por McGraw-Hill/Interamericana de España.
- REGIS J. (Bud) BATES Jr. *Comunicaciones Inalámbricas de banda Ancha*. . Primera Edición en Español por McGraw-Hill/Interamericana de España 2003.
- HUIDROBO, José Manuel y ROLDAN, David. *Tecnología VoIP y Telefonía IP*. Primera Edición. Alfaomega Grupo Editor. México, Julio 2006.

6.13 LINKOGRAFÍA

- REDES ALÁMBRICAS E INALÁMBRICAS, publicado el lunes 1 de diciembre de 2008, <http://redesinaalam.blogspot.com/>
- EQUIPOS DE RED, publicado el Domingo 3 de Abril de 2011, <http://construiryadministrarredcbtis7740ele.blogspot.com/2011/04/equipos-de-red.html>
- D-LINK. COLECCIONABLE DE VIDEO-VIGILANCIA IP. Publicado el 15 de mayo del 2011. <http://www.videovigilanciadlink.es/pdf/D-Link-Coleccionable-Videovigilancia-IP-La-Resolucion-15-05-2011.pdf>
- AXIS. GUÍA TÉCNICA DE VÍDEO IP. Publicado en el 2009. http://www.axis.com/es/products/video/about_networkvideo/index.htm
- NOGUÉS, Albert. DIRECCIONAMIENTO IPv4. Publicado el 8 de octubre del 2008. http://www.albertnogues.com/attachments/014_IntroIp.pdf
- BOSCH. ESTIMANDO EL ANCHO DE BANDA. Traducido en el centro de aplicaciones para américa latina CASAL en mayo 2006. http://www.boschsecurity.com.mx/_archivos_productos_sitios_la/boletines_informativos/ebrief/2006/Estimando_Ancho_de_Banda.pdf
- CANAL DIGITAL.VIDEO-VIGILANCIA IP. Publicado el 14 de Junio de 2006. http://www.canal-digital.es/2717_videovigilancia-ip
- DIFERENCIAS ENTRE CÁMARAS IP CMOS Y CCD. Publicado el 23 MARZO 2010. <http://blog.fashionpcs.com/2010/03/23/diferencia-entre-camaras-cmos-y-ccd/>
- GEROMETTA, Oscar. INTRODUCCIÓN A ETHERNET Y ENRUTAMIENTO IP. Subido el 21 de julio del 2012. <http://es.scribd.com/doc/100682195/Introduccion-a-Ethernet-y-Enrutamiento-IP-Demo>
- EL SUBNETEO CON VLSM. Publicado el 2 de noviembre del 2012. <http://es.scribd.com/doc/48652540/El-subneteo-con-VLSM>

- NETSTORMING. PUERTOS BIEN CONOCIDOS. Publicado el 24 de septiembre del 2009. <http://www.netstorming.com.ar/2009/09/24/puertos-bien-conocidos/>
- TEXTOS CIENTÍFICOS. REDES VIRTUALES VLANS. Publicado el viernes, 3 de noviembre del 2006. <http://www.textoscientificos.com/redes/redes-virtuales>
- CISCOPACKETS. PACKET TRACER INTERVLAN ROUTING TUTORIAL. Publicado el 29 de diciembre del 2012. <http://www.youtube.com/watch?v=WFNc-X8LgcU&feature=related>
- CISCO REDES. VLAN. Publicado el viernes 19 de Octubre del 2012. <http://www.ciscoredes.com/ccna3/90-vlan.html>
- NETSTORMING. INTRODUCCIÓN A LAS VLAN. Publicado el 18 de enero del 2010. <http://www.netstorming.com.ar/2010/01/18/introduccion-a-las-vlan/>
- ENRUTAMIENTO ENTRE VLAN. Publicado el jueves 21 de abril del 2011. <http://www.redesymas.org/2011/04/intervlan-routing.html>
- CMD SISTEMAS. VLAN NATIVA, Publicado el 11 de enero del 2012. <http://cmdsistemas.wordpress.com/2012/01/11/vlan-nativa/>
- CISCO. SWITCHES DE CISCO CATALYST SERIE 2960. [http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/catalyst_2960_series_switches/index.html#~overview,](http://www.cisco.com/web/ES/solutions/smb/products/routers_switches/catalyst_2960_series_switches/index.html#~overview)
- VIVOTEK. CAMARAS IP. Copyright 2012. <http://www.vivotek.es/products/browse/1/c%C3%A1maras-ip>
- TRENDNET. CÁMARAS DE INTERNET. Copyright 2012. <http://www.trendnet.com/langsp/products/products.asp?cat=180>
- TRENDNET. GUIA DEL USUARIO SECURVIEW PRO. Copyright 2012. http://downloads.trendnet.com/tvip572wi/manuals/ug_securviewpro.pdf
- VSTARCAM. Copyright 2012. <http://www.vstarcam.com/>

6.14 ANEXOS

ANEXO 1. ENCUESTA REALIZADA A LOS EMPLEADOS ADMINISTRATIVOS DEL GADMT

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTÓNICA Y COMUNICACIONES

Encuesta dirigida al personal que conforma la Dirección de Gestión Administrativa del GADMT

OBJETIVO: Obtener información acerca de la situación y requerimientos actuales de la red, seguridad y vigilancia de la Institución Municipal

INSTRUCTIVO: Marque con una X en el paréntesis la(s) alternativa(s) que usted eligió.

FECHA:.....

1. **¿Considera usted que el GADMT cuenta con un sistema de vigilancia que permita la continua supervisión de las instalaciones del edificio municipal?**

Si

No

2. **¿Cual de las siguientes opciones considera usted de mayor eficiencia en el ámbito de seguridad y vigilancia institucional?**

Guardias
anteriores

Video-vigilancia electrónica

Las dos opciones

3. **¿Esta de acuerdo que la información procedente de un sistema de vigilancia de oficinas municipales sea visualizada?**

Si

No

4. **¿Cree conveniente la inspección de bienes a cualquier hora del día en el interior del edificio municipal?**

Si

No

5. **Tiene usted conocimiento de sucesos que se hayan efectuado en la institución, tales como:**

Hurto de bienes institucionales

Hurto de dinero

Hurto de bienes personales

Ningún suceso indebido

6. **¿Cómo califica el hecho de contar con un mecanismo de seguridad que almacene información de modo que pueda aportar como indicio para esclarecer un suceso indebido?**

Bueno

Malo

Regular

7. ¿A su criterio cuáles son las oficinas de la entidad municipal que requieren esencialmente de un sistema de video-vigilancia?

Aquellas que tienen a su cargo:

- Recursos económicos Bienes/Equipos Institucionales
 Todas las unidades

8. A su juicio seleccione la(s) principal(es) utilidad(es) que aportará un sistema de video-vigilancia en el GADMT:

- Seguridad para empleados municipales Supervisión durante las 24 horas del día
 Conservación de evidencias Todas los anteriores

9. ¿Como contempla usted el hecho de que el GADMT cuente con un sistema de video-vigilancia IP?

- Bueno Malo Regular

10. ¿Cómo considera la velocidad de internet del GADMT?

- Buena Aceptable Mala Regular

11. ¿Cuál es el tipo de información por internet al cual accede?

- Música Video Datos

12. ¿Con que frecuencia usa internet?

- Mucho Poco Nada

GRACIAS POR SU BENEFICIOSA COLABORACION

ANEXO 2. ENTREVISTA REALIZADA A LA DIRECTORA DE LA UNIDAD DE INFORMÁTICA DEL GADMT

PREGUNTAS A FORMULARSE PARA LA ENTREVISTA

La presente entrevista será realizada a la directora de la Unidad de Informática, Ingeniera Magaly Enríquez.

Objetivos:

- Conocer la situación actual de la red del GADMT.
- Determinar la factibilidad técnica y requerimientos para un sistema de video-vigilancia IP.
- Establecer la importancia de un sistema de video-vigilancia en la institución municipal.

DESARROLLO:

1. ¿Podría proporcionar una breve explicación a cerca de la red del Municipio?
2. ¿Como considera usted la velocidad del internet proporcionado en el edificio del GADMT?
3. ¿Cuál es la situación de la red municipal en lo referente al tráfico de datos?
4. Tomando en cuenta la situación actual de la red, ¿Existen propuestas o medidas a tomarse para un mejor desempeño de la misma?
5. ¿De qué forma se realiza la asignación de IP's para cada punto de red de la institución?
6. ¿Qué páginas web son permitidas a cada usuario de la red? (existen privilegios)
7. ¿Cuál es su percepción a cerca de los beneficios y ventajas que ofrece un sistema de vigilancia que permita el acceso remoto?
8. ¿Cuán importante considera usted la existencia de un sistema de video-vigilancia en una institución pública?

9. ¿Estaría de acuerdo con que la entidad municipal cuente con un sistema de video-vigilancia IP?

10. ¿Cuáles son las expectativas que debe cumplir un sistema de video-vigilancia en la institución?, desde el punto de vista:

Técnico:

Aplicación:

Ubicación:

11. ¿A su criterio cuáles serían los principales aspectos que requieren controlarse con un sistema de video-vigilancia en las oficinas del GADMT?

12. ¿A su parecer cuáles son las oficinas del edificio Municipal que requieren de un sistema de video-vigilancia?

13. ¿Alguna recomendación en cuanto al tipo de cámaras a emplearse en un sistema de video-vigilancia IP para el GADMT?

ANEXO 3. ESPECIFICACIONES TÉCNICAS DE LAS CÁMARAS DE RED SELECCIONADAS

- **TV-IP572PI**



Cámara de Internet PoE Megapíxel para día y noche

TV-IP572PI (v1.0R)

La Cámara de internet PoE Megapíxel para día y noche, modelo, TV-IP572PI, transmite en tiempo real videos de resolución megapíxel por Internet. Grabación de video con nitidez en plena oscuridad para distancias de hasta 7.5 metros. No necesita instalar la cámara cerca de una fuente de alimentación, ya que tanto los datos como la corriente se transmiten a través de un mismo cable Ethernet gracias a la tecnología Alimentación por Ethernet (PoE) (Ver conmutadores e inyectores PoE TRENDnet).

Graba videos 1280 x 800 Megapixel (WXGA) de hasta 30 fotogramas por segundo (fps). Administra hasta cuatro videoperfiles para grabar videos de alta definición al mismo tiempo que transmite en tiempo real videos de baja resolución a un teléfono inteligente compatible. Controle hasta 32 cámaras TRENDnet con el software complementario para gestión de cámara. Las características avanzadas incluyen zonas para la grabación por detección de movimientos, alertas por correo electrónico, grabaciones programadas, compresión de imagen H.264 / MPEG-4 / MJPEG, audio de dos vías, superposición de fecha y hora, ranura para tarjetas Micro-SD para el almacenamiento de copias de seguridad, audio de dos vías (no incluye altavoces), lentes ajustables y zoom digitales 4x. Viene con kit para montaje en pared o techo y la carcasa en blanco crema de la cámara combina a la perfección con la mayoría de los ambientes.

INFORMACIÓN GENERAL DEL PRODUCTO

- Para ver resoluciones megapíxel de hasta 1280 x 800 (WXGA)
- Visibilidad nocturna en un rango de hasta 7.5 metros *
- No necesita instalar la cámara cerca de una fuente de alimentación, ya que tanto los datos como la corriente se transmiten a través de un mismo cable Ethernet
- Programa para grabación en detección de movimiento, programación de grabación, alertas por correo-e y más con el software complementario
- Audio de 2 vías

Cámara de Internet PoE Megapíxel para día y noche TV-IP572PI (v1.0R)

CÁMARA DE
INTERNET

ESPECIFICACIONES

CÁMARA	
General	<ul style="list-style-type: none"> • Sensor: Sensor CMOS de 1/4 de pulgada • Lente en tablero • Distancia focal: 4 mm • F/No: 1.5 • Iluminación mínima: 0 lux • Profundidad de enfoque: 20 cm ~ infinito • Visión: <ul style="list-style-type: none"> • Horizontal: 51.8° • Vertical: 33.8° • Diagonal: 59.6° • Zoom Digital: 4x
Audio	<ul style="list-style-type: none"> • Micrófono omni-direccional integrado • Sensibilidad: -40 dB +/- 3 dB (máx 5 metros) • Frecuencia: 100~20000Hz • S/N: >60 dB • Codec: PCM / ADPCM • Salida para altavoz externo (los altavoces se venden por separado) • Audio de dos vías con cancelado de eco
Día / Noche	<ul style="list-style-type: none"> • Construido en ICR • Visión nocturna (IR) de hasta 7.5 metros*
HARDWARE	
Red	<ul style="list-style-type: none"> • IEEE 802.3u 10/100 Mbps Auto-MDIX Fast Ethernet • IEEE 802.3af Alimentación por Ethernet (PoE)
Pantalla LED	<ul style="list-style-type: none"> • Power (Encendido), Link/Act (Enlace/Actividad)
Ranura para tarjeta Micro SD	<ul style="list-style-type: none"> • Compatible con Micro SD (de hasta 32 GB)
Botón de reinicio	<ul style="list-style-type: none"> • Configuraciones de reinicio por defecto
Consumo eléctrico	<ul style="list-style-type: none"> • Máx 4.95 Vatios
Potencia	<ul style="list-style-type: none"> • Entrada : 120~240V AC, 50~60 Hz, 0.2A • Salida: Adaptador de alimentación externo 1.2A y 5V
Dimensiones	<ul style="list-style-type: none"> • 75 x 115 x 30 mm (2.95 x 4.5 x 1.2 pulgadas)
Peso	<ul style="list-style-type: none"> • 125 g (4.4 onzas)
Temperatura	<ul style="list-style-type: none"> • Funcionamiento: 0°C ~ 40°C (32°F ~ 104°F) • Almacenaje: -25°C ~ 70°C (-13°F ~ 158°F)
Humedad	<ul style="list-style-type: none"> • Máx 95% (sin condensación)
Certificación	<ul style="list-style-type: none"> • CE, FCC

Cámara de internet PoE Megapíxel para día y noche TV4P072PI (v1.0R)



ESPECIFICACIONES

REQUISITOS	
Interfaz de gestión	<ul style="list-style-type: none"> Internet Explorer 7.0 o superior Firefox, Safari, y Chrome
Para ejecutar el software	<ul style="list-style-type: none"> Windows 7 (32/64-bit), Vista (32/64-bit), XP (32/64-bit) Windows Server 2003, 2008
SeourView Pro Software	<ul style="list-style-type: none"> Canal: soporte hasta 32 cámaras Grabación / Reproducción / Detección de Movimiento / Audio
Protocolos de red admitidos	<ul style="list-style-type: none"> IPv4, ARP, TCP, UDP, ICMP DHCP Client, NTP Client, DNS Client, DDNS Client, SMTP Client, FTP Client HTTP Samba Client PPPoE UPnP LLTD RTP (Protocolo en tiempo real) RTCP (Protocolo de control en tiempo real) RTSP (Protocolo de transmisión en tiempo real) IGMP
GESTIÓN	
Sistema	<ul style="list-style-type: none"> Administración basada en Web Soporte NTPCA
Acceso	<ul style="list-style-type: none"> Hasta 20 cuentas de usuario
Copia de seguridad / Restauración	<ul style="list-style-type: none"> Guardar / recuperar los archivos de configuración
Registro	<ul style="list-style-type: none"> Registro del sistema de hasta 500 entradas
Micro SD	<ul style="list-style-type: none"> Visualización, descarga y eliminación de archivos Formatear y retirar tarjeta Micro SD
AJUSTES	
Imagen	<ul style="list-style-type: none"> Modos de brillo, contraste, saturación, nitidez, balance de blancos, rotación, espejo (vertical / horizontal), blanco / negro, interior, exterior, modo de programación Disparador :1/3.25s, 1/7.5s, 1/10s, y 1/15s
Ajuste de video	<ul style="list-style-type: none"> Perfil 1: H.264 / MPEG-4 <ul style="list-style-type: none"> Resolución: 1280 x 800, 640 x 400, 320 x 192, 160 x 96 Velocidad de cuadros máxima: 30fps Perfil 2: H.264 / MPEG-4 <ul style="list-style-type: none"> Resolución: 640 x 400, 320 x 192, 160 x 96 Velocidad de cuadros máxima: 30fps Perfil 3: MJPEG <ul style="list-style-type: none"> Resolución: 1280 x 800, 640 x 400, 320 x 192, 160 x 96 Velocidad de cuadros máxima: 1280 x 800 @ 5fps, 640 x 400 / 320 x 192 @ 30fps Calidad JPEG: Muy Bajo, Bajo, Medio, Alto, Muy Alto Perfil 4: H.264 / MPEG-4 <ul style="list-style-type: none"> Resolución: 640 x 400, 320 x 192, 160 x 96 Velocidad de cuadros máxima: 30fps RTSP: http://pcamera_ip/3gpp
3GPP	<ul style="list-style-type: none"> Códec de video: MPEG-4 (sin soporte de audio) Protocolos: RTSP, RTP
Grabación	<ul style="list-style-type: none"> Resolución: Define resolución individual para hasta 4 perfiles Almacenamiento necesario: 32 MB (mínimo por perfil) Tipo de grabación: basado en eventos (detección de movimiento y disparador de entreda digital), continuo y programado

Cámara de Internet PoE Megapíxel para día y noche TV-IP572PI (v1.0R)



ESPECIFICACIONES

AJUSTES

Acción de eventos	<ul style="list-style-type: none">• Evento disparador: detección de movimiento o entrada de señal digital• Acción: envía en tiempo real instantáneas o grabaciones de video via FTP o correo electrónico
Ajustes del puerto	<ul style="list-style-type: none">• Puerto HTTP: 80 (predeterminado)• Puerto RTSP: 554 (predeterminado)
Hora	<ul style="list-style-type: none">• Sincronizada con servidor NTP o ajuste manual de la fecha / hora

SOLUCIÓN EN REDES



CONTENIDOS DEL PAQUETE

TV-IP572PI
CD-ROM (herramienta y guía del usuario)
Guía de instalación rápida multilingüe
Cable de red (1,5 m / 5 pies)
Adaptador de corriente (5V, 1.2A)
Conjunto de montaje de la cámara

PRODUCTOS RELACIONADOS

TV-IP572P	Cámara de internet PoE megapíxel
TV-IP572WI	Cámara de internet Megapíxel inalámbrica N para día y noche
TV-IP672PI	Cámara de internet Megapíxel inalámbrica N PTZ para día y noche

INFORMACION DE LA ORDEN



20675 Manhattan Place, Torrance, CA 90501 USA
Tel: 1-310-961-5500
Fax: 1-310-961-5511
Web: www.trendnet.com
Email: sales@trendnet.com

- **TV-IP672PI**



Cámara de Internet PoE Megapíxel PTZ para día / noche

TV-IP672PI (V1.0R)

La Cámara de internet PoE Megapíxel PTZ para día / noche, modelo TV-IP672PI de TRENDnet le ofrece vigilancia de seguridad durante el día y la noche dentro de un área muy amplia. Mueva la cámara de un lado a otro en un ángulo de 340° e inclínela hacia arriba o hacia abajo unos 115° desde cualquier conexión a Internet. Grabación de video con nitidez en plena oscuridad para distancias de hasta 7.5 metros. No necesita instalar la cámara cerca de una fuente de alimentación, ya que tanto los datos como la corriente se transmiten a través de un mismo cable Ethernet gracias a la tecnología Power over Ethernet (PoE) (Ver conmutadores e inyectores PoE TRENDnet).

Graba videos 1280 x 800 Megapixel (WXGA) de hasta 30 fotogramas por segundo (fps). Administra hasta cuatro videoperfiles para grabar videos de alta definición al mismo tiempo que transmite en tiempo real videos de baja resolución a un teléfono inteligente compatible. Controle hasta 32 cámaras TRENDnet con el software complementario para gestión de cámara. Las características avanzadas incluyen zonas para la grabación por detección de movimientos, alertas por correo electrónico, grabaciones programadas, vigilancia automática con movimiento vertical y horizontal (giro / inclinación), patrulla automática, compresión de imagen H.264 / MPEG-4 / MJPEG, audio de dos vías, superposición de fecha y hora, ranura para tarjetas Micro-SD para el almacenamiento de copias de seguridad, audio de dos vías (no incluye altavoces), lentes ajustables y zoom digitales 4x. Viene con kit para montaje en pared o techo y la carcasa en blanco crema de la cámara combina a la perfección con la mayoría de los ambientes.

INFORMACIÓN GENERAL DEL PRODUCTO

- Para ver resoluciones megapixel de hasta 1280 x 800 (WXGA)
- Visión nocturna de hasta 7.5 metros en interiores*
- Movimiento de la cámara de un lado a otro en un ángulo de 340° e inclinación hacia arriba o hacia abajo en un ángulo de 115°
- No necesita instalar la cámara cerca de una fuente de alimentación, ya que tanto los datos como la corriente se transmiten a través de un mismo cable Ethernet
- Programa para grabación en detección de movimiento, programación de grabación, alertas por correo-e y más con el software complementario
- Audio de 2 vías

Cámara de internet PoE Megapíxel PTZ para día / noche TV4P672PI (v1.0R)

CÁMARAS DE
INTERNET

ESPECIFICACIONES

CÁMARA	
General	<ul style="list-style-type: none"> • Sensor: Sensor CMOS de 1/4 de pulgada • Lente en tablero • Distancia focal: 4mm • F/No: 1.5 • Iluminación mínima: 0 lux • Profundidad de enfoque: 20 cm ~ infinito • Visión: <ul style="list-style-type: none"> • Horizontal: 51.8° • Vertical: 33.8° • Diagonal: 59.6° • Zoom Digital: 4x
Audio	<ul style="list-style-type: none"> • Micrófono omni-direccional integrado • Sensibilidad: -40 dB +/- 3 dB (máx 5 metros) • Frecuencia: 100~20000 Hz • S/N: >60dB • Formato: PCM / ADPCM • Salida para altavoz externo (los altavoces se venden por separado) • Audio de dos vías con cancelado de eco
Giro / Inclinación	<ul style="list-style-type: none"> • Giro: -170° ~ +170° • Inclinación: hacia arriba 90° y hacia abajo 25° • Posiciones predeterminada: 10
Día / Noche	<ul style="list-style-type: none"> • Construido en ICR • Visión nocturna (IR) de hasta 7.5 metros
HARDWARE	
Red	<ul style="list-style-type: none"> • IEEE 802.3u 10/100 Mbps Auto-MDIX Fast Ethernet • IEEE 802.3af Alimentación por Ethernet(PoE)
Pantalla LED	<ul style="list-style-type: none"> • Power (Encendido), Link/Act (Enlace/Actividad)
Botón de reinicio	<ul style="list-style-type: none"> • Configuraciones de reinicio por defecto
Botón de privacidad	<ul style="list-style-type: none"> • Modo de privacidad de encendido / apagado
Consumo eléctrico	<ul style="list-style-type: none"> • Máx 9 Watts
Potencia	<ul style="list-style-type: none"> • Entrada: 120~240V AC, 50~60 Hz, 0.2A • Salida: Adaptador de alimentación externo 1.25A y 12V
Dimensiones	<ul style="list-style-type: none"> • 113 x 113 x 130 mm (4.5 x 4.5 x 5.1 pulgadas)
Peso	<ul style="list-style-type: none"> • 500 g (1.1 libras)
Temperatura	<ul style="list-style-type: none"> • Funcionamiento: 0°C ~ 40°C (32°F ~ 104°F) • Almacenaje: -25°C ~ 70°C (-13°F ~ 158°F)
Humedad	<ul style="list-style-type: none"> • Máx 90% (sin condensación)
Certificación	<ul style="list-style-type: none"> • CE, FCC
REQUISITOS	
Interfaz de gestión	<ul style="list-style-type: none"> • Internet Explorer 7.0 o superior • Firefox, Safari, y Chrome
Para ejecutar el software	<ul style="list-style-type: none"> • Windows 7 (32/64-bit), Vista (32/64-bit), XP (32/64-bit) • Windows Server 2003, 2008
SecurView Pro Software	<ul style="list-style-type: none"> • Canal: soporte hasta 32 cámaras • Grabación / reproducción / detección de movimiento / audio

Cámara de internet PoE Megapixel PTZ para día / noche TVIP672PI (v1.0R)



ESPECIFICACIONES

REQUISITOS

Protocolos de red admitidos	<ul style="list-style-type: none"> • IPv4, ARP, TCP, UDP, ICMP • DHCP Client, NTP Client, DNS Client, DDNS Client, SMTP Client, FTP Client • HTTP • Samba Client • PPPoE • UPnP • LLTD • RTP (Protocolo en tiempo real) • RTCP (Protocolo de control en tiempo real) • RTSP (Protocolo de transmisión en tiempo real) • 3GPP (Sólo video)
------------------------------------	--

GESTIÓN

Sistema	• Administración basada en Web
Acceso	• Hasta 20 cuentas de usuario
Copla de seguridad / Restauración	• Guardar / recuperar los archivos de configuración
Registro	• Registro del sistema de hasta 500 entradas
Micro SD	<ul style="list-style-type: none"> • Visualización, descarga y eliminación de archivos • Formatear y retirar tarjeta Micro SD

AJUSTES

Imagen	<ul style="list-style-type: none"> • Modos de brillo, contraste, saturación, nitidez, balance de blancos, rotación, espejo (vertical / horizontal), blanco / negro, interior, exterior, modo de programación • Disparador: 1/3.25s, 1/7.5s, 1/10s, y 1/15s
Ajuste de video	<ul style="list-style-type: none"> • Perfil 1: H.264 / MPEG-4 <ul style="list-style-type: none"> • Resolución: 1280 x 800, 640 x 400, 320 x 192, 160 x 96 • Velocidad de cuadros máxima: 30fps • Perfil 2: H.264 / MPEG-4 <ul style="list-style-type: none"> • Resolución: 640 x 400, 320 x 192, 160 x 96 • Velocidad de cuadros máxima: 30fps • Perfil 3: MJPEG <ul style="list-style-type: none"> • Resolución: 1280 x 800, 640 x 400, 320 x 192, 160 x 96 • Velocidad de cuadros máxima: 1280 x 800 @ 5fps, 640 x 400 / 320 x 192 @ 30fps • Calidad JPEG: Muy Bajo, Bajo, Medio, Alto, Muy Alto • Perfil 4: H.264 / MPEG-4 <ul style="list-style-type: none"> • Resolución: 640 x 400, 320 x 192, 160 x 96 • Velocidad de cuadros máxima: 30fps • RTSP: http://ipcamera_ip/3gpp
3GPP	<ul style="list-style-type: none"> • Formato de audio: AMR • Formato de video: MPEG-4 • Protocolos: RTSP, RTP, RTCP
Grabación	<ul style="list-style-type: none"> • Resolución: Define resolución individual para hasta 4 perfiles • Almacenamiento necesario: 32 MB (mínimo por perfil) • Tipo de grabación: basado en eventos (detección de movimiento y disparador de entrada digital), continuo y programado
Instantánea	<ul style="list-style-type: none"> • Evento disparador: detección de movimiento o entrada de señal digital • Acción: envía en tiempo real instantáneas o grabaciones de video via FTP o correo electrónico.
Ajustes del puerto	<ul style="list-style-type: none"> • Puerto HTTP: 80 (predeterminado) • Puerto RTSP: 554 (predeterminado)
Hora	• Sincronizada con servidor NTP o ajuste manual de la fecha / hora

Cámara de internet PoE Megapíxel PTZ para día / noche TV-IP672PI (v1.0R)

CÁMARAS DE
INTERNET

SOLUCIÓN EN REDES



CONTENIDOS DEL PAQUETE

TV-IP672PI

CD-ROM (herramienta y guía del usuario)

Guía de instalación rápida multilingüe

Cable de red (1,5 m / 5 pies)

Adaptador de corriente (12V, 1,25A)

Conjunto de montaje de la cámara

PRODUCTOS RELACIONADOS

TV-IP672P	Cámara de internet PoE Megapíxel PTZ
TV-IP651WI	Cámara de internet inalámbrica N con movimiento horizontal y vertical para día / noche
TV-IP672WI	Cámara de internet Megapíxel inalámbrica N PTZ para día / noche

INFORMACION DE LA ORDEN

TRENDNET

20675 Manhattan Place, Torrance, CA 90501 USA

Tel: 1-310-961-5500

Fax: 1-310-961-5511

Web: www.trendnet.com

Email: sales@trendnet.com

- **TV-IP422WN**



Cámara de Internet inalámbrica N SecurView con movimiento horizontal y vertical para día/noche TV-IP422WN(V1.0R)

La cámara de Internet inalámbrica con movimiento horizontal y vertical para día/noche SecurView, modelo TV-IP422WN, ofrece protección durante el día y la noche sobre un área extensa. Mueva la cámara de un lado a otro en un ángulo de 330 grados e inclínela hacia arriba o hacia abajo unos 105 grados.

La tecnología inalámbrica N le ofrece cobertura inalámbrica sin igual así como una mejor calidad de video en tiempo real. Incorpore esta cámara a su red inalámbrica con tan sólo tocar un botón con la configuración Wi-Fi protegida (WPS).

Las bombillas de infrarrojos garantizan la visión nocturna en plena oscuridad a distancias de hasta 5 metros (16 pies). Un micrófono integrado y altavoces opcionales permiten la comunicación de audio de 2 vías. Controle hasta 32 cámaras SecurView con el software complementario para gestión de cámara. Las características avanzadas de la cámara incluyen grabación por detección de movimientos, alertas de correo electrónico, sesiones de grabación programadas, compresión de imágenes MPEG-4/MJPEG, soporte 3GPP, un puerto USB opcional, vigilancia automática predeterminada, puertos de entrada y salida, y zoom digital. Viene con kit para montaje en pared o techo y la carcasa en blanco crema de la cámara combina a la perfección con la mayoría de los ambientes.

CARACTERÍSTICAS

- Wi-Fi compatible con redes IEEE 802.11b/g/n
- zoom digital 3x
- 1 x puerto Fast Ethernet a 10/100Mbps
- 1 botón de configuración Wi-Fi protegida
- 1 puerto USB que le permite almacenar imágenes fijas directamente en una unidad flash USB*
- Mueva la cámara de un lado a otro en un ángulo de 330 grados e inclínela hacia arriba o hacia abajo unos 105 grados desde cualquier conexión a Internet.
- Grabación de video MPEG-4 y MJPEG de alta calidad
- Resolución de hasta 640 x 480 píxeles
- Indicadores LED de alimentación y actividad (se pueden desactivar)
- Visión nocturna por infrarrojos hasta 5 metros (16 pies)
- DNS dinámico
- Controles de imagen: Brillo, contraste, saturación y reflejo de imagen horizontal/vertical
- Soporta red TCP/IP, correo electrónico, HTTP, Samba y otros protocolos de Internet
- Grabe videos en tiempo real transmitidos a su computador y servidor de almacenamiento de red
- Alertas por correo electrónico y subida de imágenes via FTP accionadas por detección de movimientos
- Transmite video de la cámara de Internet a dispositivos inalámbricos compatibles con 3GPP
- Soporta 64/128-bit WEP, WPA/WPA2 y WPA-PSK/WPA2-PSK
- Escuchar y hablar con la gente en el área de visualización de la cámara a través del ordenador.
- Dos ventanas ajustables de detección de movimientos con instantánea justa a tiempo
- Instalación Universal Plug and Play (UPnP) rápida
- Software SecurView Pro gratis: gestiona hasta 32 cámaras **
- Garantía limitada de 3 años

Cámara de Internet Inalámbrica N SecurView con movimiento horizontal y vertical para día/noche TV-IP422WN[V1.0R]

Especificaciones

Cámara	
General	<ul style="list-style-type: none"> • Sensor: Sensor CMOS a color de 1/2.5 de pulgada • Resolución: 640 x 480 píxeles • Junta de lente • Distancia focal: 4.0mm • Abertura (F/No): F1.8 • LED de luz infrarroja con control de sensor de luz • Iluminación mínima: 0.5 Lux • Ángulo de visualización en diagonal: 64°
Giro y inclinación	<ul style="list-style-type: none"> • Giro: +165°~165° • Inclinación: +90° ~ -15° • Posizioni preimpostate: 20 posizioni
Imagen y vídeo	<ul style="list-style-type: none"> • Compresión: Imágenes MPEG-4/MJPEG de doble transmisión • Controllo esposizione, bilanciamento dei bianchi, controllo di guadagno: automatico • Resolución: hasta 30fps VGA (640x480), 30fps QVGA (320x240), 30fps QOVGA (160x120)
Audio	<ul style="list-style-type: none"> • Entrada de audio: Micrófono omni-direccional integrado • Sensibilidad: -48dB +/- 3dB • Frecuencia: 50 ~ 16000Hz • Salida de audio: entrada externa a altavoz activo (mono) • Cancelación de eco: procesador de voz (hardware) • Códec de audio: PCMIAMR
Hardware	
Red	<ul style="list-style-type: none"> • IEEE 802.3u 10/100Mbps Fast Ethernet, Auto-MDIX
Pantalla LED	<ul style="list-style-type: none"> • Encendido, Enlace
Botón de Reinicio	<ul style="list-style-type: none"> • Configuraciones de reinicio por defecto
Botón de WPS	<ul style="list-style-type: none"> • 1 botón pulsador de configuración Wi-Fi protegida
Consumo eléctrico	<ul style="list-style-type: none"> • 10 watts max.
Potencia	<ul style="list-style-type: none"> • Adaptador de alimentación externo 1.5A y 12V (3.5 mm plug)
Dimensiones	<ul style="list-style-type: none"> • 115 x 110 x 105 mm (4.53 x 4.33 x 4.13 pulgadas)
Peso	<ul style="list-style-type: none"> • 360 g (12.6 oz)
Temperatura	<ul style="list-style-type: none"> • Funcionamiento: 0°C ~ 45°C (32°F ~ 113°F) • Almacenaje: -15°C ~ 60°C (5°F ~ 140°F)
Humedad	<ul style="list-style-type: none"> • Max. 90% (non-condensing)
Certificación	<ul style="list-style-type: none"> • CE, FCC
Requisitos	
Interfaz de gestión	<ul style="list-style-type: none"> • Internet Explorer 6.0 o superior
para ejecutar SecurView Pro	<ul style="list-style-type: none"> • Windows 7 (32/64 bit), Vista (32/64 bit), XP (32/64 bit)
Software SecurView Pro	<ul style="list-style-type: none"> • Canal: soporta hasta 32 cámaras • Grabación/reproducción/detección de movimiento
Protocolos de red admitidos	<ul style="list-style-type: none"> • TCP/IP, UDP, ICMP, DHCP, NTP, DNS, DDNS, SMTP, FTP, HTTP, Samba, PPPoE, UPnP, Bonjour, RTP, RTSP, RTCP
Inalámbrico	
Estándares	<ul style="list-style-type: none"> • Basado en la tecnología IEEE 802.11n • compatible con redes IEEE 802.11b/g
Frecuencia	<ul style="list-style-type: none"> • 2.4 ~ 2.4835GHz
Antena	<ul style="list-style-type: none"> • 1 Antena Dipolo de 2dBi desmontable con conector SMA inverso
Transmisión de datos (Recuperación automática)	<ul style="list-style-type: none"> • 802.11n: hasta 150Mbps • 802.11g: hasta 54Mbps • 802.11b: hasta 11Mbps
Seguridad	<ul style="list-style-type: none"> • 64/128-bit WEP, WPA/WPA2-PSK
Salida de alimentación eléctrica	<ul style="list-style-type: none"> • 802.11n: 15 ±1 dBm • 802.11b: 15 ±1 dBm • 802.11g: 10 ±1 dBm
Sensibilidad de recepción	<ul style="list-style-type: none"> • 802.11n HT20: -67dBm • 802.11n HT40: -64dBm • 802.11g: -70dBm • 802.11b: -87dBm
Canales	<ul style="list-style-type: none"> • 1~11 (FCC), 1~13(ETSII)
Gestión	
Inicio de sesión remoto	<ul style="list-style-type: none"> • Gestión remota apoyo
Copia de seguridad /Restauración	<ul style="list-style-type: none"> • Guardar/recuperar los archivos de configuración

Cámara de Internet inalámbrica N SecurView con movimiento horizontal y vertical para día/noche
TV-IP422WN(V1.0R)

Especificaciones

Imagen	
Image	• Modos de brillo, contraste, saturación, rotación, espejo (vertical/horizontal), blanco/negro
Video	• Tipo de codificación: MJPEG • Resolución: 640 x 480, 320 x 240, 160 x 120 • Velocidad de cuadros: 1~30 fps • Compresión: 5 levels
Grabación	• Tipo de grabación: continua, programada o por detección de movimiento con software
Múltiple perfiles	• 3 perfiles simultáneos
Ajustes del puerto	• Puerto HTTP: 80 (predeterminado)
Zoom digital	• 3x
DNS dinámico	• Sí
Hora	• Sincronizada con servidor NTP o ajuste manual de la fecha/hora
SMTP	• Correo SMTP que admite hasta dos cuentas con software
Log de sistema	• 100 entradas (máx.)

NETWORKING SOLUTIONS



Contenidos del paquete

TV-IP422WN
QIG multilingüe
CD-ROM (herramienta y guía del usuario)
Adaptador de corriente (12V, 1.5A)
Cable de red (1.8 m/5.9 pi.)
Soporte de montaje

Productos Relacionados

TV-IP121WN	Cámara de Internet inalámbrica N SecurView para día y noche
TV-IP312WN	Cámara de Internet inalámbrica N para día y noche SecurView
TV-IP110WN	Cámara de Internet inalámbrica N SecurView

ANEXO 4. CARACTERISTICAS DE LOS SWITCHES DE CISCO CATALYST 2960

Feature	Benefit
Ease of Use and Deployment	<ul style="list-style-type: none"> • Express Setup simplifies initial configuration with a Web browser, eliminating the need for more complex terminal emulation programs and CLI knowledge. • IEEE 802.3af and Cisco prestandard PoE support comes with automatic discovery to detect a Cisco prestandard or IEEE 802.3af endpoint and provide the necessary power without any user configuration. • Auto Install for configuration and Image update: Simplify management of large number of switches, by automatically downloading specified configuration and image • DHCP autoconfiguration of multiple switches through a boot server eases switch deployment. • Automatic QoS (Auto QoS) simplifies QoS configuration in voice-over-IP (VoIP) networks by issuing interface and global switch commands to detect Cisco IP phones, classify traffic, and enable egress queue configuration. • Autosensing on each 10/100 port detects the speed of the attached device and automatically configures the port for 10- or 100-Mbps operation, easing switch deployment in mixed 10- and 100-Mbps environments. • Autonegotiating on all ports automatically selects half- or full-duplex transmission mode to optimize bandwidth. • Dynamic Trunking Protocol (DTP) helps enable dynamic trunk configuration across all switch ports. • Port Aggregation Protocol (PAgP) automates the creation of Cisco Fast EtherChannel® groups or Gigabit EtherChannel groups to link to another switch, router, or server. • Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad. This feature is similar to Cisco EtherChannel technology and PAgP. • DHCP Server enables a convenient deployment option for the assignment of IP addresses in networks that do not have without a dedicated DHCP server. • DHCP Relay allows a DHCP relay agent to broadcast DHCP requests to the network DHCP server. • 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-BX, 100BASE-FX, 100BASE-LX, 100BASE-BX, and coarse wavelength-division multiplexing (CWDM) physical interface support through a field-replaceable SFP module provides unprecedented flexibility in switch deployment. • The default configuration stored in flash memory ensures that the switch can be quickly connected to the network and can pass traffic with minimal user intervention. • Automatic medium-dependent interface crossover (Auto-MDIX) automatically adjusts transmit and receive pairs if an incorrect cable type (crossover or straight-through) is installed on a copper port. • Time-domain reflectometer (TDR) to diagnose and resolve cabling problems on copper ports. • Configuration Rollback provides the capability to replace the current running configuration with any saved Cisco IOS® Software configuration file. This functionality can be used to revert to a previous configuration state, effectively rolling back any configuration changes that were made since that configuration file was saved. • DHCP Auto Install (Boot Host DHCP) and Auto Image Update allows the switch to automatically download a configuration file and IOS image (future).

Manageability	
Superior Manageability	<ul style="list-style-type: none"> • Cisco IOS Software CLI support provides a common user interface and command set with all Cisco routers and Cisco Catalyst desktop switches. • IP Service Level Agreement (responder only) uses active monitoring to generate traffic in a continuous, reliable, and predictable manner, thus enabling the measurement of network performance and health. • Switching Database Manager templates for security and QoS allow administrators to easily adjust memory allocation to the desired features based on deployment-specific requirements. • VLAN trunks can be created from any port using standards-based 802.1q tagging. • Up to 255 VLANs per switch and up to 128 spanning-tree instances per switch are supported. • Four thousand VLAN IDs are supported. • Voice VLAN simplifies telephony installations by keeping voice traffic on a separate VLAN for easier administration and troubleshooting. • Cisco VTP supports dynamic VLANs and dynamic trunk configuration across all switches. • IGMPv3 snooping for IPv4 and MLD v1 and v2 Snooping for IPv6 provide fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. • Remote SPAN (RSPAN) allows administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network. • For enhanced traffic management, monitoring, and analysis, the Embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events). • Layer 2 trace route eases troubleshooting by identifying the physical path that a packet takes from source to destination. • All RMON groups are supported through a SPAN port, which permits traffic monitoring of a single port, or a group of ports, from a single network analyzer or RMON probe. • Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent timestamp to all intranet switches. • Multifunction LEDs per port for port status; half-duplex and full-duplex mode; and 10BASE-T, 100BASE-TX, and 1000BASE-T indication as well as switch-level status LEDs for system, and redundant power supply provide a comprehensive and convenient visual management system. • Cisco Discovery Protocol Versions 1 and 2 help enable automatic switch discovery for network management tools and communicate Voice VLAN information with Cisco IP phones. • Link Layer Discovery Protocol (LLDP) and LLDP Media Extensions (LLDP-MED) including client location information. Switches exchange link and device information in multivendor networks. • IPv6 Host provides basic IPv6 management such as IPv4/IPv6 dual stack, unicast address types, ICMPv6, AAAA DNS lookup over IPv4, Secure Shell (SSH) for v6, IPv6 neighbor discovery, CDP, Telnet, TFTP, SNMP, HTTP, HTTPS, Traceroute, syslog for v6.
Cisco Network Assistant Software	<ul style="list-style-type: none"> • Cisco Network Assistant is a no-charge, Windows-based application that simplifies the administration of networks of up to 250 users. It supports a wide range of Cisco Catalyst intelligent switches. With Cisco Network Assistant, users can manage Cisco Catalyst switches and launch the device managers of Cisco Integrated Services Routers and Cisco Aironet® WLAN access points. • The easy-to-use graphical interface provides both a topology map and front-panel view of the cluster and stacks. • Configuration wizards need just a few user inputs to automatically configure the switch to optimally handle different types of traffic: voice, video, multicast, and high-priority data. • A security wizard is provided to restrict unauthorized access to applications, servers, and networks. • Upgrading the Cisco IOS Software on Cisco Catalyst switches is a simple matter of pointing and clicking, with one-click upgrades. • Cisco Network Assistant supports multilayer feature configurations such as routing protocols, ACLs, and QoS parameters. • Multidevice and multipoint configuration capabilities allow administrators to save time by configuring features across multiple switches and ports simultaneously. • The user-personalized interface allows modification of polling intervals, table views, and other settings. • Alarm notification provides automated e-mail notification of network errors and alarm thresholds.
Cisco Express Setup	<ul style="list-style-type: none"> • Express Setup simplifies initial configuration of a switch through a Web browser, eliminating the need for terminal emulation programs and CLI knowledge. • The Web interface helps less-skilled personnel quickly and simply set up switches, thereby reducing the cost of deployment.

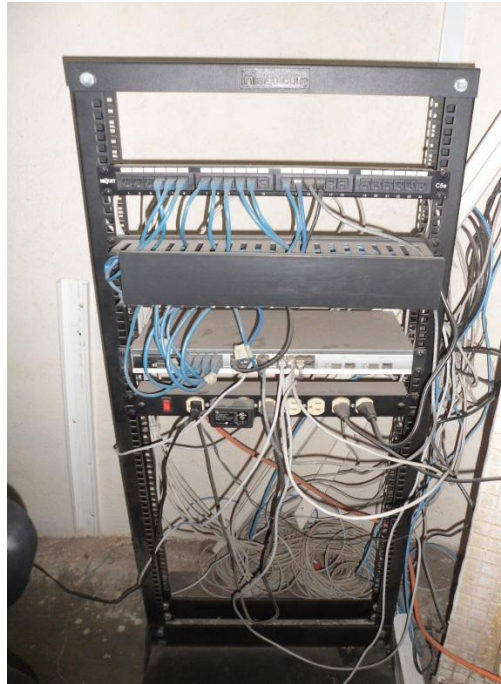
CiscoWorks Support	<ul style="list-style-type: none"> • CiscoWorks network-management software provides management capabilities on a per-port and per-switch basis, providing a common management interface for Cisco routers, switches, and hubs. • SNMPv1, v2c, and v3 and Telnet Interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. • The CiscoWorks LAN Management Solution supports the Cisco Catalyst 2960 Series.
Availability and Scalability	
Superior Redundancy for Fault Backup	<ul style="list-style-type: none"> • IEEE 802.1x Voice-aware security disables the offending data VLAN when a violation is detected without affecting Voice VLAN on the same switch port. • IEEE 802.1x readiness check determines readiness of connected end hosts, before configuring 802.1x on the switch. • Cisco UplinkFast and BackboneFast technologies help ensure quick failover recovery, enhancing overall network stability and reliability. • IEEE 802.1w Rapid Spanning Tree Protocol provides rapid spanning-tree convergence independent of spanning-tree timers and the benefit of distributed processing. • Per-VLAN Rapid Spanning Tree Plus (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. • Command-switch redundancy enabled in Cisco Network Assistant software allows designation of a backup command switch that takes over if the primary command switch fails. • Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD allow unidirectional links to be detected and disabled to avoid problems such as spanning-tree loops. • Switch port autorecovery (errdisable) automatically attempts to re-enable a link that is disabled because of a network error. • Cisco Redundant Power System 2300 (RPS 2300) support provides superior internal power-source redundancy for up to six Cisco networking devices, resulting in improved fault tolerance and network uptime. • Bandwidth aggregation up to 8 Gbps through Cisco Gigabit EtherChannel technology and up to 800 Mbps through Cisco Fast EtherChannel technology enhances fault tolerance and offers higher-speed aggregated bandwidth between switches and to routers and individual servers. • Flex Links provides link redundancy with convergence time 100ms without requiring Spanning Tree Protocol. • VLAN Flex Links load balancing improves network throughput by utilizing both links for traffic distribution for different VLANs. • Link State Tracking provides Layer 2 redundancy in the network when used in conjunction with server or programmable logic controller (PLC) network interface card (NIC) adapter teaming.
Integrated Cisco IOS Software Features for Bandwidth Optimization	<ul style="list-style-type: none"> • Per-port broadcast, multicast, and unicast storm control prevents faulty end stations from degrading overall systems performance. • IEEE 802.1d Spanning Tree Protocol support for redundant backbone connections and loop-free networks simplifies network configuration and improves fault tolerance. • PVST+ allows for Layer 2 load sharing on redundant links to efficiently use the extra capacity inherent in a redundant design. • IEEE 802.1s Multiple Spanning Tree Protocol allows a spanning-tree instance per VLAN, enabling Layer 2 load sharing on redundant links. • Egress committed rate (ECR) guarantee provides load balancing and redundancy. • Local Proxy Address Resolution Protocol (ARP) works in conjunction with Private VLAN Edge to minimize broadcasts and maximize available bandwidth. • VLAN1 minimization allows VLAN1 to be disabled on any individual VLAN trunk link. • VLAN Trunking Protocol (VTP) pruning limits bandwidth consumption on VTP trunks by flooding broadcast traffic only on trunk links required to reach the destination devices. • Internet Group Management Protocol (IGMP) version 3 snooping provides fast client joins and leaves of multicast streams and limits bandwidth-intensive video traffic to only the requestors. • IGMP filtering provides multicast authentication by filtering out no subscribers and limits the number of concurrent multicast streams available per port. • Multicast VLAN registration (MVR) continuously sends multicast streams in a multicast VLAN while isolating streams from subscriber VLANs for bandwidth and security reasons.

QoS and Control	
Advanced QoS	<ul style="list-style-type: none"> • Standard 802.1p CoS and DSCP field classification are provided, using marking and reclassification on a per-packet basis by source and destination IP address, source and destination MAC address, or Layer 4 TCP or UDP port number. • Cisco control-plane and data-plane QoS ACLs on all ports help ensure proper marking on a per-packet basis. • Four egress queues per port enable differentiated management of up to four traffic types. • SRR scheduling ensures differential prioritization of packet flows by intelligently servicing the ingress and egress queues. • Weighted tail drop (WTD) provides congestion avoidance at the ingress and egress queues before a disruption occurs. • Strict priority queuing guarantees that the highest-priority packets are serviced ahead of all other traffic. • There is no performance penalty for highly granular QoS functions.
Granular Rate Limiting	<ul style="list-style-type: none"> • The Cisco CIR function guarantees bandwidth in increments as small as 1 Mbps. • Rate limiting is provided based on source and destination IP address, source and destination MAC address, Layer 4 TCP and UDP information, or any combination of these fields, using QoS ACLs (IP ACLs or MAC ACLs), class maps, and policy maps. • Asynchronous data flows upstream and downstream from the end station or on the uplink are easily managed using ingress policing and egress shaping. • Up to 64 aggregate or individual polices are available per Fast Ethernet or Gigabit Ethernet port.

ANEXO 5. FOTOS DE LA RED DE COMUNICACIONES ACTUAL DEL GADMT

- **PLANTA BAJA**

Rack Planta Baja - Rentas

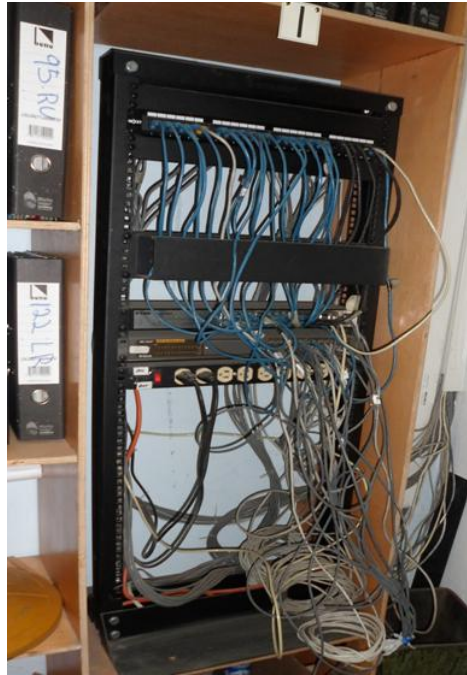


Rack Planta Baja – Ventanillas de recaudación



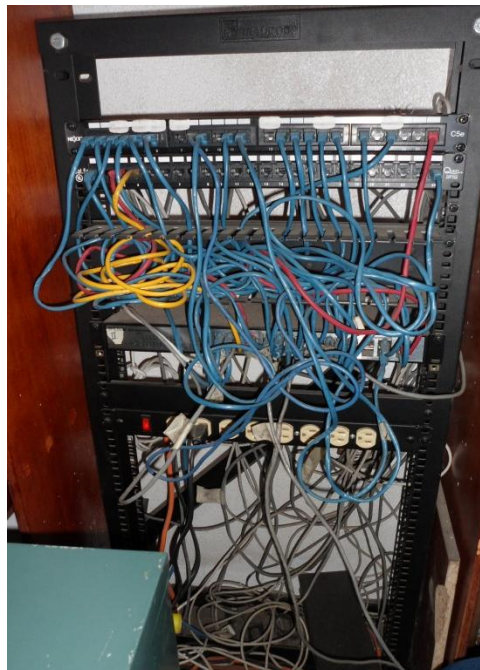
- **PRIMER PISO**

Rack Primer Piso - Proyectos



- **SEGUNDO PISO**

Rack Segundo Piso - Contabilidad

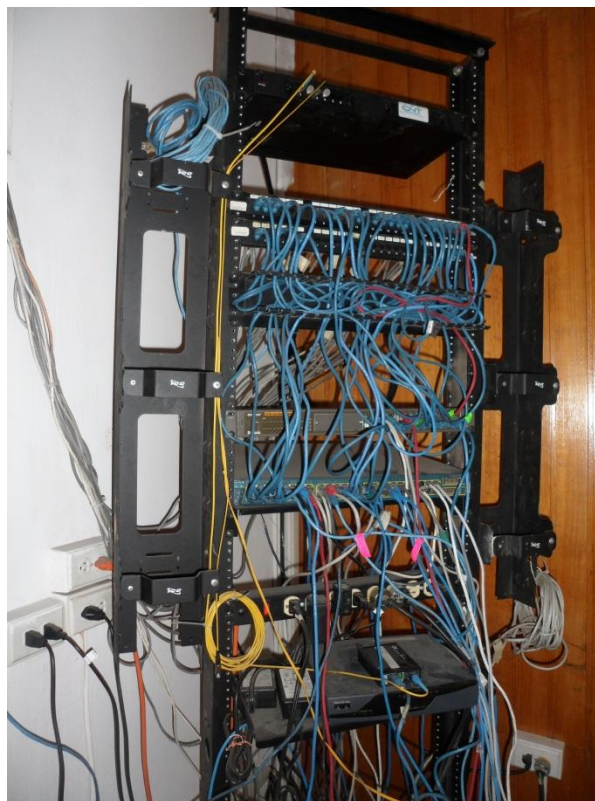


- **TERCER PISO**

Cuarto de Comunicaciones del GADMT



Rack Principal



Rack de extensiones telefónicas

