



ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERIA DE SISTEMAS

Carrera de Ingeniería Informática

TESIS

**“DISEÑO Y CONSTRUCCIÓN DE UN PROTOTIPO DE
MONITOREO Y SEGURIDAD BASADO EN CÁMARAS IP PARA
UNA INSTITUCIÓN EDUCATIVA MEDIA DE QUITO”.**

Autor: Terán Moreno Mibzar Antonio

mteran@hotmail.com

Director: Ing. Recalde Varela Pablo Marcel

pablo.recalde@gmail.com

DECLARACIÓN

Yo, Mibzar Antonio Terán Moreno, declaro que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se incluye en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondiente a este trabajo, según lo establecido por la ley de Propiedad Intelectual, por su Reglamento y la normatividad institucional vigente.

Mibzar Antonio Terán Moreno

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado en su totalidad por el señor Mibzar Antonio Terán Moreno bajo mi supervisión.

Ing. Pablo Recalde

DIRECTOR DEL PROYECTO

INDICE

CAPITULO1: SITUACION ACTUAL.....	1
1.1 ANTECEDENTES	1
1.2 SISTEMA DE CABLEADO ESTRUCTURADO.....	2
1.2.1 SUBSISTEMAS DE DISTRIBUCIÓN.....	3
1.2.2 SUBSISTEMA VERTICAL	8
1.2.3 SUBSISTEMA DE CABLEADO HORIZONTAL	10
1.3 EQUIPOS DE RED.....	11
1.3.1 EQUIPOS DE INTERCONECTIVIDAD	11
1.3.2 EQUIPOS DE USUARIO	13
1.4 DIRECCIONAMIENTO IP	18
1.4.1 CONFIGURACION DE RED DE LOS EQUIPOS.....	19
1.5 SOFTWARE	20
1.5.1 SOFTWARE DE RED	20
1.5.2 SOFTWARE ESTACIONES DE TRABAJO	26
1.6 SEGURIDAD.....	27

1.6.1 SEGURIDAD FÍSICA	27
1.6.2 SEGURIDAD LÓGICA	28
1.7 DIAGNÓSTICO.....	32
1.8 ANALISIS DE REQUERIMIENTOS.....	35
1.8.1 MONITOREO IP	36
1.8.2 HARDWARE Y SOFTWARE DE RED.....	39
1.8.3 MEDIOS DE ALMACENAMIENTO.....	44
1.8.4 FORMATOS DE COMPRESION DE VIDEO	47
1.8.5 TRANSPORTE DE PAQUETES DE VIDEO.....	50
1.8.6 DIGITALIZACION DE IMAGENES DE VIDEO.....	51
1.8.7 SEGMENTACION DE LA RED.....	55
1.8.8 USUARIOS DE MONITOREO	57
 CAPITULO 2: DISEÑO DEL MODELO DE MONITOREO Y	
SEGURIDAD.....	58
2.1 FACTORES DE SEGURIDAD	¡ERROR! MARCADOR NO
	DEFINIDO.
2.2 SEGURIDAD DE LOS BIENES MUEBLES.	61
2.2.1 SEGURIDAD DE LOS CASILLEROS	61
2.2.2 SEGURIDAD EN LOS LABORATORIOS DE CÓMPUTO.....	61

2.2.3 SEGURIDAD EN LAS OFICINAS.....	61
2.2.4 SEGURIDAD EN CAFETERIA.....	61
2.3 ANÁLISIS DE UBICACIÓN DE CÁMARAS.....	62
2.3.1 PREESCOLAR.....	64
2.3.2 ENTRADA - SALIDA DE BUSES.....	64
2.3.3 LABORATORIO CÓMPUTO.....	65
2.3.4 GARITA (ENTRADA PRINCIPAL).....	65
2.3.5 CAFETERÍA.....	65
2.3.6 CASILLEROS SECUNDARIA.....	65
2.3.7 PARQUEADERO DE ENTRADA.....	65
2.3.8 ADMINISTRACIÓN.....	66
2.3.9 ESTADIO.....	66
2.4 OBRA CIVIL.....	67
2.5 DISEÑO DE SEGMENTACION DE LA RED.....	69
2.5.1 DISEÑO Y OBJETIVOS DE LA ARQUITECTURA DE RED.....	69
2.5.2 SEGMENTACIÓN.....	73
2.5.3 CONFIGURACIÓN DE LAS VLANS.....	74
2.6 TECNOLOGIAS DE TRANSPORTE DE VIDEO.....	79
2.7 ADMINISTRACION DE ALERTAS DE MONITOREO.....	87

2.8 USUARIOS DE MONITOREO	87
2.8.1 Seguridad	88
2.8.2 JEFE DE SEGURIDAD Y GERENCIA.....	88
2.8.3 Inspección general.....	88
 2.9 FORMAS DE ALMACENAMIENTO DE LOS EVENTOS	
MONITOREADOS	89
2.10 POLITICAS DE BACKUP	90
CAPITULO 3: IMPLEMENTACION DEL PROTOTIPO.....	91
3.1 ANALISIS DE COSTOS.....	91
3.2 ANALISIS TECNICO Y DE FACTIBILIDAD.....	94
3.2.1 ANALISIS TECNICO	94
3.2.3 SELECCION DE CAMARAS IP.	95
3.2.4 SELECCIÓN DEL SOFTWARE DE MONITOREO	95
3.3 ANALISIS LEGAL	96
3.4 IMPLANTACION DEL PROTOTIPO.	97
3.4.1 INSTALCIÓN DE CAMARAS	97
3.4.2 INSTALACION DEL SERVIDOR DE CAMARAS.....	98
3.4.3 INSTALACION DE SOFTWARE DE CAMARAS.....	98

3.4.4 INSTALACION DEL SOFTWARE DE MONITOREO	99
GRÁFICO 3.11 PANTALLA DE CREACIÓN VISTA DE CÁMARAS	107
3.4.6 CONFIGURACION DEL ACCESO REMOTO.....	109
3.4.7 PRUEBAS DE MONITOREO	109
CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES	111
4.1 CONCLUSIONES.....	111
4.2 RECOMENDACIONES	112
ANEXOS.....	113
ANEXO 1 DETALLE DE USUARIOS DE LA RED DE LA INSTITUCIÓN	113
ANEXO 2. DETALLE DE ESTACIONES DE TRABAJO	115
ANEXO 3. DIRECCIONAMIENTO IP	118
ANEXO 4. CARACTERISTICAS DE LOS SWITCH 3COM.....	123
<i>MDF: Laboratorios.....</i>	<i>125</i>
<i>IDF: Inspección General.....</i>	<i>127</i>
<i>SDF 1: Primaria 1.....</i>	<i>128</i>
<i>SDF 2: Biblioteca.....</i>	<i>128</i>
<i>SDF 3: Administración.....</i>	<i>129</i>
<i>SDF 4: Secundaria.....</i>	<i>130</i>
<i>SDF 5: Preescolar.....</i>	<i>131</i>

Índice de gráficos

<i>Gráfico 1.1: Ubicación de los subsistemas de administración del campus</i>	5
<i>Gráfico 1.2 de estructura general de la red</i>	8
<i>Gráfico 1.3: Esquema del subsistema de cableado vertical</i>	9
<i>Gráfico 1.4: Distribución de los elementos de interconectividad</i>	14
<i>Gráfico 1.5: Módulos del sistema académico</i>	25
<i>Gráfico 1.6 Seguridad de red con Firewall</i>	30
<i>Gráfico 1.7 Video Analógico CCTV</i>	36
<i>Gráfico 1.8 Video IP Digital CCTV</i>	38
<i>Grafico 1.9 técnicas de compresión de video</i>	50
<i>Gráfico 1.10 de transporte de video</i>	52
<i>Grafico 2.1 Ubicación de cámaras</i>	¡Error! Marcador no definido.
<i>Grafico 2.1 Ubicación de cámaras</i>	63
<i>Gráfico 2.2 Cámara Preescolar (referencia)</i>	64
<i>Gráfico 2.4 de ubicación cámara para la zona entrada de buses</i>	69
<i>GRAFICO 2.7 CREACION DE VLAN</i>	72
<i>GRAFICO 2.8 Transporte de video</i>	80
<i>Grafico 2.9 Transmisión TCP</i>	83
<i>GRAFICO 2.10 USUARIOS DEL SISTEMA</i>	88
<i>Gráfico 3.1 Ubicación cámara parqueadero</i>	97
<i>Gráfico 3.2 configuración cámaras Axis</i>	99

<i>Gráfico 3.3 Pantalla Principal instalación software de monitoreo</i>	99
<i>Gráfico 3.4 Instalación del Software de monitoreo D3Data NETVM</i>	100
<i>Gráfico 3.5 Pantalla de opciones de configuración D3Data NETVM</i>	101
<i>Gráfico 3.6 Pantalla para añadir las cámaras al software de monitoreo</i>	102
<i>Gráfico 3.7 número de cámaras totales configuradas</i>	103
<i>Gráfico 3.8 Pantalla creación de usuarios y permisos de acceso</i>	104
<i>Gráfico 3.9 Pantalla para creación de grupos de usuarios</i>	105
<i>Gráfico 3.10 Pantalla autenticación para el ingreso al sistema de cámaras</i>	106
<i>Gráfico 3.11 Pantalla de creación vista de cámaras</i>	107
<i>Gráfico 3.12 DIRECTORIO D:\GRABACION\CAMARA1</i>	108
<i>Gráfico 3.13 Pantalla de visualización de cámaras</i>	110

Índice de tablas

<i>Tabla 1.1 características de la fibra óptica utilizada</i>	9
<i>Tabla 1.2: Longitud de los enlaces de fibra</i>	10
<i>Tabla 1.3: Resumen de número de enlaces por bloque</i>	11
<i>Tabla 1.4 Equipos de Interconectividad</i>	11
<i>Tabla 1.5: Roles de los servidores</i>	13
<i>Tabla 1.6: Resumen características de las estaciones de trabajo</i>	15
<i>Tabla 1.7: Estaciones de trabajo por ambiente</i>	16
<i>Tabla 1.8: Lista de impresoras</i>	17

<i>Tabla 1.9 Otros dispositivos en la red.....</i>	<i>18</i>
<i>Tabla 1.10 Rangos IP.....</i>	<i>19</i>
<i>Tabla 1.11 configuración IP.....</i>	<i>19</i>
<i>Tabla 1.12: Resumen de sistemas operativos instalados.....</i>	<i>23</i>
<i>Tabla 1.13: Servicios configurados en el Firewall.....</i>	<i>31</i>
<i>Tabla 1.14: Políticas de acceso a los servicios del Firewall.....</i>	<i>31</i>
<i>Tabla 1.15: Porcentaje de disponibilidad de los elementos activos.....</i>	<i>33</i>
<i>TABLA 2.1 UBICACIONDE CAMARAS (REFERENCIA).....</i>	<i>62</i>
<i>TABLA 2.2 HORARIO DE GRABACION DE CAMARAS.....</i>	<i>89</i>
<i>Tabla 3.1 Cotizaciones Cámaras.....</i>	<i>91</i>
<i>Tabla 3.2 Cotizaciones Cámaras Axis.....</i>	<i>91</i>
<i>Tabla A1.1: Número de estudiantes por grado / paralelo.....</i>	<i>113</i>
<i>Tabla A1.2: Distribución personal docente por departamento o área.....</i>	<i>113</i>
<i>Tabla A1.3: Distribución del personal administrativo.....</i>	<i>114</i>
<i>Tabla A3.1 Distribución de direcciones IP.....</i>	<i>118</i>
<i>Tabla 2.5: Detalle de enlaces edificio Laboratorios.....</i>	<i>125</i>
<i>Tabla 2.6: Detalle de enlaces edificio Inspección General.....</i>	<i>127</i>
<i>Tabla 2.7: Detalle de enlaces edificio Oficinas Departamentos.....</i>	<i>127</i>
<i>Tabla 2.8: Detalle de enlaces edificios Primaria 1, Primaria 2 y Cafetería.....</i>	<i>128</i>
<i>Tabla 2.9: Detalle de enlaces edificio Biblioteca.....</i>	<i>128</i>
<i>Tabla 2.10: Detalle de enlaces edificio Administración.....</i>	<i>129</i>

Tabla 2.11: Detalle de enlaces edificio Administración 130

Tabla 2.12: Detalle de enlaces edificio Laboratorio Preescolar 131

CAPITULO1: SITUACION ACTUAL

1.1 ANTECEDENTES

El acelerado avance de la informática, las telecomunicaciones, las redes electrónicas y las tecnologías de multimedia han tenido un fuerte impacto en toda la actividad humana y la necesidad automatizar procesos que se desarrollan manualmente y buscar nuevas alternativas aplicables al medio, en base a estas necesidades se plantea este tema para la presente investigación

Para el desarrollo del proyecto se tomará como modelo de trabajo la situación de una institución educativa privada de Quito. Esta institución como otras en su medio desde hace algún tiempo han adoptado a la tecnología de las redes de información y la computación como una herramienta de apoyo al proceso pedagógico y administrativo. Para cumplir con este objetivo los administradores de la institución han tenido que realizar grandes inversiones llegando a formar una gran infraestructura al servicio de los distintos miembros que componen la comunidad.

El proceso hasta llegar a tener la infraestructura que hoy en día posee la institución ha tomado varios años. En cada año se ejecutaron proyectos cada uno de los cuales constituyeron una etapa en la que se incorporaron nuevos elementos a la infraestructura montada; dicho proceso empezó a finales de los años ochenta en los que se adquirió algunas computadoras para cumplir tareas específicas y siguió a un ritmo creciente más o menos continuo hasta llegar a estos días en que se cuenta con una red de datos con una variedad de servicios como Internet, correo electrónico, sistema de calificaciones, etc. que están disponibles para los usuarios. La misión es continuar con este proceso proponiendo nuevas alternativas que se ajusten a las necesidades de la institución.

Cabe decir que el tema planteado se constituye en una de esas alternativas, pero antes de entrar en la esencia del mismo es recomendable hacer una revisión de la

situación actual de la red de datos de la institución y realizar un diagnóstico de la misma.

La revisión de la situación actual empezará con una descripción de la distribución de las instalaciones de la institución, continuará con una descripción de cada uno de los elementos que componen el sistema de cableado estructurado existente actualmente. Otra faceta del análisis será la descripción de los elementos activos que interconectan este sistema y los distintos dispositivos de usuario conectados a la red (servidores, estaciones de trabajo, impresoras, etc.) así como los servicios y aplicaciones disponibles para los usuarios. Posteriormente se hará un análisis del tráfico de la red y los esquemas de seguridad existentes en la misma. Finalmente se realizará el diagnóstico de la situación encontrada.

1.2 SISTEMA DE CABLEADO ESTRUCTURADO

Al instalar cableado en una red de datos mediante uso estándares o normas como EIA/TIA 568 A ó B es hablar de los conectores RJ45 y de las diversas categorías del cable UTP con sus respectivos códigos de colores, la norma 568A comienza con el color blanco-verde, mientras que la norma 568B con el blanco-naranja, tal como se describe a continuación:

Norma EIA/TIA 568 A

PIN	COLOR HILO
1	Blanco - Verde
2	Verde
3	Blanco - Naranja
4	Azul
5	Blanco - Azul
6	Naranja
7	Blanco - Café
8	Café

Norma EIA/TIA 568 B

PIN	COLOR HILO
1	Blanco - Naranja
2	Naranja
3	Blanco - Verde
4	Azul
5	Blanco - Azul
6	Verde
7	Blanco - Café
8	Café

El cableado estructurado existente está construido según la norma EIA/TIA 568 B, de cableado estructurado corresponde a la categoría 5e del cable UTP y de acuerdo a la misma norma tiene una topología en estrella.

En forma resumida, el sistema de cableado estructurado de datos de la institución está configurado de la siguiente forma:

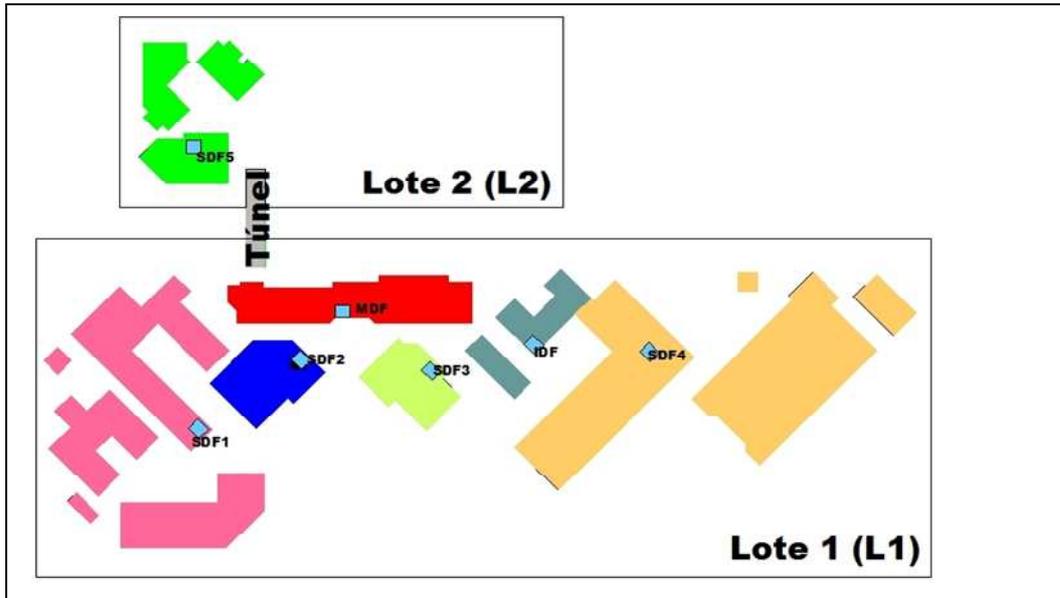
En la sala de servidores del edificio Laboratorios está el cuarto principal de comunicaciones denominado MDF¹ (bloque principal de fibra óptica), el MDF está interconectado por medio de fibra óptica a cinco cuartos secundarios denominados SDF (bloque secundario de fibra óptica) ubicados en los edificios de Primaria 1, Biblioteca, Administración, Inspección General y Preescolar. El SDF de Inspección General es a su vez un cuarto intermedio que sirve para enlazar también por medio de fibra óptica al SDF que existe en el edificio Secundaria, en el gráfico 1.1 se puede observar esta distribución. Finalmente, cada puesto de trabajo en las aulas y oficinas están enlazadas a los cuartos de distribución mediante cable UTP categoría 5e.

¹ Bloque principal de fibra óptica, el centro de cómputo es el bloque principal.

1.2.1 SUBSISTEMAS DE DISTRIBUCIÓN SDF²

En el gráfico 1.1 se muestra la ubicación de los cuartos de distribución existentes en el campus, estos se mencionan a continuación:

Gráfico 1.1: Ubicación de los subsistemas de administración del campus



Subsistema de distribución Principal (MDF: Laboratorios)

Está ubicado en la sala de servidores de edificio Laboratorios, es el punto de distribución de los enlaces de red del edificio Laboratorios y además es el punto central de interconexión del resto de subsistemas de distribución del campus de la institución.

Tiene los siguientes elementos:

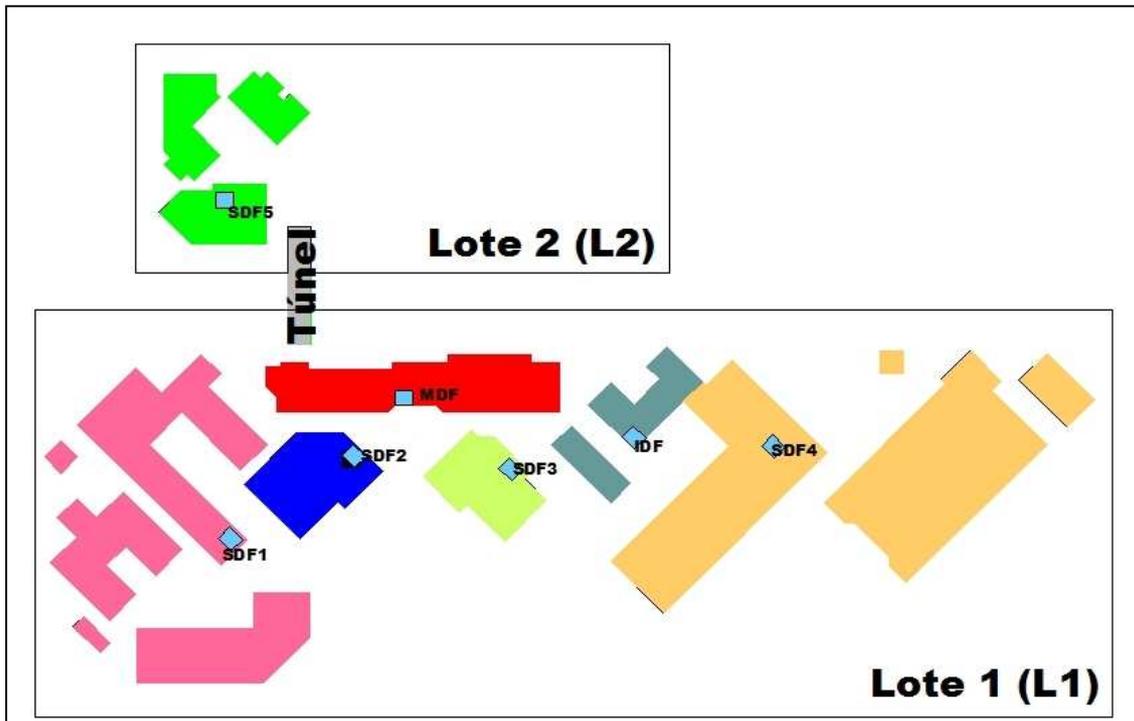
- Un Rack abierto de piso de 42U EIA
- Un Patch panel para conexión de fibra óptica con 28 puertos
- Un Patch panel R&M de 56 puertos categoría 5e
- Una Bandeja tomacorriente de 6 puertos

² Denominación para representar bloques secundarios de fibra óptica.

1.2.1 SUBSISTEMAS DE DISTRIBUCIÓN SDF

En el gráfico 1.1 se muestra la ubicación de los cuartos de distribución existentes en el campus, estos se mencionan a continuación:

Gráfico 1.1: Ubicación de los subsistemas de administración del campus



Subsistema de distribución Principal (MDF: Laboratorios)

Está ubicado en la sala de servidores de edificio Laboratorios, es el punto de distribución de los enlaces de red del edificio Laboratorios y además es el punto central de interconexión del resto de subsistemas de distribución del campus de la institución. Tiene los siguientes elementos:

- Un Rack abierto de piso de 42U EIA
- Un Patch panel para conexión de fibra óptica con 28 puertos
- Un Patch panel R&M de 56 puertos categoría 5e
- Una Bandeja tomacorriente de 6 puertos

Subsistema de distribución intermedio (IDF: Inspección General)

Está ubicado en la oficina de Inspección General en el edificio del mismo nombre. Es el punto de distribución de este edificio y del edificio Oficinas de Departamentos, además es el punto de interconexión intermedio entre el cuarto de distribución principal y el cuarto de distribución secundario de Secundaria. Está compuesto de los siguientes elementos:

- Rack pletina de pared
- Un Patch panel para conexión de fibra óptica con 8 puertos
- Un Patch panel R&M de 24 puertos categoría 5e
- Un Organizador de cable horizontal

Subsistema de distribución secundario (SDF1: Primaria 1)

Está ubicado en la oficina de Subinspección en el edificio Primaria 1. Es el punto de distribución de los edificios Primaria 1, Recursos de Psicopedagogía y Cafetería. Está compuesto de los siguientes elementos:

- Rack pletina de pared
- Un Patch panel para conexión de fibra óptica con 4 puertos
- Un Patch panel R&M de 24 puertos categoría 5e
- Un Organizador de cable horizontal

Subsistema de distribución secundario (SDF2: Biblioteca)

Está ubicado en la en la sala de lectura del edificio Biblioteca, este subsistema distribuye exclusivamente a este edificio y está compuesto de los siguientes elementos:

- Rack pletina de pared
- Un Patch panel para conexión de fibra óptica con 4 puertos
- Un Patch panel R&M de 24 puertos categoría 5e
- Un Organizador de cable horizontal

Subsistema de distribución secundario (SDF3: Administración)

Está ubicado junto al ambiente de cafetería del edificio Administración, es el punto de distribución de todo este edificio. Está compuesto de los siguientes elementos:

- Rack pletina de pared
- Un Patch panel para conexión de fibra óptica con 4 puertos
- Un Patch panel R&M de 24 puertos categoría 5e
- Un Organizador de cable horizontal

Subsistema de distribución secundario (SDF4: Secundaria)

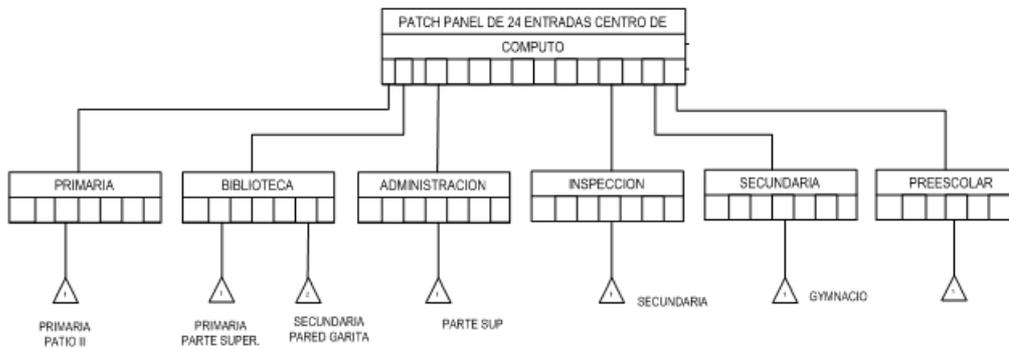
Está ubicado en la sala de reuniones de vicerrectorado en el segundo piso del edificio Secundaria. Este subsistema sirve de punto de distribución de los edificios Secundaria y Gimnasio, tiene los siguientes elementos:

- Rack pletina de pared
- Un Patch panel para conexión de fibra óptica con 4 puertos
- Un Patch panel R&M de 24 puertos categoría 5e
- Un Organizador de cable horizontal

Subsistema de distribución secundario (SDF5: Preescolar)

Está ubicado en el laboratorio de computadores del edificio Laboratorio Preescolar, sirve de punto de distribución de este edificio y tiene los siguientes elementos:

- Rack pletina de pared
- Un Patch panel para conexión de fibra óptica con 4 puertos
- Un Patch panel R&M de 24 puertos categoría 5e
- Un Organizador de cable horizontal

Gráfico 1.2 de estructura general de la red

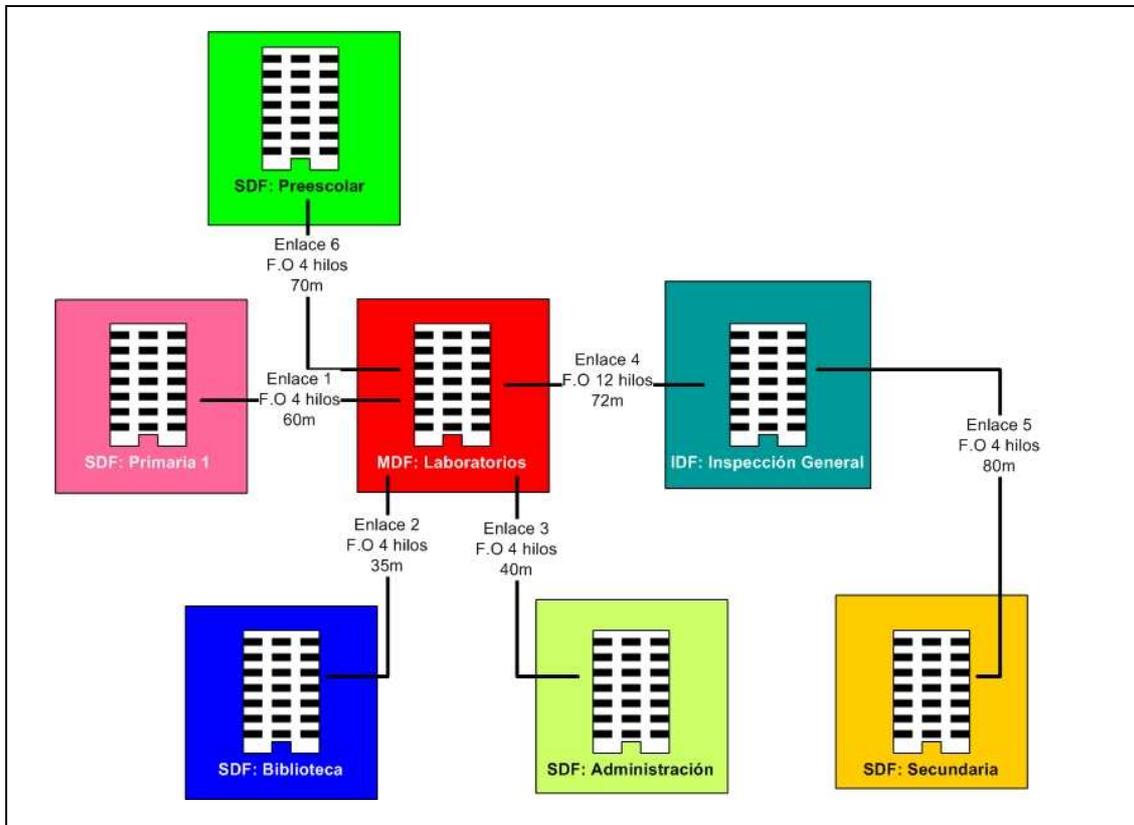
1.2.2 SUBSISTEMA VERTICAL

El subsistema vertical o backbone es el medio de interconexión entre el sistema de administración principal (MDF) y cada uno de los subsistemas de administración secundarios (SDF), en el gráfico 1.3 se muestra un esquema de este subsistema en el campus de la institución.

El punto central de este subsistema está en la sala de servidores del edificio Laboratorios, a partir de este lugar se extiende la fibra óptica a los distintos cuartos de distribución de la siguiente manera:

1. Laboratorios – Primaria 1
2. Laboratorios – Biblioteca
3. Laboratorios – Administración
4. Laboratorios – Inspección General
5. Inspección General – Secundaria
6. Laboratorios – Preescolar

Gráfico 1.3: Esquema del subsistema de cableado vertical



El medio de transmisión utilizado para unir estos enlaces es la fibra óptica.

Características Técnicas de la Fibra óptica

Tabla 1.1 características de la fibra óptica utilizada

Diámetro de la Cubierta	125 micras
Diámetro Interior	62,5 micras
Tipo de Fibra	Multimodo
Resistencia al Quiebre	750 μ /cm
Atenuación Máxima	5 dB/Km
Mínimo Ancho de Banda	160 Mhz/Km

Tabla 1.2: Longitud de los enlaces de fibra

#	Enlace	# Pares	Longitud (metros)
1	Laboratorios – Primaria 1	4	60
2	Laboratorios – Biblioteca	4	35
3	Laboratorios – Administración	4	40
4	Laboratorios – Inspección General	12	72
5	Inspección General – Secundaria	4	80
6	Laboratorios – Preescolar	4	70

Los enlaces de fibra óptica definidos se extienden a través del campus por dentro de ductos que tienen las siguientes características:

Tubería a base de manguera de 2" de diámetro enterrada a 80cm de profundidad

Cajas de revisión de ladrillo de 40cm x 40cm, existe una caja de revisión cada 20m entre el MDF y el SDF

1.2.3 SUBSISTEMA DE CABLEADO HORIZONTAL

El subsistema de cableado horizontal está compuesto de cable UTP categoría 5e y parte de cada uno de los subsistemas de distribución hacia las áreas de trabajo más próximas. Categoría 5e es un estándar dentro de las comunicaciones en redes LAN. Es capaz de soportar comunicaciones de hasta 100 Mbps. con un ancho de banda de hasta 100 Mhz. Este tipo de cable es de 8 hilos, es decir cuatro pares trenzados. La atenuación del cable de esta categoría esta referida a una distancia estándar de 100 metros.

Comparado a otros medios de transmisión guiados el par trenzado está limitado en distancia, ancho de banda y data rate, además la atenuación es una función fuertemente dependiente de la frecuencia. La interferencia y el ruido externo también son factores importantes a tomar en cuenta, para ello se usan las

coberturas externas y el trenzado. Para señales analógicas se requieren amplificadores cada 5 o 6 km. Para señales digitales se requieren repetidores cada 2 o 3 km.

En la tabla 1.3 se muestra un resumen del número de enlaces por cada subsistema de administración.

Tabla 1.3: Resumen de número de enlaces por bloque

#	MDF /SDF	Número de enlaces
1	Laboratorios	49
2	Primaria	7
3	Biblioteca	8
4	Administración	21
5	Inspección General	16
6	Secundaria	13
7	Preescolar	16

1.3 EQUIPOS DE RED

1.3.1 EQUIPOS DE INTERCONECTIVIDAD

En la tabla 1.4 se resume los elementos de interconectividad que forman parte de la red de datos de la institución.

Tabla 1.4 Equipos de Interconectividad

RACK	SWITCH 24 PUERTOS 3COM	CONVERTID OR D-Link
Administración	SuperStack® II Baseline 10/100	1 DFE-855
Biblioteca	SuperStack® II Baseline 10/100	1 DFE-855
Inspección	SuperStack® II Baseline	1 DFE-855

Primaria	10/100	
Inspección General	SuperStack® II Baseline 10/100	1 DFE-855
Preescolar	SuperStack® II Baseline 10/100	1 DFE-855
Secundaria	SuperStack® II Baseline 10/100	1 DFE-855
Ubicación	Descripción	Cantidad
Sala de servidores	Switch 3Com SuperStack® II Baseline 10/100 24 puertos	3
	Switch 3Com SuperStack® III 4500 26 puertos	1
	CONVERTIDOR D-Link 1 DFE-855	6
	Firewall 3Com Superstack 3, puertos LAN, DMZ y WAN, modelo 3CR164110-97	1
Primaria	Switch 3Com SuperStack® III Baseline 10/100 24 puertos	1
	CONVERTIDOR D-Link 1 DFE-855	1
Biblioteca	Switch 3Com SuperStack® III Baseline 10/100 24 puertos	1
	CONVERTIDOR D-Link 1 DFE-855	1
Administración	Switch 3Com SuperStack® III Baseline 10/100 24 puertos	1
	Switch 3Com SuperStack® III 4500 26 puertos	1
	CONVERTIDOR D-Link 1 DFE-855	1
Inspección general	Switch 3Com SuperStack® III Baseline 10/100 24 puertos	1
	CONVERTIDOR D-Link 1 DFE-855	1
Secundaria	Switch 3Com SuperStack® III Baseline 10/100 24 puertos	1
	CONVERTIDOR D-Link 1 DFE-855	1
Gimnasio	Switch 3Com SuperStack® III 4500 26 puertos	1
Preescolar	Switch 3Com SuperStack® III Baseline 10/100 24 puertos	1

En el anexo 4. Se puede encontrar las características de los elementos anteriormente citados.

El gráfico 1.4 muestra físicamente la ubicación de estos dispositivos en los distintos edificios del campus de la institución.

1.3.2 EQUIPOS DE USUARIO

Servidores

Existen ocho equipos que cumplen la tarea de servidor y tienen las siguientes características:

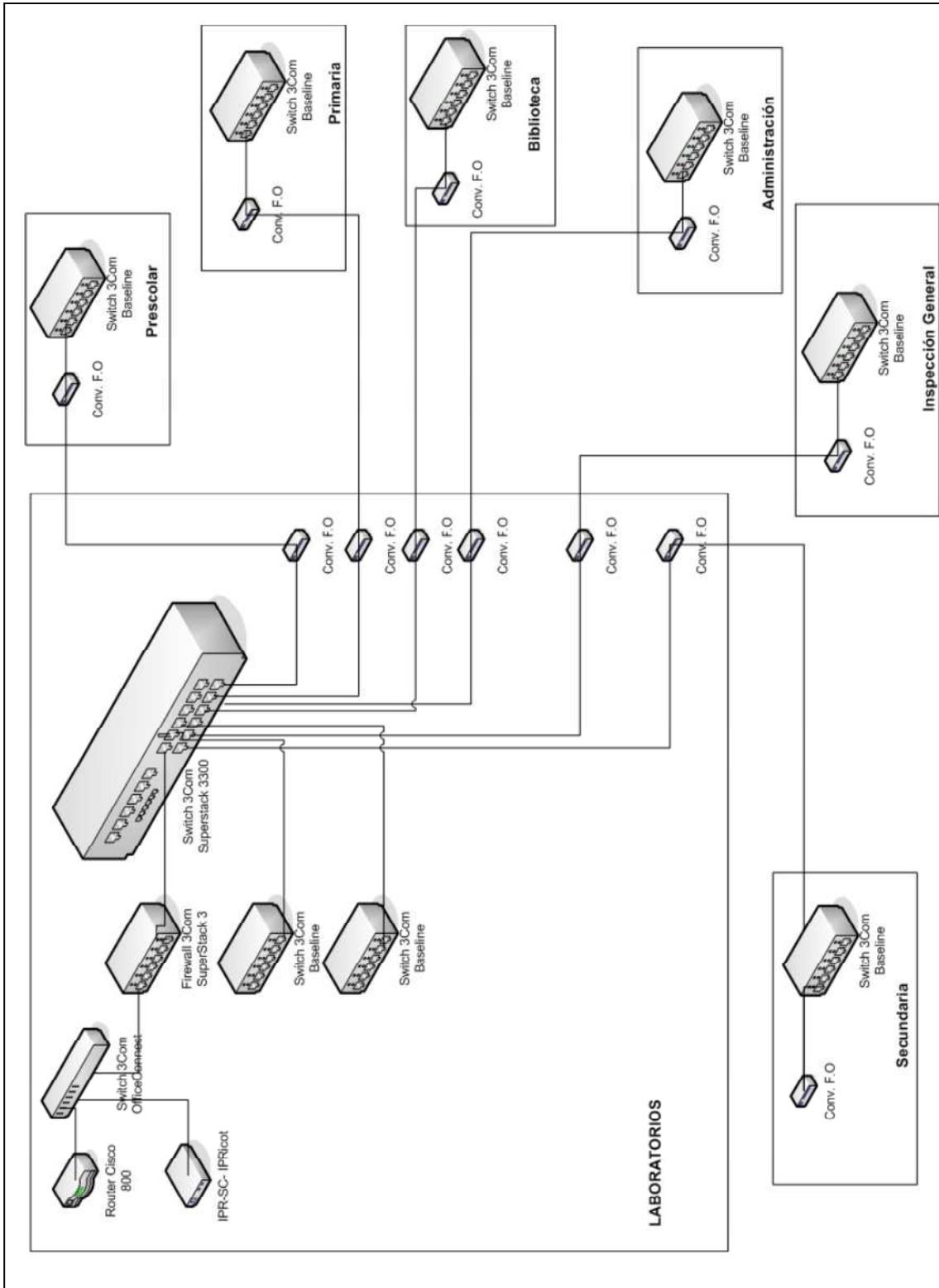
- Tarjeta madre Intel modelo 875
- Procesador Pentium IV 3.1 Ghz
- Memoria RAM 1GB
- Dos discos duros 120GB
- Unidad de CD 52x y CD Writer
- Unidad de disquetes
- Tarjeta de red incorporada 10/100 Mbps

Estos equipos cumplen distintos roles que se describen en la tabla 1.5

Tabla 1.5: Roles de los servidores

Servidor	Rol o servicio
PC Clon Intel 1	Directorio activo principal y DHCP
PC Clon Intel 2	Correo electrónico, directorio activo secundario
PC Clon Intel 3	Archivos profesores
PC Clon Intel 4	Archivos estudiantes
PC Clon Intel 5	Proxy
PC Clon Intel 6	Aplicaciones
PC Clon Intel 7	Base de datos
PC Clon Intel 8	Aplicaciones, archivos

Gráfico 1.4: Distribución de los elementos de interconectividad



ESTACIONES DE TRABAJO

Existen 100 estaciones de trabajo distribuidas en oficinas y laboratorios, todas conectadas a la red de la institución. En cuanto a los equipos no todos estos tienen las mismas características, en la tabla 1.6 se describe las características de las estaciones de trabajo en funcionamiento.

En la tabla 1.7 se muestra un resumen de las estaciones de trabajo que existen en los distintos ambientes del campus, el detalle de la distribución de las estaciones de trabajo se muestra en el anexo 2.1

Tabla 1.6: Resumen características de las estaciones de trabajo

Equipo	Característica	Cantidad
Clon 2	Procesador Pentium III 800 Mhz, RAM 128MB, Disco Duro 20GB	10
Clon INTEL 1	Procesador Pentium IV 1.6 Ghz, RAM 256MB, Disco Duro 80GB	16
Clon INTEL 2	Procesador Pentium IV 1.8 Ghz, RAM 256MB, Disco Duro 80GB	10
Clon INTEL 3	Procesador Pentium IV 2.4 Ghz, RAM 512MB, Disco Duro 80GB	30
Clon INTEL 4	Procesador Pentium IV 2.8 Ghz, RAM 512MB, Disco Duro 80GB	18
IMac G3	Procesador G3 233Mhz, RAM 160MB, Disco Duro 4GB	10
Power PC	Procesador G3 300Mhz, RAM 256MB, Disco Duro 8GB	01
Power PC	Procesador G4 1Ghz, RAM 512MB, Disco Duro 40GB	01
Compaq Armada 1500c	Procesador INTEL Celeron 350 Mhz. RAM 64MB, Disco Duro 4GB	01

Tabla 1.7: Estaciones de trabajo por ambiente	
Ubicación - Ambiente	#
Arte	2
Asesoría Universitaria	1
Asistente Contabilidad	1
Biblioteca	3
Centro de cómputo	6
Ciencias Experimentales	2
Ciencias Sociales	2
Colecturía	1
Contabilidad	2
Coordinación BI	1
Dep. Cultura Física	2
Experimentación	1
Garita	1
Gerencia	1
Hebreo	2
Idiomas	3
Inspección General	2
Lab Biología	1
Lab CCNN	1
Lab Física	1
Lab Química	1
Laboratorio Génesis	14
Laboratorio PC2	14
Laboratorio Preescolar	12
Letras	3
Mantenimiento	2
Multimedia	1
Oficina de Suministros	2
Oficina Preescolar	1

Psicología	2
Recepción	1
Rectorado	1
Recuperación. Psicopedagógica	1
Relaciones Públicas	1
Secretaria Académica	1
Secretaria Gerencia	1
Secretaria Rectorado	1
Secretaría Vicerrectorado	1
Seguridad	1
Subinspección General	2
Vicerrectorado	1

IMPRESORAS

Se dispone de diez impresoras láser de red que se conectan a la red utilizando una dirección IP. Existe al menos una impresora en cada zona del campus, adicionalmente se dispone de tres impresoras láser compartidas en las zonas de biblioteca y preescolar y una impresora de inyección de tinta en el departamento de diseño gráfico, la tabla 1.8 es un resumen de las impresoras que existen en la institución.

Tabla 1.8: Lista de impresoras		
Impresora	Cantidad	Tipo
HP Láser 1000	2	Compartida
HP Láser 1100	1	Compartida
HP Láser Jet 1200n	2	Red
HP Láser Jet 1300n	4	Red
HP Láser Jet 2300dn	1	Red
HP Láser Color Jet 2500	1	Red
Xerox Work Centre 315 /320	1	Red
Xerox Document Centre 332/340	1	Red

Tabla 1.8: Lista de impresoras		
Impresora	Cantidad	Tipo
HP DeskJet 1220c	1	Compartida

OTROS DISPOSITIVOS

Existen además otros dispositivos o equipos que no se conectan a la red pero sirven como herramientas para el desempeño diario de los usuarios, estos dispositivos se resumen en la tabla 1.9.

Tabla 1.9 Otros dispositivos en la red

Dispositivo	Descripción	Cantidad
HP Desk Writer	Dispositivo de grabación de CD	1
HP Scanner 1200	Escáner	4
HP Scanner	Escáner	1
IOmega Jazz	Dispositivo de respaldo de información	1

1.4 DIRECCIONAMIENTO IP

La red de datos de la Institución está configurada como una red tipo C. Esta clase de red permite cerca de 2 millones de redes con más de 254 estaciones de trabajo por cada subred, cada estación de trabajo en la configuración de red está compuesta por el número IP y la máscara de red 255.255.255.0 que permite a un computador determinar si un datagrama de salida va destinado dentro de la misma red ó a otra diferente para lo cual utiliza un encaminador.

De acuerdo a las características de la red tipo C configurada e instalada en la Institución, la asignación de direcciones IP para el caso de direcciones dinámicas utiliza DHCP y para el caso de direcciones estáticas configuradas en estaciones de trabajo, impresoras, cámaras y servidores se detalla en la tabla 1.10.

DHCP (*Dynamic Host Configuration Protocol*) configurado en el servidor Bdcnorton para asignar direcciones IP dinámicas, este método permite la reutilización de direcciones IP. El rango de direcciones IP para el DHCP van desde 192.168.0.81 hasta la 192.168.0.200 y cada ordenador cliente de la LAN tiene su software de comunicación TCP/IP configurado para solicitar una dirección IP del servidor DHCP cuando su tarjeta de interfaz de red se inicie.

IP Estáticas, configurado manualmente de acuerdo a las necesidades de utilización de direcciones IP.

Tabla 1.10 Rangos IP.

SECCION	DESDE	HASTA
Red tipo C	192.0.0.0	223.255.255.0
Servidores	192.168.0.1	192.168.0.25
Impresoras de red	192.168.0.26	192.168.0.40
Direcciones Libres	192.168.0.41	192.168.0.80
DHCP	192.168.0.81	192.168.0.200
Cámaras IP	192.168.0.201	192.168.0.230
Laboratorio MAC	192.168.0.231	192.168.0.254

1.4.1 CONFIGURACION DE RED DE LOS EQUIPOS

Cada estación de trabajo tiene configurada una dirección IP sea esta dinámica o fija con su máscara de red respectiva como se indica en la tabla 1.18

Tabla 1.11 configuración IP

CONFIGURACION IP	LOCAL	PUBLICA
DIRECCION IP (FIJA, DINAMICA)	192.168.0.0	200.63.215.88
MASCARA DE RED	255.255.255.0	255.255.255.248
PUERTA DE ENLACE	192.168.0.1	248.63.215.89
DNS PRIMARIO	192.168.0.11	200.63.212.1
DNS SECUNDARIO		200.63.192.1

Además se cuenta con dos direcciones públicas adicionales que por el momento no están siendo utilizadas.

1.5 SOFTWARE

1.5.1 SOFTWARE DE RED

Los sistemas operativos instalados en los servidores y estaciones de trabajo son los siguientes:

- Servidores: Microsoft Windows 2003 Server Estándar
- Estaciones de trabajo: Microsoft Windows XP y Mac OS 9

En la tabla 1.12 se muestra un resumen del número de licencias existentes de cada sistema operativo.

El sistema operativo de red instalado en todos los servidores es Windows 2003 Server, el servidor principal tiene configurado los siguientes servicios:

- Active Directory con todas las cuentas y passwords de usuarios
- Catalogo Global
- Dns
- Controlador Primario de Dominio
- Servidor de Replica

El servidor de Exchange trabaja conjuntamente con el Active Directory y el Dns del servidor principal, está instalado y configurado Exchange 2003 Server, en este servidor están creadas todas las cuentas de email de todo el personal y estudiantes tanto para envío interno como externo, además este servidor está configurado como el segundo controlador de dominio.

En el servidor de archivos de estudiantes y de profesores están configuradas las carpetas de red con su respectiva identidad de cada uno de los usuarios con respectivos permisos y accesos.

Servidor de Aplicaciones está instalado el software Micro Isis para el sistema de catalogación y prestamos de libros de la biblioteca, a demás el software Tmax para el sistema contable en la parte administrativa y por último se tiene el sistema de matriculas y calificaciones de los estudiantes desarrollado en Microsoft Access como Front end y Microsoft SQL Server como Back end.

SERVICIO DE IMPRESIÓN

El servicio de impresión de la institución está disponible para todos los usuarios de la red, el derecho a uso de las impresoras se da tomando en cuenta el tipo de usuario y su ubicación habitual en el campus. Así por ejemplo los usuarios estudiantes solo tienen derecho a usar las impresoras ubicadas en laboratorios y biblioteca, los profesores acceden a las impresoras próximas a su oficina departamental, laboratorios y biblioteca; mientras que el personal administrativo normalmente pueden imprimir en las impresoras próximas a su puesto de trabajo con algunas excepciones que adicionalmente tienen derecho de impresión en las impresoras de los Laboratorios y Biblioteca.

Los usuarios que acceden a las impresoras de Laboratorios, Biblioteca, Inspección General y Primaria tienen asignadas cuotas de impresión, el programa que administra estas cuotas se llama Print Manager Plus Edición Estándar Versión 5.0.0.34; los profesores y personal administrativo tiene una cuota de impresión de 100 hojas semanales, mientras que los estudiantes tienen una cuota de 30 hojas semanales. El resto de impresoras están restringidas a usuarios que están más próximos a la zona en la cual está instalado dicho dispositivo.

Adicionalmente en cada uno de estos servidores está configurado el Software de impresión Print Manager Plus sirve específicamente para controlador el volumen de impresión de los usuarios por medio de cuotas que se puede establecer un número fijo por semana ó mensualmente, también ofrece características de habilitar o deshabilitar la impresión de un documento de acuerdo al tipo de archivo por su extensión o tamaño, también se puede habilitar a un usuario para impresión a color.

ISA SERVER. Servicio de Internet

La institución tiene contratado un enlace dedicado para proveer el servicio de Internet con la empresa Megadatos. Las características del servicio son las siguientes:

DownLink: Servicio de Internet Premium TX 128K / RX 128K CIR 384 BURST (IPBroadcast)

UpLink: Última milla 128K (ADSL)

Para distribuir este servicio en la red interna se tiene configurado un equipo en el que está instalado ISA Server 2000 Estándar, programa que hace las veces de filtro de seguridad, servidor Proxy y servidor de caché.

Las estaciones de trabajo cliente acceden a este servicio a través de Internet Explorer ver 6.0.2900, sin embargo unas cuantas estaciones también tienen instalado Netscape 7.0

En el servidor de Internet está instalado ISA Server 2000 el cuál esta configurado para el acceso a Internet de todas las estaciones de trabajo, a demás está configurado el servicio OWA es decir el Outlook Web Access para el acceso al mail desde cualquier parte externa del establecimiento, este servidor también está configurado el filtrado de páginas Web de acuerdo a categorías.

NORTON ANTIVIRUS

En el servidor de antivirus está configurado el Norton Antivirus la versión 9.0, es el encargado de detectar y limpiar los virus y gusanos incluidos en la definición semanales de Symantec, también está configurado el servicio de asignación de IP dinámica a todas las estaciones de trabajo es decir DHCP, es este mismo servidor también está configurado el servicio WSUS, en este servidor se almacenan todas las actualizaciones de Windows update en línea para más tarde distribuir a las estaciones de trabajo que las requieran localmente.

CORREO ELECTRÓNICO

Este servicio está disponible para todos los usuarios que tiene una cuenta de acceso a la red. Cada usuario tiene asignado para sí un casillero de correo electrónico. La plataforma sobre la cual está montado este servicio es Microsoft Exchange Server 2003. Para acceder a los casilleros de correo existen dos alternativas:

La primera alternativa es Outlook 2003 de Microsoft Office 2003, esta opción está configurada para aquellos usuarios que tienen asignado para sí una estación de trabajo.

La segunda alternativa es Outlook Web Access que se trata de un programa desarrollado con tecnología ASP de Microsoft al cual se puede acceder desde un browser mediante un usuario y contraseña desde cualquier estación de trabajo de la red interna o del mundo que tenga acceso a Internet.

Tabla 1.12: Resumen de sistemas operativos instalados

Sistema Operativo	Número Licencias
Microsoft Windows 2003 Server Estándar	8
Microsoft Windows XP	88
Macintosh OS 9.0	12

SISTEMA ACADÉMICO

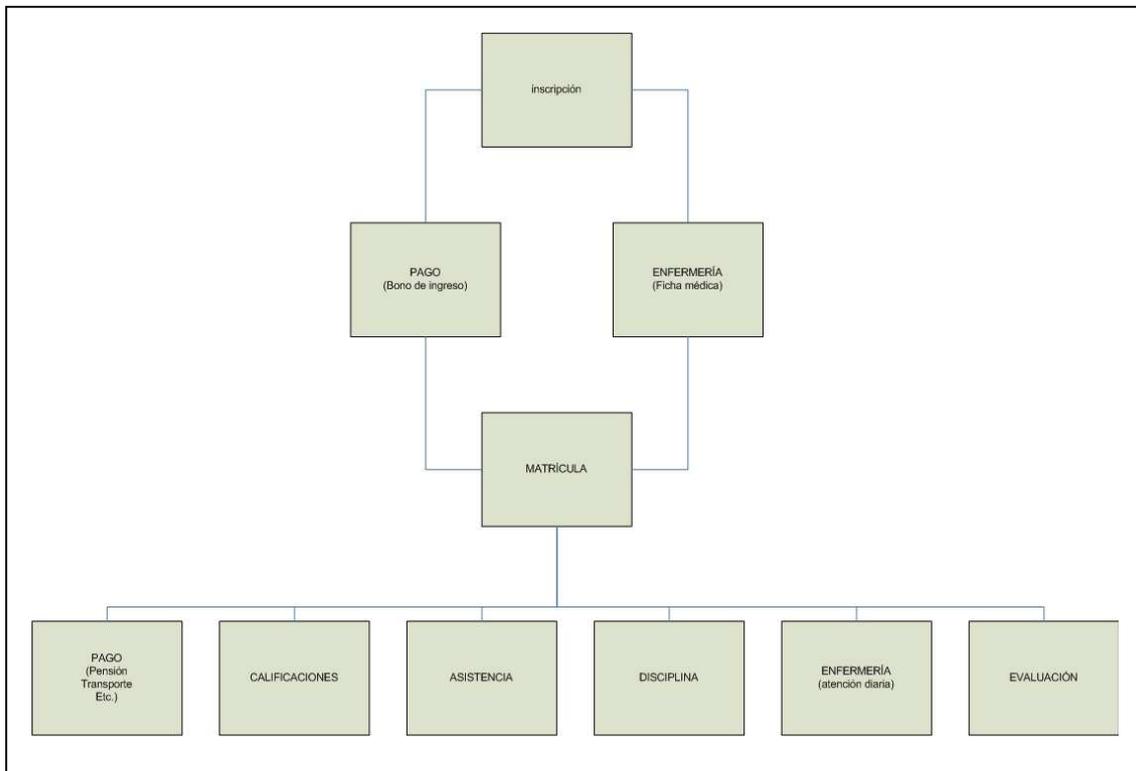
Es una aplicación de dos capas del tipo “Cliente Servidor” desarrollado en Microsoft Access 2003.

La lógica del sistema está en un archivo mde (DBCAEMDE.MDE) y que está instalado en cada una de las estaciones de trabajo. Los datos del sistema se almacenan en un archivo mdb (CAE2003.MDB) en uno de los servidores asignados como servidor de base de datos.

El desarrollo, mantenimiento y actualización de este sistema es responsabilidad íntegra del personal del departamento de Tecnología y Sistemas de la institución, en el gráfico 1.5 se puede visualizar el esquema de los módulos que componen el sistema en mención.

Una breve descripción de los módulos del sistema es la siguiente:

- Inscripciones. Registro de las aplicaciones de alumnos candidatos a ingresar a la institución.
- Matrículas. Registro del alumno en el año escolar asignado a un grado determinado
- Pagos. Generación de facturas al aplicante o al alumno de la institución por rubros calculados de acuerdo a parámetros personalizados.
- Calificaciones. Registro de calificaciones por parte de profesores por cada materia, emisión de cuadros estadísticos por aporte, emisión de libretas, y pases de año.
- Asistencia. Registro de la asistencia diaria de los alumnos, para los alumnos de primaria se hace un registro diario mientras que para los alumnos de secundaria el registro de asistencia es por horas que corresponde a las materias recibidas en el día.
- Disciplina. Registro de la disciplina diaria de los alumnos (aumentos y rebajas de puntos), registro de disciplina del alumno por aporte por parte de cada profesor, cálculo de la disciplina por aporte.
- Enfermería. Registro de las fichas médicas de cada aplicante y registro de atención diaria de cada estudiante de la institución.
- Evaluaciones al personal. Evaluación del desempeño del personal de la institución por parte de los alumnos y personal directivo del plantel.

Gráfico 1.5: Módulos del sistema académico

Se debe señalar que existe un plan en marcha de migración de la base de datos de este sistema de Access 2003 a Microsoft SQL Server 2000.

SISTEMA FINANCIERO

Es una aplicación e arquitectura orientada a servidor cuyos datos se almacenan en archivos DBF y tiene una interfaz DOS. El sistema es el conocido TMAX2000.

Este es un sistema modular y funciona con un número de licencias concurrentes limitado, para la institución se adquirió el sistema con 5 licencias de acceso concurrente. Los módulos contratados como parte de este sistema son:

- Contabilidad
- Cobranzas
- Roles

- Activos Fijos
- Base de datos

Los datos generados por las aplicaciones se almacenan en repositorios de base de datos, estos repositorios están instalados en el servidor “Server11” y son los siguientes:

- Microsoft SQL Server 2000
- Microsoft Access 2003
- Archivos DBF

Las bases de datos de las aplicaciones académicas activas se almacenan en repositorios de Microsoft Access 2003.

Las bases de datos de las aplicaciones académicas de pruebas se almacenan en Microsoft SQL Server.

Las bases de datos de las aplicaciones contables se almacenan en archivos DBF.

1.5.2 SOFTWARE ESTACIONES DE TRABAJO.

El software instalado en la mayor parte de las estaciones de trabajo se detalla a continuación:

- Windows XP Profesional de 32 de bits
- Suite Microsoft Office Profesional 2003
- Micromundos utilizado como apoyo a los profesores y estudiantes de la sección primaria en la elaboración de proyectos como complementos en las materias.
- Interactive Physics 2000, sofía utilizado para la enseñanza de física para los alumnos de los tres últimos niveles en la sección secundaria.
- Mecanografía, utilizado por los estudiantes de la primaria desde tercero de básica para la utilización del teclado y escritura en el computador.

- Cliente Norton antivirus para protección y prevención de daños que pueden ser causados por virus.
- Microsoft Student,
- Acceso al sistema de Calificaciones y Evaluaciones, utilizado por el personal para el ingreso de notas y por los estudiantes para evaluar a los profesores y materias.
- Nero Express
- Acrobat Reader
- Winzip ver. 9.0
- Acceso al Tmax en el departamento de Contabilidad
- Acceso al Isis para consulta de libros

1.6 SEGURIDAD

1.6.1 SEGURIDAD FÍSICA

Proteger los Sistemas.

El sistema de calificaciones como el contable cuenta con usuarios y passwords exclusivos para personal autorizado, cada usuario de acuerdo a su perfil tiene habilitado las opciones del sistema parcial o total, por ejemplo la secretaría académica es la única instancia autorizada para la corrección de notas.

Recuperación de Máquinas.

El centro de cómputo tiene como política tener imágenes de las estaciones de trabajo de acuerdo al tipo y características de hardware, en cuanto al software se tiene estandarizado los programas instalados en cada estación de trabajo, con el objetivo de minimizar los tiempos de inoperancia de las máquinas, tiempo máximo de recuperación 2 horas.

- Gestionar y Coordinar Políticas Internas.

- El centro de cómputo gestiona y coordina directivas de seguridad, establece sus propias reglas que son impartidas y acatadas por los usuarios como:
- Solo personal autorizado tiene acceso a las instalaciones del centro de cómputo, es decir que este personal tiene llaves de las puertas para el ingreso.
- Los equipos de uso común como son Laptops e Infocus deben ser reservados con 24 horas de anticipación.
- Buzón de correos de Exchange tiene un límite de 50 Mega bytes.
- Los Passwords deben ser cambiados cada tres meses.

Directivas de Restricción al Sistema Operativo.

Se cuenta con un mecanismo basado en directivas de grupo (GPO) para identificar el software que está en ejecución en el dominio, también se utiliza este método para impedir la ejecución de software no deseado como virus, caballos de Troya o programas que provoquen conflictos con otras aplicaciones. Con este método se puede aplicar un mismo perfil de seguridad a varios equipos.

1.6.2 SEGURIDAD LÓGICA

En cuanto a seguridad lógica están establecidas las siguientes políticas:

Autenticación y acceso a los servicios de la red

- Todo usuario para acceder a un servicio disponible en la red debe primero autenticarse con un nombre de usuario y una contraseña, además de acuerdo al servicio o aplicación y dependiendo de su función a cada usuario se le autoriza a acceder a una parte o a la totalidad de los recursos disponibles en la red.
- El tipo de autenticación que se hace es “Autenticación Básica” que es un método que provee el sistema operativo Windows 2003 Server.
- El acceso a los recursos se asigna cumpliendo las siguientes políticas generales:

- Todo usuario accede a los recursos mediante un usuario y una contraseña
- El nivel de acceso a los recursos está determinado de acuerdo al tipo de usuario, su función y el departamento al que pertenece
- De acuerdo a características comunes los usuarios son clasificados en grupos que pueden ser departamentos docentes y administrativos, grados y cursos y otros grupos personalizados, todo usuario pertenece al menos a un grupo.
- El acceso a los recursos se asigna al grupo y en excepciones al usuario

PRIVACIDAD DE LA INFORMACIÓN

De acuerdo al tipo de usuario cada uno de ellos tiene acceso exclusivo a su información personal, ese es el caso de la carpeta asignada en el servidor de archivos y la cuenta de correo electrónico disponible desde el servidor de correo electrónico, es decir que ninguna otra persona que no sea el dueño de la cuenta y el administrador general de la red puede acceder a los recursos de asignados.

ANTIVIRUS

La amenaza que representa la proliferación de distintos tipos de virus que pueden acceder a la red interna a través de Internet, para minimizar este riesgo se utiliza la suite de antivirus de Symantec y con este producto se estableció un esquema bastante aceptable de protección contra virus que consiste en lo siguiente:

La suite de antivirus de Symantec tiene una consola central de administración desde la cual se puede monitorear y escanear todas las estaciones de red, además tiene un calendario de actualización de definiciones de virus que son propagadas a las estaciones de trabajo una vez que se descarga del sitio remoto de Symantec.

Cada estación de trabajo tiene instalado el programa de antivirus de Symantec

El servidor de correo electrónico tiene su propia versión de protección de correo y spam basado en Symantec

FIREWALL

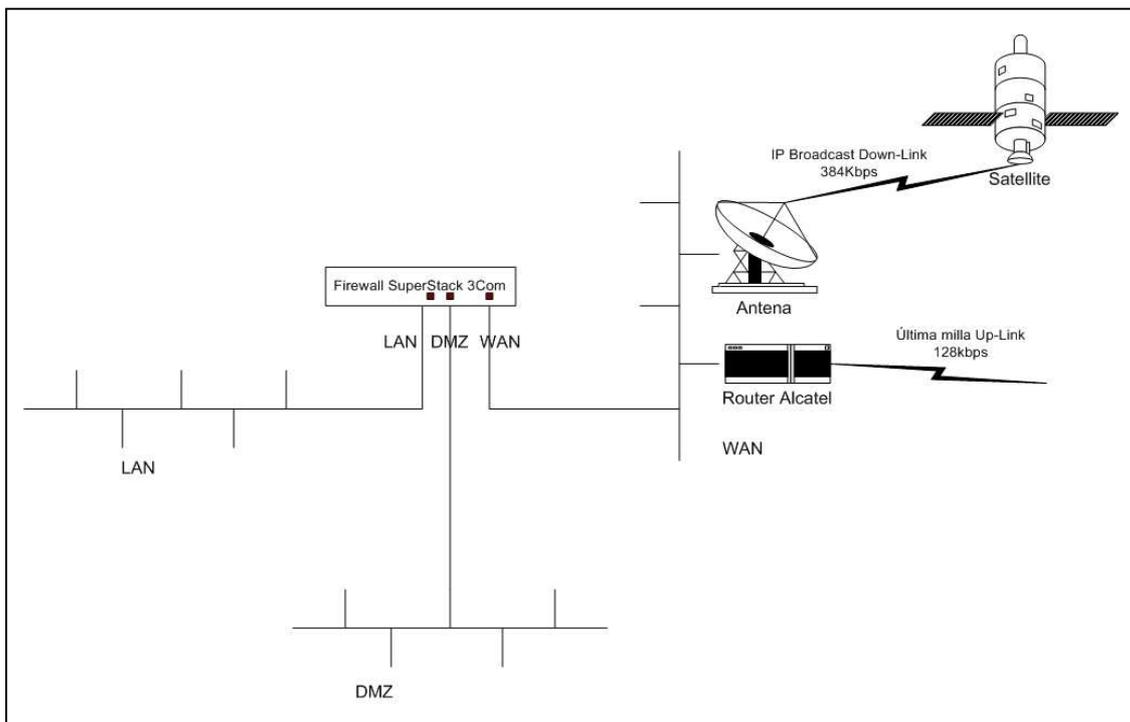
Existe el servicio de Internet al cual se accede mediante una conexión dedicada, este hecho ocasiona la amenaza de agentes externos y también existen políticas implantadas que proporcionan protección contra estos agentes, por ejemplo denegación de servicios, robo de recursos y de información, etc.

Para minimizar este riesgo existe un firewall de marca 3Com el mismo que divide a la red privada de la institución de la red pública, esto es posible porque el dispositivo mencionado como lo muestra el gráfico 1.6 tiene que tiene 3 zonas o puertos definidos que aíslan a las redes, estas zonas son:

LAN: A esta zona se conecta la red LAN de la institución, es la zona privada y más segura.

WAN: Es la zona pública y conecta todos los elementos de interconectividad necesarios para acceder a Internet.

Gráfico 1.6 Seguridad de red con Firewall



Los servicios y políticas establecidas en el firewall se muestran en las tablas 1.13 y 1.14 respectivamente

Tabla 1.13: Servicios configurados en el Firewall

Servicio	LAN Out	DMZ In
Web (HTTP)	X	X
File Transfer (FTP)	X	X
Send Email (SMTP)	X	X
Retrieve Email (POP3)	X	X
Name Service (DNS)	X	X
Ping	X	X
HTTPS	X	X
AOL	X	X
RPC	X	X
Default	X	X

Tabla 1.14: Políticas de acceso a los servicios del Firewall

Acción	Servicio	Origen	Destino
Allow	Default	WAN	DMZ
Allow	Default	DMZ	WAN
Deny	Default	*	LAN
Allow	Default	LAN	*

1.7 DIAGNÓSTICO

DEL SISTEMA DE CABLEADO ESTRUCTURADO

El sistema de cableado estructurado actual es relativamente nuevo, de su estructura y funcionalidad se puede decir lo siguiente.

El sistema de administración principal está ubicado en el bloque de Laboratorios que es una zona relativamente central del campus de la institución, esta característica facilita la posibilidad de distribuir los servicios de red a partir de esta ubicación, además las acometidas de los servicios públicos están cerca de este sector.

Existen seis sistemas de administración secundaria ubicados en distintos lugares del campus, esto permite una descentralización de la administración y monitoreo de la red y permite además un crecimiento más cómodo.

En el sistema de campus todos los enlaces que unen el MDF con cada uno de los SDF son de fibra óptica, cada enlace está constituido por cuatro hilos de fibra óptica, un par está activo para la transmisión mientras que el par restante sirve de respaldo en caso de alguna anomalía del par de hilos activo.

El subsistema de cableado horizontal consiste de algunos enlaces de cable UTP entre los SDF y las áreas de trabajo ubicadas en las oficinas y unas pocas aulas. El medio de transmisión utilizado es el cable UTP categoría 5e. Estos cables pasan a través de canaletas decorativas y ductos de manguera de 1", Las áreas de trabajo están cubiertas en un 54% y a pesar de que existen 127 puntos de red, estos en un 39% están en tres áreas de trabajo que son los laboratorios Micromundos e iMac en el bloque Laboratorios y el laboratorio existente en el bloque Preescolar, además el 60% de los puntos de red están en áreas con fines netamente administrativos.

DE LOS EQUIPOS DE LA RED

Los equipos de interconectividad son switches que soportan velocidades de 100 Mbps, la tabla 1.15 muestra el porcentaje disponibilidad por cada zona. Los resultados muestran que en promedio hay un 41% de puertos disponibles, sin embargo a excepción de las zonas Biblioteca, Primaria y Secundaria el resto de zonas tienen un porcentaje de crecimiento futuro limitado.

DE LOS EQUIPOS DE USUARIO

Existen ocho servidores cada uno con tareas específicas para cumplir. Aunque se tratan de equipos clones han cumplido sin problemas su función de servidor, esto se debe a su configuración y características.

Las características de las estaciones de trabajo permiten que en cualquiera de ellas se pueda utilizar todos los servicios y recursos que se disponen a través de la red. El número de estaciones de trabajo garantiza que cada vez menos usuarios carezcan de este recurso, el problema en menor medida existe pero es por la concentración de estos equipos en determinadas zonas en detrimento de otras.

Tabla 1.15: Porcentaje de disponibilidad de los elementos activos

#	MDF /SDF	Puertos			
		Puertos	Utilizados	Libres	% Disp
1	Laboratorios	72	52	17	24%
2	Primaria	24	8	16	67%
3	Biblioteca	24	9	15	63%
4	Administración	24	19	5	21%
5	Inspección General	24	17	7	29%
6	Secundaria	24	13	11	43%
7	Preescolar	24	15	9	38%
	Porcentaje de disponibilidad global				41%

Las diez impresoras de red y las cuatro impresoras compartidas actualmente son suficientes para cubrir las necesidades de impresión en todas las zonas que componen el campus de la institución.

DE LA SEGURIDAD FÍSICA

Todos los usuarios podrían en determinado momento acceder a todas las estaciones de trabajo de la institución utilizando su usuario y contraseña.

Los elementos de interconectividad ubicados en los distintos ambientes del campus están expuestos al público a excepción del Cuarto principal de comunicaciones ubicado en la Sala de servidores que es un cuarto privado con llaves al que solo tiene acceso el personal de Sistemas.

DE LA SEGURIDAD LÓGICA

La red de datos de la institución trabaja bajo el ambiente Windows, esta familia de Sistemas tiene un esquema de seguridad denominado Autenticación Básica basado en Usuario y Contraseña, todos los usuarios para acceder a los servicios y recursos necesitan autenticarse y de acuerdo a su perfil tendrán más o menos privilegios de acceso. Existe un esquema definido para la creación de usuarios y grupos. Existe un grupo de usuarios alumnos de 1ro a 5to EGB que tienen contraseñas fáciles de descifrar cuyas cuentas en un momento determinado pueden ser utilizadas para otros fines.

Existen sistemas de protección contra virus en las estaciones de trabajo y servidores, estos antivirus también protegen servicios de correo electrónico y Web. Faltan sistemas de filtrado de contenido de acceso a sitios web.

Un recurso adicional que existe en cuanto a seguridad es el firewall que es una barrera contra agentes externos, este equipo cumple su función básica de bloquear puertos y otras propias de este recurso. Sin embargo su configuración no es completa lo que no garantiza una protección entera.

Existe también un esquema de respaldo de información definido que consiste en respaldar la información de las bases de datos de los sistemas de la institución, las bases de datos del correo electrónico y los documentos que almacena el personal en cada carpeta asignada en el servidor de archivos. No hay un esquema para respaldo de información de los datos almacenados en los computadores ubicados en las oficinas.

SEGMENTACION DE LA RED

Actualmente todo el tráfico está disponible para la Internet, aplicaciones DOS y datos en general, por esta razón es necesario reordenar el tráfico IP para video, es decir se requiere segmentar la red o crear VLANs para las aplicaciones de video.

1.8 ANALISIS DE REQUERIMIENTOS

Con el apareamiento de las redes de computadoras los procesos se han ido simplificando de forma significativa en las Organizaciones, el ahorro de recursos y la integración de los sistemas de información han sido las características principales una Lan.

Cada vez se requiere que las redes de área locales integren más servicios en una organización como son los sistemas de base de datos, servidores de impresión, servicios de backup, seguridad de los datos, lo que significa una parte estratégica dentro de las organizaciones, es así que también hoy en día se requiere que las redes integren servicios adicionales como la transmisión de audio y video, con la premisa de no solo proteger los datos si no también el recurso humano.

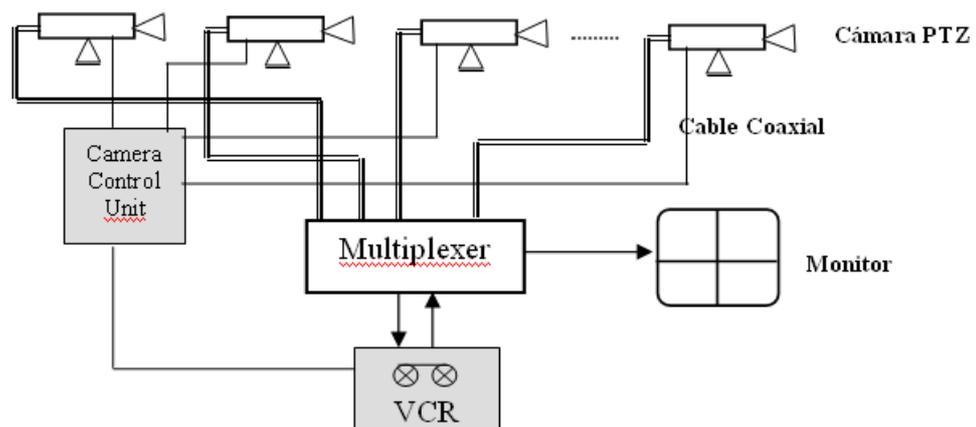
A continuación se detalla los requerimientos tanto en hardware como en software para el presente proyecto:

1.8.1 MONITOREO IP

Los sistemas de televisión de circuito cerrado CCTV y los de vigilancia por video IP se está convirtiendo en un componente vital en la mayoría de la Instituciones, la vigilancia es un componente integral de los métodos de control y acceso implementando sistemas de autenticación biométricos, sistemas de rastreo de seguridad y sistemas de rastreo de acceso.

Los sistemas análogos tradicionales CCTV fueron diseñados para transmisión punto a punto de video desde una cámara hasta una grabadora en el mismo sitio utilizando cable coaxial de 75 Ohm. Varias cámaras se conectaban por medio de este cableado y se conectaban en home-run a multiplexores que alimentaban varias grabadoras de video en un cuarto de control central gráfico 1.7, se podía mirar las imágenes en tiempo real por medio de varios monitores, se disponía de un switch para cambiar a la cámara deseada a un monitor específico, o de monitores capaces de aceptar múltiples fuentes de video en ventanas separadas.

Gráfico 1.7 Video Analógico CCTV



Siemón, Network Cabling Solutions. [Disponible en http://www.siemon.com/la/white_papers/SD-03-08-CCTV.asp]

La desventaja en este método radica en el costo de la estación de monitoreo, el monitoreo centralizado constituye un punto de falla crítico dentro de la infraestructura de seguridad. Todas las alimentaciones de video y cables de control tienen que ser instalados en home-run hacia este punto.

Si una cámara era reubicada frecuentemente se requería un nuevo tendido de cable, las cintas requerían muchas cintas y debido a que los medios magnéticos son susceptibles a descargas magnéticas o electroestáticas estos sistemas no siempre proporcionaban el total de la funcionalidad para lo cuál fueron diseñadas. El factor humano también era parte de este sistema ya que una persona era el responsable de cambiar físicamente las cintas, monitorear las sesiones de grabación, etc. En ocasiones el uso de fibra óptica era necesario en ambientes donde las distancias requerían el uso de repetidores para ampliar la señal a donde la interferencia electromagnética representa un problema.

Con el apareamiento de cámaras de red nace un sistema de segunda generación. Las cámaras direccionables IP pueden ser incorporadas actualmente en la infraestructura existentes en edificios. El desarrollo de imágenes digitales se almacena en formato digital en servidores u otras computadoras en lugar de cintas de video, aliviando los problemas inherentes a medios magnéticos.

Esta nueva especie de video permite transmisiones IP de las señales de video a los dispositivos direccionables IP y pueden transmitirse en combinación con secuencia de voz y/o video.

Adicionalmente los movimientos y cambios son más fáciles ya que las cámaras pueden instalarse dondequiera que exista un punto de red. El cableado viaja hacia un multiplexor que soporta los populares conectores RJ45. Las cámaras tradicionales o analógicas con conectores coaxiales pueden reacondicionarse con baluns (balanced/unbalanced) que convierten la señal de un cable coaxial (no balanceada) a la del cable de par trenzado (balanceada).

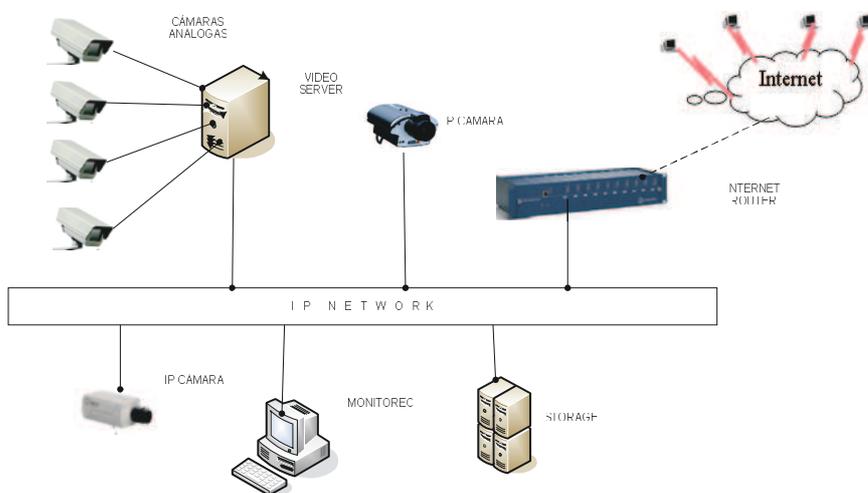
Los Equipos electrónicos que manejan el tráfico en la red IP se han vuelto parte integral en los sistemas de vigilancia por el almacenamiento de video en formato

digital que pueden ser vistos desde cualquier lugar de la red con nuevas capacidades de seguridad para los archivos administrados como parte de las políticas de seguridad de la red.

TCP/IP es el protocolo utilizado para la mayoría de redes su arquitectura abierta permite que varios sistemas puedan compartir el espacios de red y aprovechar estas nuevas tecnologías para aumentar su capacidad, escalabilidad u accesibilidad de los recursos de la red. Los administradores y usuarios de la red tienen la ventaja de monitorear desde cualquier estación de trabajo con acceso a la red, de igual forma el personal de seguridad de la Institución. La cámara digital se vuelve ahora en el punto de falla y ya no en el centro de control ya que se puede tener servidores redundantes digitales ya sea en solo sitio o distribuido en múltiples ubicaciones.

Un sistema típico CCTV basado en IP se indica en el gráfico 1.8 como se puede apreciar las cámaras y los servidores de video IP pueden colocarse en cualquier punto de la red, como en el protocolo IP las funciones de administración son incorporadas en la transmisión, esto incluye **DSP** (Digital Signal Procesing) manejo de alarmas, grabación capacidades de búsqueda y/o archivo, calendarización y automatización. Estas funciones de administración y control utilizan SNMP (Simple Network Management Protocol).

Gráfico 1.8 Video IP Digital CCTV



Siemón, Network Cabling Solutions. [Disponible en http://www.siemon.com/la/white_papers/SD-03-08-CCTV.asp]

Las cámaras IP pueden equiparse con características avanzadas según la necesidades del caso tales como sensores de movimiento, **PTZ** (Pan Tilt and Zoom) automatizado, y si se desea salidas análogas de video, las versiones más actualizadas de estas cámaras vienen equipadas con DVR internos que pueden replicarse con un servidor DVR centralizado.

Es necesario establecer el ancho de banda de la red que consiste en decidir cuántas cámaras se necesitan, qué calidad de vídeo es necesaria para el visionado y la grabación, y cuántos días de grabación se necesitan. Después se puede utilizar esta información para calcular cuánto ancho de banda y almacenamiento de grabaciones se necesita.

Es fundamental que a cada cámara se le asigne una dirección IP, asegurándose que se encuentran en la misma subred y por lo tanto se pueden realizar pruebas de comunicación para verificar si cada cámara responde.

1.8.2 HARDWARE Y SOFTWARE DE RED

SERVIDOR DE MONITOREO.

Un único servidor típicamente sirve a una multitud de clientes, ahorrando a cada uno de ellos el problema de tener la información instalada y almacenada localmente, permitiendo al servidor enviar una sola copia de la información a múltiples clientes quienes deseen recibir la información. Para el efecto se puede utilizar una computadora con características similares en hardware que se esta utilizando en el área de servidores con software Windows 2003 Server.

En hardware se requiere un servidor con las siguientes características:

- Tarjeta madre Intel modelo 875
- Procesador Pentium IV 3.1 Ghz
- Memoria RAM 1GB
- Dos discos duros 120GB
- Unidad de DVD - Writer

- Tarjeta de red incorporada 10/100 Mbps

En software el servidor requiere el siguiente software a ser instalado.

- Sistema Operativo Windows 2003 Server
- Service Packs de Windows Actualizados
- Software de Monitoreo

CÁMARAS IP.

Una cámara de red tiene su propia dirección IP y características propias para gestionar la comunicación en la red. Todo lo que se precisa para la visualización de las imágenes a través de la red se encuentra dentro de la misma unidad. Una cámara de red puede describirse como una cámara y un computador combinados. Se conecta directamente a la red como cualquier otro dispositivo de red e incorpora software propio para servidor Web, servidor FTP, cliente FTP y cliente de correo electrónico. También incluye entradas para alarmas y salida de relé. Las cámaras de red más avanzadas también pueden equiparse con muchas otras funciones de valor añadido como son la detección de movimiento y la salida de vídeo analógico.

La razón más habitual de una calidad de imagen pobre es la insuficiencia de luz. Con un nivel de luz muy bajo el nivel de los colores será sombrío y las imágenes borrosas. El nivel de luz se mide en Lux. La luz solar fuerte tiene aproximadamente 100.000 Lux, la luz diurna tiene aproximadamente 10.000 Lux y la luz de una vela tiene aproximadamente 1 Lux. Habitualmente se precisan al menos 200 Lux para capturar imágenes de buena calidad. Las áreas brillantes deben ser evitadas dado que las imágenes pueden resultar sobre-expuestas y que los objetos aparezcan muy oscuros. Este problema ocurre igualmente cuando se intenta capturar un objeto con luz negra. Una cámara ajusta la exposición para conseguir una buena media de nivel de luz para la imagen, pero el contraste de color entre el objeto y el fondo influye en la exposición. Para evitar este problema

los objetos oscuros pequeños deberían disponerse delante de un fondo oscuro para conseguir el color y el contraste correctos.

A continuación se describen las siguientes características que deben considerarse en la elección de las cámaras IP.

CALIDAD DE IMAGEN.

Esta característica es una de las más importantes, si la calidad de la imagen no es buena el resto de factores es irrelevante, una mejor calidad de la imagen permite al usuario obtener mejores resultados en detalles y cambio en la imágenes según su evento, es importante tener en consideración cuál es su sensibilidad lumínica, si la imagen es clara, que calidad tiene la imagen cuando existe movimiento. Se debe considerar los siguientes factores:

- Permitir zoom de la imagen
- Sensibilidad lumínica día noche
- Permitir ángulos de cobertura
- Cámaras día noche, grabación con detección de movimiento, audio
- Cámaras día noche espía
- Cámaras día, grabación con detección de movimiento

En el capítulo 3 sección 3.1 se describe el tipo de cámaras IP que se requieren para el presente proyecto.

FACILIDAD DE INTEGRACIÓN.

Las cámaras IP deben ser capaces de integrarse a plataformas abiertas es decir que puedan ser configuradas fácilmente para operar con otros tipos de cámaras de fabricantes distintos con sus respectivas aplicaciones de software.

Una particularidad importante se trata que cuando la cámara sea instalada, configurada y posea una dirección IP dentro de la red local ésta sea fácil de

de incorporarse a cualquier software de monitoreo y no limitarse exclusivamente al software del fabricante específico.

COMPRESION COMPATIBLE CON LOS ESTANDARES JPEG³, MPEG4⁴

Una compatibilidad a los estándares asegura flexibilidad en el uso de muchas aplicaciones de video diferente garantizándose así la visualización de video por largo tiempo con sistemas patentados de acuerdo a las normas internacionales. Se debe tener en consideración la cantidad de licencias que se deben adquirir para el circuito IP.

Las cámaras de tecnología IP que se incorporarán al presente proyecto deben cumplir con los estándares de video existentes en el mercado por la sencilla razón que permite la optimización de los sistemas para que consigan la mejor calidad de imagen y el menor consumo de ancho de banda y que sean compatibles con diferentes tipos de cámaras que usan los mismos tipos de estándares.

Requisitos de sistema para visualización de cámaras vía IP.

Navegadores Web compatibles: Windows -

- Internet Explorer
- Mozilla 1.4* ó posterior
- Mac OS X - Mozilla 1.4* ó posterior y
- Netscape 7.1* ó posterior

Sistemas operativos compatibles: Windows XP, 2000, NT4.0, ME y 98, Linux y Mac

³ método comúnmente utilizado para la compresión de imágenes fotográficas

⁴ Moving Picture Expert Group. grupo de estándares de codificación de audio y video

Hardware: según las especificaciones del sistema que puede ser las estaciones de trabajo con las características mencionadas anteriormente operativo y el navegador.

SOFTWARE DE MONITOREO

Se requiere implementar un software que permita gestionar el sistema de cámaras de video IP para potencializar al máximo las aplicaciones en calidad tecnología de compresión y beneficios del video IP.

Dichas aplicaciones de software posibilitan el control, administración y visionado tanto de las grabaciones en directo como del vídeo grabado a través de la red IP. El poder construir un circuito cerrado de monitoreo IP no se encuentra en la cámara sino en el software de gestión, que ofrece una aplicación útil al usuario final. Por lo tanto, el rendimiento general depende fundamentalmente de la interacción del software con la cámara IP, el hardware de grabación y la red.

El circuito cerrado IP se trata de un conjunto de componentes que se distribuyen a través de una red IP, siendo el componente absolutamente esencial el software que gestiona el resto de los componentes. Así que las cámaras IP no son suficientes por sí solas. Su funcionalidad real se encuentra en el software, que debería ser la prioridad al decidir qué solución de vídeo IP se va a elegir, dicho software depende en última instancia del rendimiento del sensor de imagen y la calidad de compresión.

Además debe incorporar la visualización o monitoreo dentro de la red local como hacia fuera, la posibilidad de integrar cámaras de distinta tecnología que disponga una interfaz de sistema abiertos es decir una interfaz de programación.

Se ha intentado de incorporar software libre (Licencia Pública General GNU) como una alternativa para el desarrollo de este proyecto, debido a políticas de seguridad la licencia adquirida debe ser de uso exclusivo de la institución,

además que la inserción y utilización de la GNU puede encontrar dificultades desde el punto de vista de la aplicación y validez, debido a la rigidez o contravención de leyes y normas en defensa de los derechos de los consumidores.

En el capítulo 3 sección 3.2.4 se describe el software de monitoreo que se requiere para el presente proyecto.

FUNCIONALIDAD Y SEGURIDAD DE RED.

Se debe determinar si la cámara ofrece funciones y seguridad de red adecuadas por la razón que cada dispositivo de estos utiliza una dirección de red, de igual forma el acceso o monitoreo remoto se deben establecer las seguridades en el protocolo HTTPS.

Para el acceso remoto los protocolos a utilizarse son el HTTP puerto 80 y el protocolo HTTPS que utiliza el puerto 8080, estas configuraciones de acceso se los configura en el servidor ISA con las reglas de publicación de un servidor para permitir tráfico de redes externas.

1.8.3 MEDIOS DE ALMACENAMIENTO

Todos los eventos ocurridos deben ser registrados o almacenados en algún lugar de la red de acuerdo de acuerdo a la política de grabación previamente definida con el jefe de seguridad.

En el capítulo 2 sección 2.9 se indica un gráfico en el número de horas que una cámara debe grabar por día.

Los eventos digitales se graban en discos duros de la misma forma en que un archivo se almacena en una PC, esto método permite obtener redundancia, monitoreo descentralizado y mayor longevidad de las grabaciones. En las computadoras se cuentan con discos duros de tecnología IDE - ATA.

La mayor parte de las computadoras tienen discos de tipo IDE (que por evidentes razones económicas son los más utilizados en la actualidad), es posible afirmar que en los últimos años sus prestaciones han mejorado bastante, se ha conseguido que los últimos modelos de discos IDE alcancen las 7.200 revoluciones por minuto (los IDE anteriores eran de 5.400 r.p.m.), lo cual significa mayor velocidad en la lectura de los datos.

Serial ATA o S-ATA es una interfaz para discos que sustituye a la tradicional Paralelo ATA o P-ATA (estándar que también se conoce como IDE o ATA). El S-ATA proporciona mayores velocidades, mejor aprovechamiento cuando hay varios discos, mayor longitud del cable de transmisión de datos y capacidad para conectar discos en caliente (con la computadora encendida). Ancho de banda: Mientras que la especificación SATA1 llega como máximo a unos 1.5 GBit/s, SATA2 incrementa el límite a 3 GBit/s. Actualmente es una interfaz ampliamente aceptada y estandarizada en las placas base de PC.

A continuación se describe los requerimientos necesarios y características de los discos que se necesitan como medios de almacenamiento:

Capacidad. Cantidad de datos que pueden almacenar. Un disco duro actual debe de tener, al menos, 20 Gb.

Velocidad de giro. Muy importante que sea de al menos 7.200 R.P.M., se nota la diferencia de velocidad respecto de los de 5.400 R.P.M. Si es SCSI lo podremos encontrar de hasta 10.000 R.P.M.

Tiempo de acceso. Nos marca el tiempo que tarda en acceder a cualquier parte del disco de manera aleatoria. Lógicamente, cuanto más baja menor. Se suele medir en milisegundos (ms) y actualmente ronda los 10-8 ms.

Tipo de transmisión. Hay que fijarse que un disco duro IDE sea ATA 100. Esto es el sistema de transmisión, que podría alcanzar los 100 Mb por segundo, pero, claro está, esto es teórico porque un disco duro suele mover unos 30 Mb por

segundo como mucho, aunque ya empiezan a aparecer discos duros y placas base ATA 133. Si es SCSI la transmisión podrá ser de 80, 160 o 320 Mb/s.

Caché del disco. Este es un dato importante. Es un tipo de memoria que intenta mantener constante el envío de datos a la controladora. Suelen rondar los 2 Mb,

Estas características de los discos duros son parámetros referenciados desde la información de los fabricantes, con el fin de obtener la mayor información posible para ser incorporada a las estaciones de trabajo que forman parte del proyecto.

En este ámbito, los nuevos equipos que se están adquiriendo en este caso los computadores tienen tecnología SATA2 por los beneficios anteriormente mencionados.

1.8.4 FORMATOS DE COMPRESION DE VIDEO

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. Para almacenar y transmitir imágenes a través de una red los datos deben estar comprimidos o consumirán mucho espacio en disco o mucho ancho de banda. Si el ancho de banda está limitado la cantidad de información que se envía debe ser reducida rebajando el número de frames⁵ por segundo o aceptando un nivel de calidad inferior.

Existen múltiples estándares de compresión que resuelven los problemas de número de frames por segundo y calidad de imagen de diferentes formas. De los estándares más comunes tanto el JPEG como el MPEG transmiten vídeo de alta calidad, mientras que los estándares-H, usados normalmente en videoconferencia, no generan imágenes claras de objetos que se mueven a gran velocidad. Cada punto de la imagen se le asigna un determinado número de bits que representarán el color de dicho punto. Si la imagen es en blanco y negro, bastará un bit para representarlo, mientras que para 256 colores serán necesarios 8 bits. De esta forma tendremos la imagen digitalizada, pero almacenar esta información dependerá del número de pixels que utilicemos por imagen. Por ejemplo una imagen de 640 x 480 puntos con 256 colores ocupan 300 Kb, y si tenemos una secuencia de vídeo a 25 fotogramas por segundo significaría que un solo segundo ocuparía 7.500 Kb. La información de vídeo compuesta de esta manera posee una cantidad tremenda de información; por lo que, para transmisión o La compresión del vídeo generalmente implica una pérdida de información y una consecuente disminución de calidad. Pero esto es aceptable porque los algoritmos de codificación están diseñados para descartar la información redundante o que no es perceptible por el ojo humano.

⁵ Es una imagen independiente, sucesión de frames compone una animación

El vídeo comprimido en general debe transmitir información por un canal más pequeño del que necesitaría para ser transmitido y poder ser visualizado en tiempo real. Así la información de audio y vídeo deben ser procesadas por los codecs antes de ser transmitidos. Los codecs derivan de las palabras compresor y descompresor, y son los módulos de software que permiten la compresión y descompresión de los ficheros de audio y vídeo para que puedan ser transmitidos por redes de baja velocidad. La técnica de compresión de vídeo consiste de tres pasos fundamentalmente, primero el preprocesamiento de la fuente de vídeo de entrada, paso en el cual se realiza el filtrado de la señal de entrada para remover componentes no útiles y el ruido que pudiera haber en esta. El segundo paso es la conversión de la señal a un formato intermedio común (CIF), y por último el paso de la compresión. Las imágenes comprimidas son transmitidas a través de la línea de transmisión digital y se hacen llegar al receptor donde son reconvertidas al formato común CIF.

Mediante la compresión de la imagen se elimina información redundante. Se ayuda de la redundancia espacial y temporal. La redundancia temporal es reducida primero usando similitudes entre sucesivas imágenes, usando información de las imágenes ya enviadas. Cuando se usa esta técnica, sólo es necesario enviar la diferencia entre las imágenes, es decir las zonas de la imagen que han variado entre dos fotogramas consecutivos, lo que elimina la necesidad de transmitir la imagen completa. La descompresión es el proceso inverso de la compresión. La compresión espacial se vale de las similitudes entre píxeles adyacentes en zonas de la imagen lisas, y de las frecuencias espaciales dominantes en zonas de color muy variado. El método para eliminar las redundancias en el dominio del tiempo pueden ser eliminadas mediante el método de codificación de intercuadros, que también incluye los métodos de compensación/estimación del movimiento, el cual compensa el movimiento a través de la estimación del mismo.

Los estándares de vídeo digital más conocidos son: MPEG, Quicktime, AVI, MOV, real vídeo, ASF. JMPEG MPEG (Grupo de Expertos en Imágenes en movimiento) es un estándar internacional, definido por un comité llamado MPEG formado por

la ISO, para la representación codificada y comprimida de imágenes en movimiento y audio asociado, orientado a medios de almacenamiento digital, MPEG-1 guarda una imagen, la compara con la siguiente y almacena sólo las diferencias. Se alcanzan así grados de compresión muy elevados. Define tres tipos de fotogramas:

Fotogramas I o Intra-fotogramas, son los fotogramas normales o de imagen fija, proporcionando una compresión moderada, en JPEG.

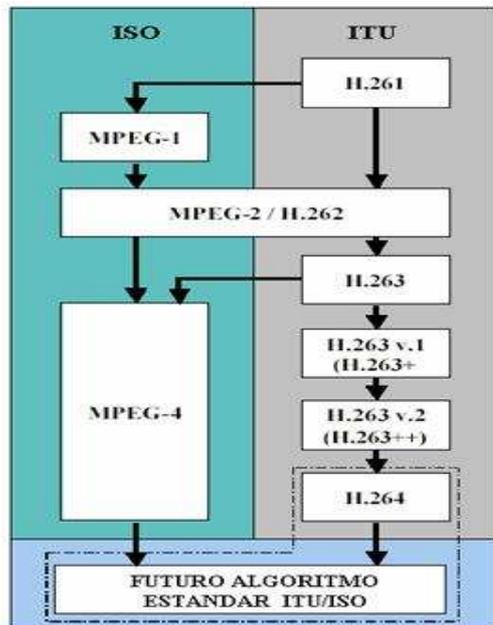
Fotogramas P o Predichos: son imágenes predichas a partir de la inmediatamente anterior. Se alcanza una tasa de compresión muy superior.

Fotogramas B o bidireccionales: se calculan en base a los fotogramas inmediatamente anterior y posterior. Consigue el mayor grado de compresión a costa de un mayor tiempo de cálculo. Estándar escogido por Vídeo-CD: calidad VHS con sonido digital.

MPEG-2

Con una calidad superior al MPEG-1, MPEG-2 fue universalmente aceptado para transmitir vídeo digital comprimido con velocidades mayores de 1Mb/s aproximadamente

MPEG4 es un estándar relativamente nuevo orientado inicialmente a las videoconferencias, y para Internet, (gráfico 1.9). El objetivo es crear un contexto audiovisual en el cual existen unas primitivas llamadas AVO (objetos audiovisuales). Se definen métodos para codificar estas primitivas que podrían clasificarse en texto y gráficos. JPEG utiliza una técnica de compresión espacial, la intracuadros o DCT. El sistema JPEG solamente utiliza la compresión espacial al estar diseñado para comprimir imágenes individuales.

Grafico 1.9 técnicas de compresión de video

1.8.5 TRANSPORTE DE PAQUETES DE VIDEO

La transmisión digital y la distribución de audio y video permite la comunicación multimedia sobre las redes que soportan la transmisión de datos, brindando la posibilidad de enviar imágenes en movimiento a cualquier sitio remoto, el video es muy sensible al retardo en la red, ya que puede provocar cortes en la secuencias.

La pérdida de información en el video sin comprimir no es muy sensible ya que al perderse un fotograma, el siguiente fotograma proporciona la suficiente información para poder interpretar la secuencia, en cambio el video comprimido es más sensible a errores de transmisión ya que las técnicas de compresión se valen de redundancia temporal que pueden perder información.

Algunas técnicas de compresión compensan esta sensibilidad a la pérdida de datos enviando la información completa sobre un fotograma cada cierto tiempo, incluso si los datos del fotograma no han cambiado. Esta técnica también es útil para los sistemas de múltiples clientes, para que los usuarios que acaban de

conectarse, reciban las imágenes completas. Si se dispone de un alto ancho de banda el tipo de red adecuada es ATM; para un entorno de red de área local podríamos usar Fast Ethernet, y actualmente para que el usuario de Internet ADSL. Pero la solución para resolver el cuello de botella del ancho de banda del vídeo no está en un solo tipo de red, sino en una infraestructura de red flexible que pueda manejar e integrar diferentes redes y que deje paso también a futuras redes sin cambiar el hardware. También debe ser capaz de negociar las variables de ancho de banda, resolución, número de fotogramas por segundo y algoritmo de compresión de audio. Así que se necesita un nodo que permita la interconectividad entre todas las redes.

1.8.6 DIGITALIZACION DE IMAGENES DE VIDEO

Cada muestra de color se codifica en señal Y-U-V (Y- luminancia, U y V crominancia) partiendo de los valores del sistema RGB. Con este sistema las diferencias de color pueden ser muestreadas sin resultados visibles, lo que permite que la misma información sea codificada con menos ancho de banda.

Luminancia(Y): $720 \times 576 \times 25 \times 8 = 82.944.000$ bits por segundo

Crominancia(U): $360 \times 576 \times 25 \times 8 = 41.472.000$ bits por segundo

Crominancia(V): $360 \times 576 \times 25 \times 8 = 41.472.000$ bits por segundo

Las imágenes de vídeo están compuestas de información en el dominio del espacio y el tiempo.

La información en el dominio del espacio es provista por los píxel, y la información en el dominio del tiempo es provista por imágenes que cambian en el tiempo. Puesto que los cambios entre cuadros colindantes son diminutos, los objetos aparentan moverse suavemente. El valor de luminancia de cada píxel es cuantificado con ocho bits para el caso de imágenes blanco y negro. En el caso de imágenes de color, cada píxel mantiene la información de color asociada; una imagen completa es una composición de tres fotogramas, uno para cada

componente de color, así los tres elementos de la información de luminancia designados como rojo, verde y azul, son cuantificados a ocho bits.

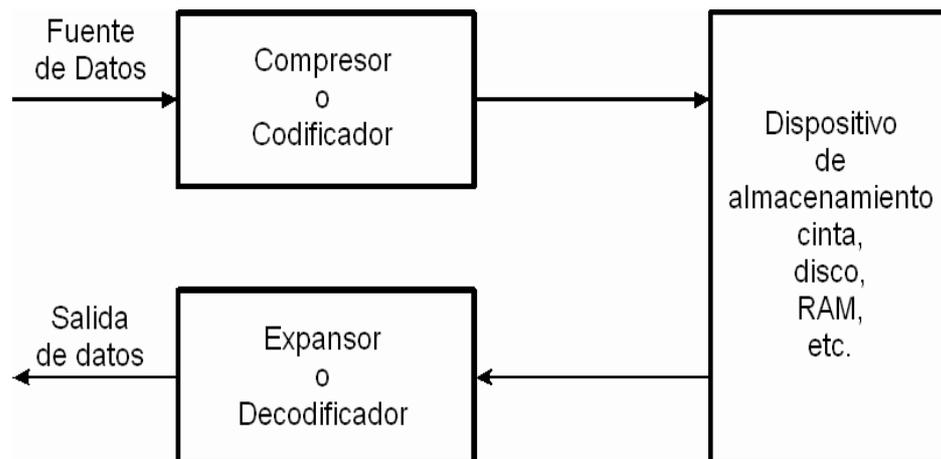


Gráfico 1.10
de transporte
de video

FALLAS EN LA TRANSMISION.

Muchas cosas pueden pasar entre la fuente del video y el receptor de video, en este contexto se derivan fallas de transmisión en la red que se deben considerar cuando se planea la transmisión de video.

PERDIDA DE PAQUETES.

Un paquete es declarado perdido cuando no llega a tiempo a su destino, esto puede ser causado por muchas circunstancias tales como fallas en la red debido a que un simple bit dentro del paquete puede estar defectuoso o erróneo o por fallas en la configuración de la red como envíos de paquetes erróneos al destino, en muchos de los casos los paquetes pueden perderse ocasionalmente en la transmisión sobre redes IP.

Los paquetes IP incluyen un checksum en cada cabecera, este checksum es utilizado para realizar pruebas en la cabecera si esta corrupta en la transmisión. En cada lapso de tiempo un paquete es recibido, el checksum es recalculado, si el

resultado de la recalculación no es igual al checksum entrante, la cabecera ha sido corrompida y el paquete será rechazado.

Una forma de calcular el porcentaje de error de transmisión de los paquetes es chequear el BER (Bit Error Ratio) es el número de bits defectuosos dividido por el número total de bits transmitidos. Muchos tipos de fibra óptica especifican el BER como 1×10^{-9} en porcentaje de error.

REORDENAMIENTO DE PAQUETES.

Los paquetes se reordenan en una red cuando los paquetes son recibidos en diferente orden que originalmente fueron enviados, como por ejemplo algún tipo de e-mail o transferencias de archivos esto no es un problema mientras los paquetes sigan llegando.

El video streaming particularmente MPEG tiene definida una buena estructura y secuencia, esta estructura es necesaria para permitir una correcta decodificación y determinar en donde cada píxel necesita ser reemplazado en la imagen, la sincronización de estos datos es muy importante, si algunos de los datos para una imagen no es el correcto en esta sincronización para desplegar una imagen, la imagen tendrá errores y no podrá ser desplegada completamente.

Cuando los paquetes llegan fuera de orden deben ser retransmitidos en una secuencia correcta para que la decodificación de video sea operable.

Los paquetes pueden llegar en desorden por varias razones, una de las posibles causas pueden darse cuando existe muchos caminos desde la fuente a los destinos, los paquetes destinos pueden utilizar diferentes caminos y diferentes tiempos para llegar a su destino, también puede darse por congestión en la red, los paquetes pueden retardarse mientras esperan por su turno para ser enviados.

Los paquetes que llegan en desorden pueden fácilmente reordenarse a través del uso de un buffer de manera que esto puede causar más retardo en el envío de información, cuando se evalúa una red para el tráfico de video se debe examinar

este parámetro de reordenamiento de paquetes, para lo cual se podrá decidir si va a servir la transmisión de video.

RETARDO

Existen dos causas principales para el retardo: Propagación en el retardo y switching retardo.

Propagación Delay. Es la cantidad de tiempo que toma la información para viajar desde una localización a otra, con las redes modernas la información puede viajar tomando como referencia la velocidad de la luz usando ondas de radio o fibra óptica.

Switching delay ocurre en cualquier punto de la red donde una señal necesita ser ruteada o switched. El retardo en este punto puede darse por varios motivos como la cantidad de paquetes que el ruteador está procesando, también por congestión o el tiempo de procesamiento que utiliza el ruteador.

El ruteador utiliza el mecanismo de llamada de colas para manejar los paquetes que es muy similar a línea de cajeros en un supermercado, los paquetes van ubicándose en diferentes colas dependiendo de su prioridad, tamaño y tiempo.

La cantidad de tiempo que toma un paquete para viajar a través de un ruteador es afectado por el sitio donde esté ubicada.

JITTER Es una medición de la variación de tiempo de la llegada de los paquetes, por ejemplo un remitente está transmitiendo 500 paquetes por segundo o uno cada 2000 microsegundos un jitter ideal a cero sería que los paquetes lleguen al receptor sincronizadamente de la misma forma que fueron enviados es decir uno cada 2000 microsegundos, jitter puede ocurrir cuando los paquetes recibidos tienen diferente sincronización que puede ser 20 microsegundos temprano o 50 microsegundos después, es decir que el retardo entre paquetes no es constante.

Latencia es el tiempo que se tarda en obtener una respuesta, es la suma del retardo de la red y los servidores, retardo de propagación y de transmisión (dependiente del tamaño del paquete).

Un tiempo de latencia variable se define como Jitter (fluctuación del retardo) sobre los datos de recepción, la solución del jitter es guardar los datos en memorias buffer, lo cual hace al retardo mayor formas de buffer

VIDEO EN INTERNET

Existen dos métodos para la distribución de contenido con audio y vídeo sobre la Web. El primer método usa un Servidor Web estándar para repartir los datos a un medio visualizador. El segundo método usa un servidor de streaming.

SERVIDOR WEB

Cuando se ha digitalizado la información el archivo deberá ser codificado o comprimido a un archivo para ser distribuido sobre una red con un específico ancho de banda que puede ser un MODEM a 56kbps. Usando el protocolo http desde cualquier lugar podríamos conectarnos al servidor Web y visualizar el video.

Este protocolo no está optimizado para aplicaciones en tiempo real, el objetivo es maximizar el ratio de transferencia para lo cual utiliza un algoritmo llamado "comienzo lento". TCP manda primero paquetes con un bajo ratio y gradualmente va incrementando el ratio hasta que el destinatario comunica una pérdida de paquetes, entonces TCP asume que se ha llegado al límite el ancho de banda y vuelve a enviar la información a baja velocidad y volverá a incrementar la velocidad repitiendo el proceso anterior.

1.8.7 SEGMENTACION DE LA RED.

Los archivos de datos corporativos de gran tamaño (Tmax, Isis), como los correspondientes a contabilidad y biblioteca deberán ser accesibles por parte de distintos usuarios en un tiempo determinado mas las aplicaciones de video

provocarán congestión en la red, para optimizar el rendimiento de la red y el uso adecuado del ancho de banda es necesario establecer vlans para tráfico de video y tráfico de datos mediante segmentos de red.

Con el aumento de nuevos laboratorios de cómputo e incremento de usuarios y se pretende añadir video en movimiento y aplicaciones multimedia, estos factores representan una exigencia aún mayor para la capacidad de ancho de banda.

Cuando cada vez más usuarios utilizan la red para compartir archivos, acceder a servidores de archivo y conectarse a Internet, ordenes de impresión a gran escala, se produce la congestión de red. Esto puede dar como resultado tiempos de respuesta más lentos, transferencias de archivos más largas y usuarios de red menos productivos debido a los retardos de red. Para aliviar la congestión de red, se necesita más ancho de banda o bien, el ancho de banda disponible debe usarse con mayor eficiencia.

Con la segmentación de la red se logrará:

- Optimizar el ancho de banda
- En cada segmento de red disminuir el broadcast (difusión).
- En cada segmento reducir el dominio de colisiones.
- En cada segmento de red crear una conexión directa entre el emisor y el receptor para disminuir la sobre carga en el tráfico.

En este ámbito surge la necesidad de dividir la red en unidades denominadas segmentos. Cada segmento usa el protocolo de Acceso múltiple con detección de portadora y detección de colisiones (CSMA/CD) y mantiene el tráfico entre los usuarios en el segmento. Al utilizar segmentos en una red, hay menos usuarios/dispositivos que comparten el mismo ancho de banda al comunicarse entre sí dentro del segmento. Cada segmento se considera como su propio dominio de colisión.

En este aspecto la segmentación se realizará incorporando switchs de mejores características a los actuales que están incorporados a la red, con esto se logra

implementar VLANS para la red de datos como se encuentra actualmente, mas la red de cámaras con el servidor de video que generan trafico multimedia.

1.8.8 USUARIOS DE MONITOREO

Las políticas de acceso y control al sistema de cámaras depende del nivel de usuario y al grupo que pertenece de a cuerdo a los permisos establecidos y configurados en el sistema, se ha identificado los siguientes usuarios:

- Departamento de Seguridad
- Jefe de Seguridad y Gerencia
- Inspección General

CAPITULO 2: DISEÑO DEL MODELO DE MONITOREO Y SEGURIDAD

2.1 FACTORES DE SEGURIDAD

El colegio cuenta con el departamento de seguridad que es el encargado directo de controlar y vigilar tanto los bienes muebles, estudiantes, áreas de acceso al establecimiento, cuenta con nueve integrantes y un jefe de seguridad, este departamento son los responsables de coordinar, dirigir y hacer las cumplir las diferentes normas y políticas al entorno de la institución. Además se debe mencionar que la institución cuenta con personal de mantenimiento y aseo que elabora en jornada tarde y noche.

SEGURIDAD ESTUDIANTIL

El estudiantado es el recurso de más importancia dentro de la seguridad del colegio, especialmente la sección preescolar y primaria desde 2EGB⁶ hasta 4EGB por motivos que en ocasiones se han suplantado falsos representantes que van a recoger a los niños al colegio después de la jornada estudiantil y que luego son motivo de extorsión hacia los padres.

Conjuntamente con el departamento de inspección general se coordina los respectivos permisos o salvo conductos para que los estudiantes puedan abandonar el recinto estudiantil, esto es previa autorización con los respectivos representantes o padres familia cuya autorización pueden hacer llegar vía email, fax o llamada telefónica, generalmente está autorización se lo debe realizar antes del medio día.

El personal de seguridad asignado para la entrada principal (Garita) del establecimiento consta de dos guardias, quienes son los encargados de controlar las autorizaciones de salida de cada estudiante y verificar de forma responsable que

⁶ Segundo año de Educación General Básica

Una persona lo acompaña al momento de abandonar el establecimiento especialmente al término de la jornada estudiantil. El procedimiento anterior se genera exclusivamente con los estudiantes que salen del colegio y que por distintas razones no toman bus de recorrido.

TRANSPORTE ESTUDIANTIL

El colegio cuenta con buses de recorrido estudiantil para cada sector de la ciudad, esta cooperativa de buses no es propia de la institución es subcontratada, cada bus cuenta con una inspectora que tiene a su cargo cierto número de estudiantes y que cuya función es la de controlar que los estudiantes asignados a su respectivo número bus puedan embarcarse y llegar a su destino final. Es necesario recalcar que las inspectoras de los buses forman parte del personal de la institución y que conjuntamente con los conductores de los buses tienen asignados su respectiva identificación.

Los inconvenientes en este punto surgen cuando una inspectora notifica a última hora que por diversas circunstancias no puede arribar al colegio y en su lugar envía a otra persona sin el conocimiento de las debidas autoridades. Otro de los factores sucede de igual forma cuando los buses tienen algún desperfecto y no son operables razón por la cual se debe requerir otra unidad que viene a veces con un conductor desconocido, este hecho empeora la orientación de los estudiantes especialmente de los pequeños que por error toman buses equivocados y al respecto en muchos de los casos no existe ninguna notificación a este problema.

SEGURIDAD EN EL PERIMETRO DEL COLEGIO.

Generalmente en horas de noche a existido intento de intrusiones hacia las instalaciones del colegio en la zona donde está ubicado el estadio. Por la falta de vigilancia, el personal de seguridad tiene asignado horarios o turnos durante las 24 horas del día, la mayor parte de personal obviamente está asignado en la jornada laboral. En la noche se asigna el 30 % del personal, que generalmente realizan rondas de vigilancia cada dos horas, esto implica una falla de seguridad

bastante crítica debido a la extensión geográfica con la que cuenta el plantel que aproximadamente son 3 hectáreas. En esta zona la parte más crítica es el sector lateral norte del estadio que ha sido el lugar vulnerable en donde se ha detectado intentos de intrusiones

SEGURIDAD PREESCOLAR.

El personal de seguridad asignado a esta sección tiene la responsabilidad de vigilar y supervisar la integridad de los estudiantes más pequeños cuyas edades están comprendidas entre 4 y 6 años de edad. La mayoría de los niños en esta sección después de la jornada estudiantil son recogidos por sus padres o representantes, los inconvenientes surgen cuando el personal de seguridad asignado no tiene el suficiente control de la situación por diversas razones.

SEGURIDAD ENTRADA PRINCIPAL (GARITA).

El personal asignado a esta área es la encargada de tener un registro de todas las personas que ingresan o salen de la institución, en este registro consta el nombre de la persona que ingresa, la identificación, la fecha, hora de entrada y salida, al lugar o departamento donde se dirige, el nombre de la persona con quién se va a reunir. En circunstancias donde la aglomeración de personas es intensa se cumple este procedimiento pero es imposible saber con certeza la identificación física de la persona que entró a una hora determinada.

Seguridad puerta de acceso a parqueaderos y estacionamientos.

El ingreso de vehículos es constante tanto en la mañana como en la tarde cuando se da el inicio y fin de la jornada estudiantil, es difícil para el personal de seguridad en ese momento saber que el vehículo que está ingresando es de algún padre de familia, también la dificultad de tomar la placa del vehículo o el nombre del conductor, en esta situación ciertos vehículos no salen del parqueadero acción que se toma en cuenta después de buen lapso de tiempo.

2.2 SEGURIDAD DE LOS BIENES MUEBLES.

2.2.1 SEGURIDAD DE LOS CASILLEROS.

En los pasillo del colegio están ubicados los casilleros para cada estudiante tanto para la sección de primaria como la de secundaria, cada casillero consta de un número de identificación que se le asigna al estudiante, por su parte cada dueño es el responsable de traer un candado y su llave para guardar sus libros, ropa de deporte etc.

2.2.2 SEGURIDAD EN LOS LABORATORIOS DE CÓMPUTO.

En los laboratorios de cómputo se dan casos de sustracciones de Mouse, rayado de pantallas, pérdida de celulares, sustracciones de teclas de los teclados, roturas de los lectores ópticos, sustracciones de memoria RAM, desconexiones de los cables, maltrato de los CPU. Estos problemas cusan mucho malestar en el uso de las instalaciones y también pérdidas económicas.

2.2.3 SEGURIDAD EN LAS OFICINAS

En secretaria académica consta toda la documentación relacionada a cada estudiante como son notas, pases de año, documentos relacionados con el Ministerio de Educación, en fin documentos relacionados a la institución.

En colecturía contabilidad este departamento maneja la parte financiera del colegio, como el pago de pensiones que realizan los padres, ingreso egreso de facturas, pago a proveedores, flujo de caja chica etc.

2.2.4 SEGURIDAD EN CAFETERIA.

Las sucesivas desapariciones de los productos de expendio, maltrato de máquinas surtidoras de alimentos y bebidas lácteas, rompimiento de mesas y sillas, son las situaciones que se presenta cuando existe aglomeración de estudiantado particularmente en los recreos, es difícil determinar al responsable o

responsables de estos actos. En la tarde y noche han existido sustracciones de dinero que de igual forma ha resultado difícil determinar al responsable.

2.3 ANÁLISIS DE UBICACIÓN DE CÁMARAS.

Para realizar un monitoreo de las diferentes áreas del campus del colegio se ha tomado en cuenta las siguientes referencias.

La cantidad de cámaras instaladas deben permitir un monitoreo adecuado, es decir el número de cámaras no debe ser excesivo.

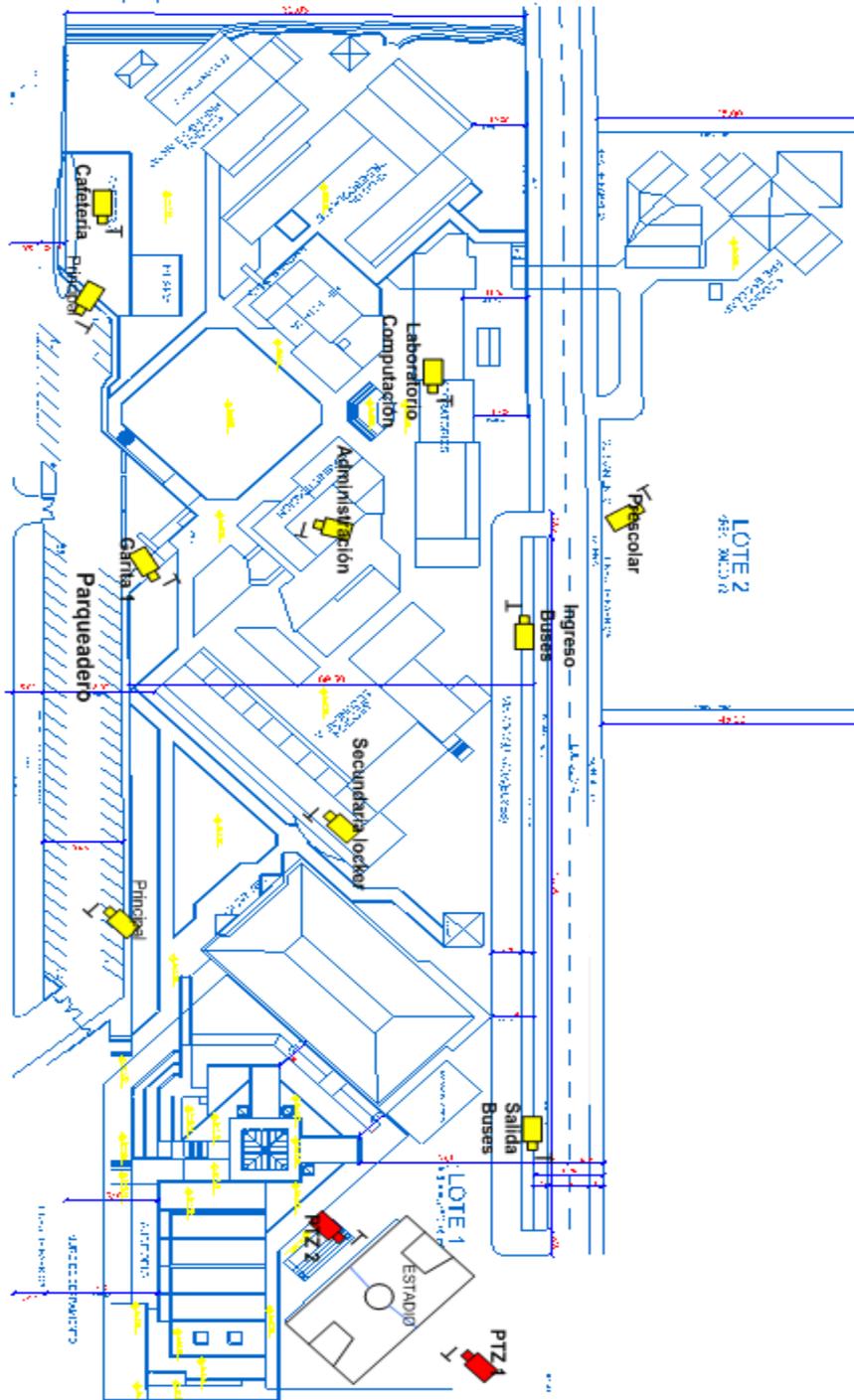
La mayor parte de cámaras se instalarán en áreas de acceso, ingreso de puertas principales, zonas de circulación.

Analizados los puntos críticos donde se necesita que el sistema de cámaras ayude a incrementar la seguridad la ubicación de cámaras se tiene:

TABLA 2.1 UBICACION DE CAMARAS (REFERENCIA)

UBICACIÓN	NÚMERO DE CAMARAS
PREESCOLAR	1
ENTRADA DE BUSES	1
SALIDA DE BUSES	1
LABORATORIOS COMPUTO	2
GARITA	1
CAFETERIA	1
LOKERS SECUNDARIA	1
PARQUEADERO	1
ADMINISTRACIÓN	1
ESTADIO	2

Grafico 2.1 Ubicación de cámaras

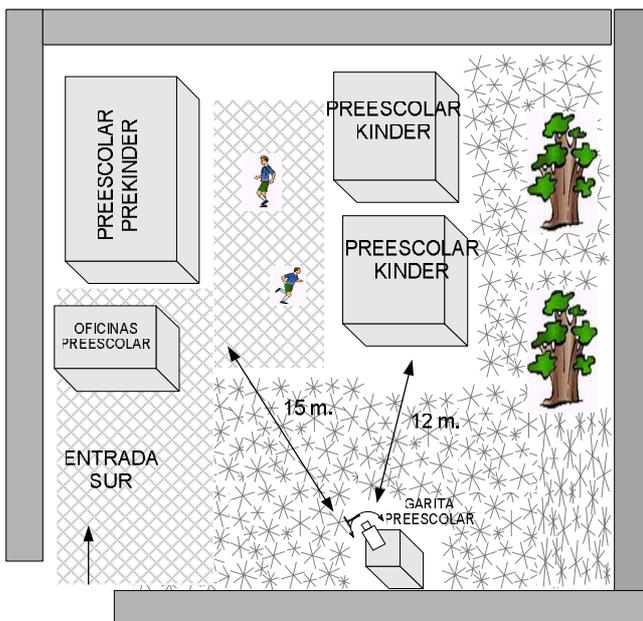


2.3.1 PREESCOLAR.

Esta cámara debe estar ubicada en la garita de esta sección, con esta se cubre el acceso a preescolar, aulas y espacio de juegos.

Para esta cámara el cable debe salir desde el rack del laboratorio de computación, se debe realizar el tendido de tuberías desde esta sala hasta la garita y la instalación de canaletas.

Gráfico 2.2 Cámara Preescolar (referencia)



2.3.2 ENTRADA - SALIDA DE BUSES.

Se ubicarán dos cámaras una con dirección a la puerta de entrada de buses y otra con dirección a la puerta de salida de buses.

El tendido de cables para estas cámaras deben instalarse desde el rack de la oficina de inspección general

2.3.3 LABORATORIO CÓMPUTO.

El tendido de cable de estas cámaras se conectará desde el cuarto de servidores a cada uno de los laboratorios. Estas cámaras deben tener la propiedad de poder realizar zoom.

2.3.4 GARITA (Entrada Principal)

La ubicación de esta cámara debe cubrir la puerta peatonal, y la parte de la ventana de recepción de documentos para poder ingresar al plantel. La conexión de esta cámara se la debe realizar desde el rack ubicado en administración. La característica de este dispositivo debe permitir zoom de las imágenes monitoreadas.

2.3.5 CAFETERÍA

Esta cámara debe tener una cobertura de 360 grados ubicada en la parte central de la cafetería, donde se puede visualizar los puntos críticos a ser monitoreados, además esta cámara tiene la propiedad de ser una cámara oculta. También la capacidad de detección de movimiento y que sea día noche con zoom, la instalación se realizará desde el rack ubicado en oficina de primaria.

2.3.6 CASILLEROS SECUNDARIA

Esta cámara se debe ubicar en la parte superior del pacillo de las aulas de secundaria donde están los casilleros. El cable para esta cámara debe ser instalado desde el rack de secundaria, esta cámara debe tener la propiedad de poder realizar zoom de las imágenes monitoreadas y zoom de las imágenes grabadas.

2.3.7 PARQUEADERO DE ENTRADA.

La primera cámara se ubicará en la parte norte a la altura de cafetería.

La segunda cámara en la parte sur a la altura de la puerta norte de entrada de vehículos.

Estas cámaras cubrirán toda el área de parqueaderos, puertas de ingreso y salida de vehículos, se debe realizar el tendido de tuberías, cableado, hasta los dos lugares donde se ubicarán las cámaras.

2.3.8 ADMINISTRACIÓN

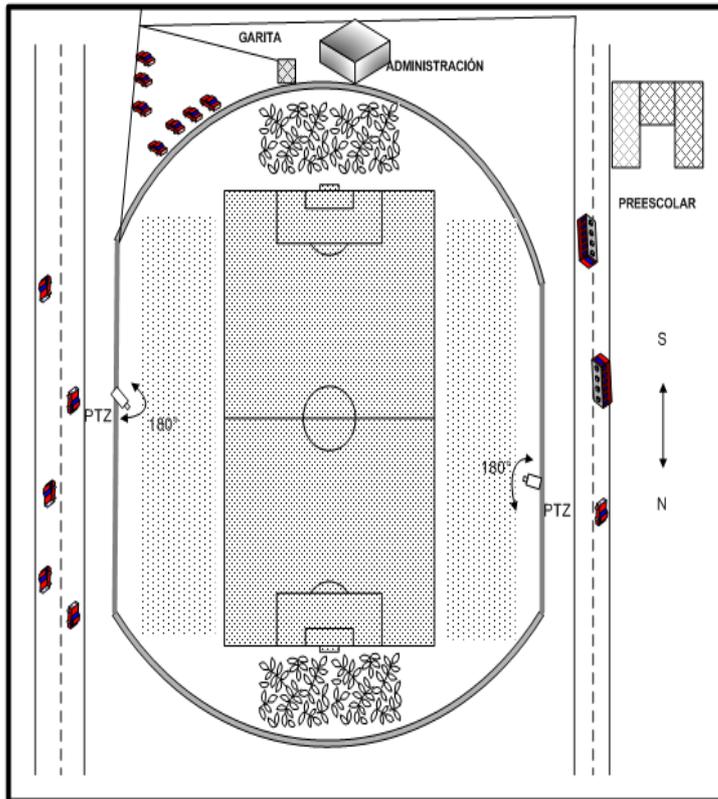
De igual forma la ubicación de esta cámara debe estar en la parte central de administración que tiene cobertura a las puertas de acceso a las diferentes oficinas, especialmente a Colecturía, la característica de ésta cámara es que debe tener una cobertura de 360 grados, zoom, día noche, oculta.

La instalación se llevará a cabo desde el propio rack de administración.

2.3.9 ESTADIO.

Esta zona es bastante amplia, para lo cual se ha visto la posibilidad de instalar dos cámaras PTZ con ángulos de 180 grados una en frente de la otra, con las características día noche, zoom, detección de movimiento, la instalación se lo realizará desde el rack ubicado en gimnasio, esta cámara debe ser ubicada en la parte superior del auditorio.

GRAFICO 2.3



Presentar gráficos o fotos de las coberturas

2.4 OBRA CIVIL

Para la realización de la obra civil se requiere del personal de mantenimiento del establecimiento (3 o 4 personas) para ejecutar el tendido de cable por los ductos existentes a los distintos puntos donde se instalarán las cámaras.

Para el tendido de cable, instalación de canaletas y conectorización se requiere de al menos dos personas.

En las pruebas iniciales y puesta a punto de cámaras se trabajará con una persona.

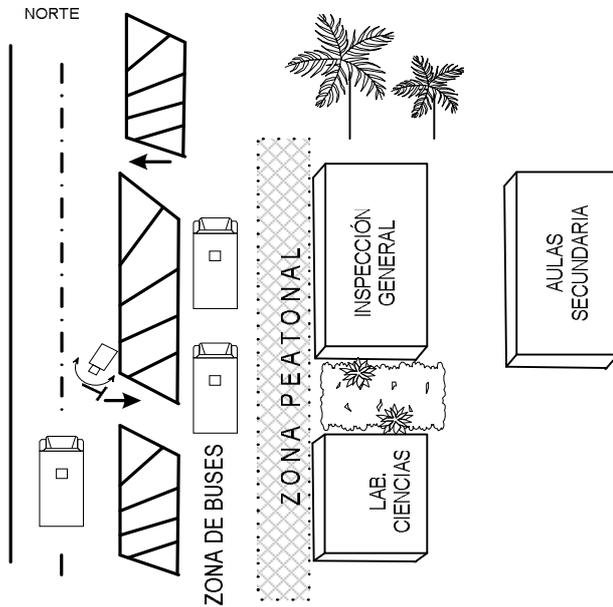
Instalación y configuración del servidor de cámaras.

Para esto se deben realizar tareas como: abertura de zanjas para tubería, construcción de pozos de revisión, instalación de tubería y cableado (video y eléctrico), instalación de canaletas, tendido de cable, instalación de cajetines, prueba de cámaras, instalación y manejo de software, puesta en funcionamiento del sistema de cámaras.

En el gráfico 2.4 se puede observar la ubicación de la cámara para el área de ingreso de buses, está ubicada en la parte superior de la pared, la misma tiene una altura de 2.30m. en la superior de la pared se instaló un pedestal para poder subir la altura de la cámara, la altura total se ubicó en los 2.90 m desde el piso.

El ángulo de de ubicación corresponde a 30 grados noroeste, con este ángulo se logra visualizar perfectamente los buses que entran a la zona de embarque del colegio y poder confirmar efectivamente el número de la unidad correspondiente y a su conductor, adicionalmente se realizó el cableado de tendido eléctrico para poder energizar a la cámara y con juntamente con esta tarea se realizó el tendido del cable UTP desde el centro de cómputo hasta el sitio donde se ubica la cámara.

Gráfico 2.4 de ubicación cámara para la zona entrada de buses



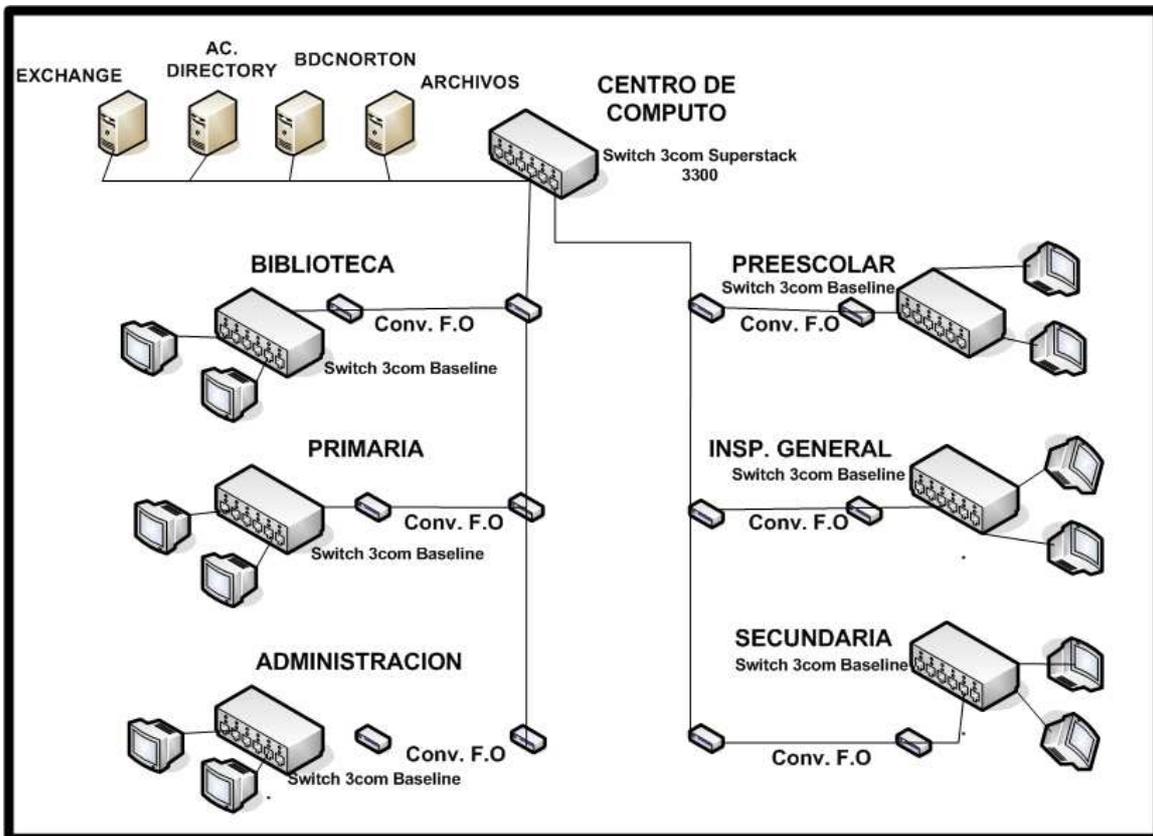
2.5 DISEÑO DE SEGMENTACION DE LA RED

2.5.1 DISEÑO Y OBJETIVOS DE LA ARQUITECTURA DE RED

La red LAN de la institución consiste en un conjunto de hardware y software compartido, utiliza la topología en estrella, toda la transmisión que se genera en el medio es de tipo broadcast (difusión), es decir que la transmisión que se genera por parte de una estación de trabajo puede ser escuchada por cualquier otra estación, de modo que una transmisión realizada desde un dispositivo se puede recibir en los restantes dispositivos conectados a la red.

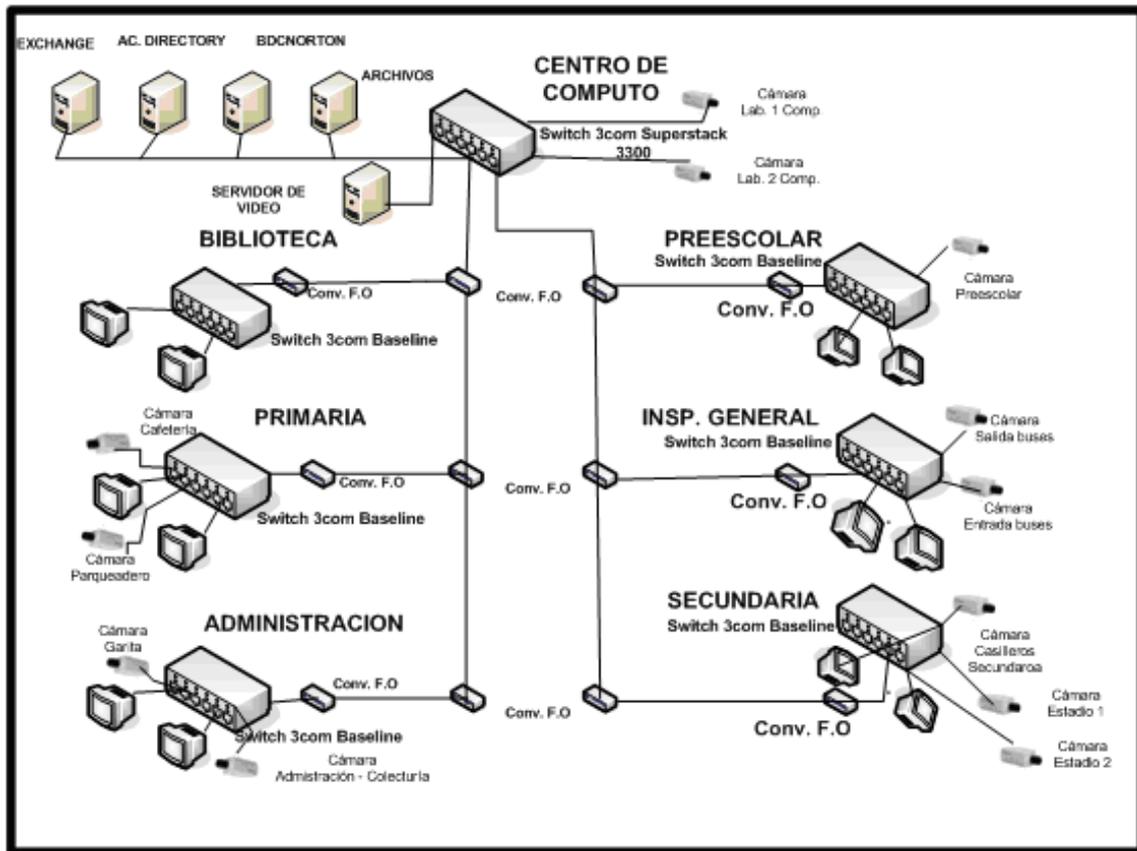
El gráfico 2.5 se puede observar el esquema de la red de la institución educativa con los respectivos elementos de conectividad que conforman la red, en este esquema el diseño no incluye el tráfico de video es decir las cámaras IP.

Grafico 2.5 Red de Computadores de la Institución



En base a la infraestructura actual de la red se requiere instalar cámaras de tecnología IP. Con el incremento de las aplicaciones multimedia mas los servicios anteriormente descritos en el capítulo anterior, varias aplicaciones compartirán el mismo canal. Los archivos más pesados como el video y sonido, los programas ejecutables en DOS, requieren aún una mayor capacidad de transmisión, necesitan todo el ancho de banda disponible. En el gráfico 2.6 se indica un esquema de la red con la incorporación de cámaras IP

Grafico 2.6 Con Cámaras IP.



Con el aumento de dispositivos en la red es probable que aumente el número de colisiones, conforme aumenta el número de colisiones disminuye el rendimiento de la red ocasionando congestionamiento y disminución de la velocidad degradando el ancho de banda.

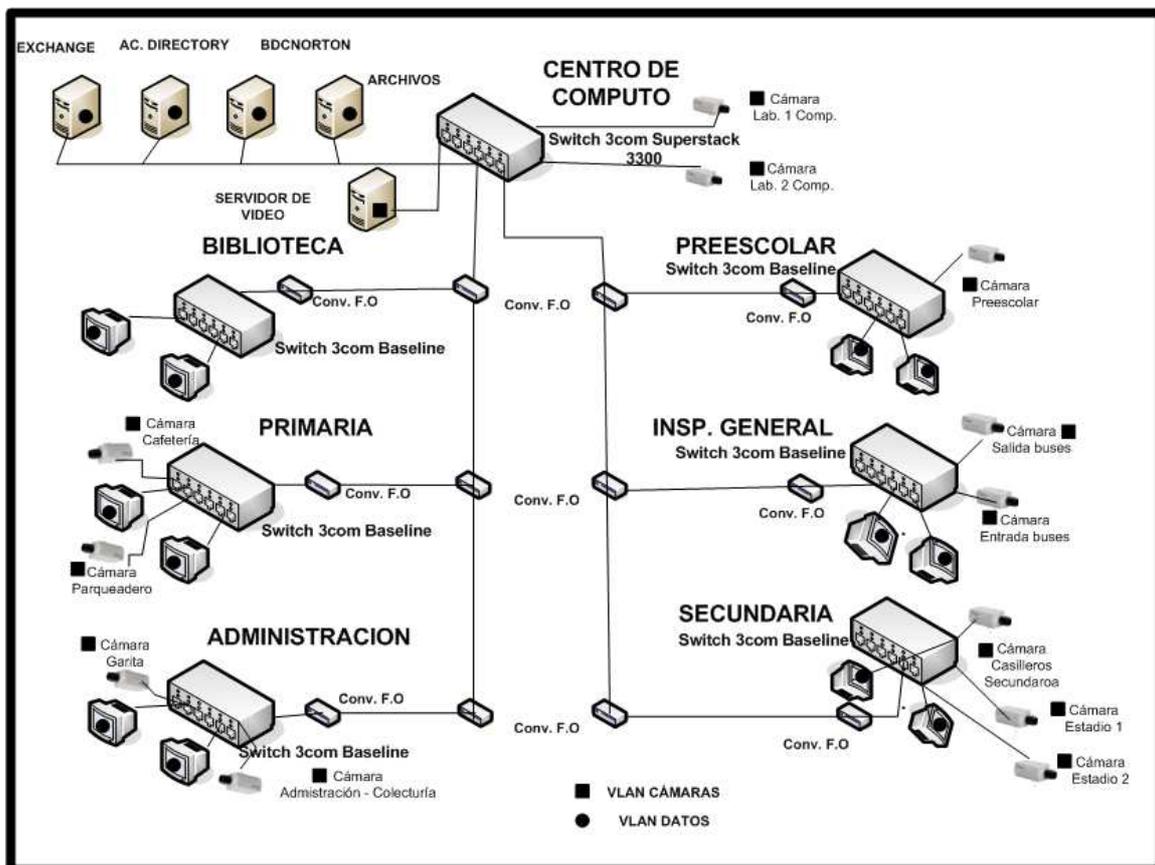
.En el grafico 2.7 se puede observar el segmento de red creado para el trafico de video, asignando un ancho de banda dedicado a cada dispositivo reduciendo así los cuellos de botella, si un dispositivo envía un mensaje a otro de la red mediante un conmutador (switch) este solo será enviado al equipo receptor y no a toda red como lo hacen los Hubs, evitando así colisiones en ese instante con otros equipos de la red.

El diseño que se plantea para segmentación de la red es flexible, ya que usa las tecnologías VLAN para optimizar la red de datos y el tráfico de video. Las VLAN principales o segmentos de red que atienden a los distintos requisitos de tráfico del servidor son:

- La red de infraestructura de datos
- El sistema de cámaras o tráfico de video
- Administración del flujo de tráfico

Esta opción de segmentar la red permite administrar el tráfico de forma eficaz gracias a la creación de una serie de directivas de seguridad a las que es posible aplicar reglas.

GRAFICO 2.7 CREACION DE VLAN



DISPONIBILIDAD DE LA RED

La disponibilidad de la red puede mejorarse si se logra la redundancia en todos los niveles y se utiliza conmutación automática tras error. Dentro de cada nivel de la arquitectura se incluyen dos dispositivos de red para lograr una gran disponibilidad en el nivel de red. Si un servidor de seguridad deja de funcionar, otro de reserva asume su función. Si un conmutador no funciona, otro se ocupará de toda su carga hasta que se repare. Si el adaptador de red de un servidor Web presenta un error, otra NIC se activa automáticamente, sin que el flujo de tráfico se vea afectado. Si un servidor Web no funciona, se puede poner fuera de conexión, reparar y agregar de nuevo a la matriz Web sin afectar a la producción.

ESCALABILIDAD DE LA RED

El tráfico de red es cada vez menos predecible, el diseño de la red contempla nuevas tecnologías, como dispositivos de Nivel 2 y Nivel 3 que conmuten y enruten el tráfico a la velocidad que permita el hardware. Los switch modulares y apilables ofrecen una densidad de puertos y velocidades de hasta 100 Mega bits por segundo (Mbps). Estos dispositivos también aportan soluciones para los centros de datos de comercio electrónico en las que los conmutadores pueden combinarse con vínculos Ethernet (1000 Mbps) Giga bits e incluir miles de puertos de alta velocidad.

La mayor disposición de ancho de banda para los servidores se consigue a través de múltiples tecnologías de adaptador que eliminan los cuellos de botella del servidor al permitir aumentar de forma gradual el ancho de banda entre un servidor y un conmutador. Estas tecnologías hacen posible una transmisión a alta velocidad que sobrepasa la capacidad del medio físico.

2.5.2 SEGMENTACIÓN

Un switch es un dispositivo de propósito especial diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch puede agregar mayor ancho de banda, acelerar la

salida de paquetes, reducir tiempo de espera y bajar el costo por puerto. Opera en la capa 2 del modelo OSI y reenvía los paquetes en base a la dirección MAC. El switch segmenta económicamente la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final. No están diseñados con el propósito principal de un control íntimo sobre la red o como la fuente última de seguridad, redundancia o manejo. Al segmentar la red en pequeños dominios de colisión, reduce o casi elimina que cada estación compita por el medio, dando a cada una de ellas un ancho de banda comparativamente mayor. Con los switches se crean pequeños dominios, llamados segmentos, la microsegmentación se realiza conectando cada estación de trabajo y cada servidor directamente a puertos del switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

Una de las ventajas que se pueden notar en las VLAN es la reducción en el tráfico de la red ya que solo se transmiten los paquetes a los dispositivos que estén incluidos dentro del dominio de cada VLAN, una mejor utilización del ancho de banda y confidencialidad, alta performance, reducción de latencia, facilidad para armar grupos de trabajo.

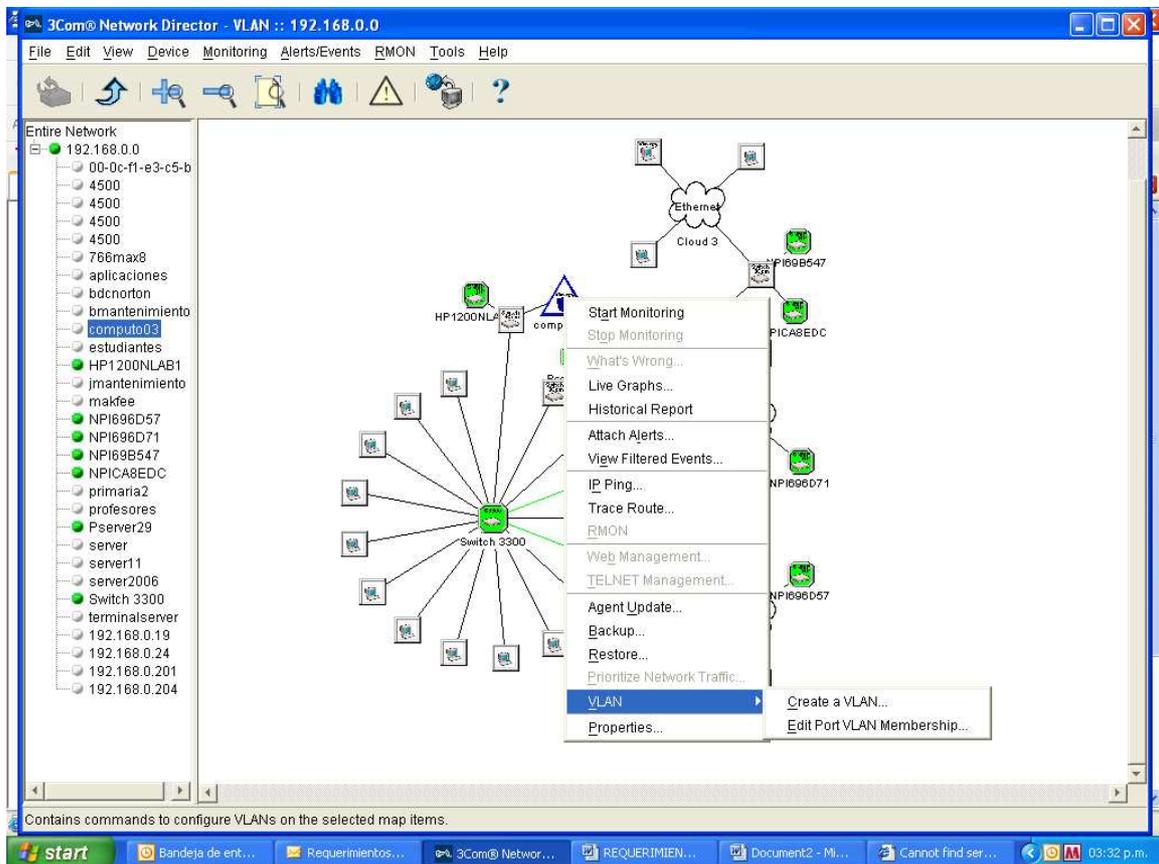
2.5.3 CONFIGURACIÓN DE LAS VLANS.

La configuración se realiza por medio de puertos o direcciones IP utilizando el software de 3com Network Director como se indica a continuación.

En el gráfico siguiente se muestra la información relacionada con la red al momento de ejecutar el software de 3 com.

Mediante el asistente se empieza a crear las vlans, el primer paso consiste en seleccionar los dispositivos que conformara la vlan, usando clic derecho seleccionar la opción VLAN luego CREATE VLAN, en esta opción escriba el nombre de la vlan a ser creada y la vlan ID. El nombre el ID es la identificación necesaria que se utilizará para cada switch seleccionado.

El nombre asignado a la vlan puede tener una longitud de 32 caracteres, el campo vlan ID es utilizada por los switches de la red para identificar a cada vlans creada.



Las vlans son grupos lógicos de dispositivos que están en cualquier lugar de la red las cuales se comunican si están en el mismo segmento físico, con la vlans se puede segmentar la red de acuerdo a:

- Grupos departamentales. Se crear una o varias vlans de acuerdo a grupo departamentales como por ejemplo una vlan para el administración, otra para la sección primaria, para secundaria, etc.
- Grupos de usuarios. Se pueden crear vlans para usuarios de email y para usuarios multimedia.
- Grupos de jerarquía. Se puede crear vlans para directores departamentales, para profesores, estudiantes.

BENEFICIOS DE LAS VLANS.

- Provee un sistema de segmentación de red que es más flexible que una red tradicional, si un usuario es movido a otro sitio de trabajo las direcciones de cada estación son actualizadas manualmente con las vlans solo es necesario mover el puerto.
- Las vlans ayudan al control de tráfico, incrementan la eficiencia de la red porque las vlans contienen un conjunto de dispositivos que se comunican entre ellos, si existe un paquete de broadcast, multicast o una dirección de destino desconocida dentro una vlan, el switch reenvía el paquete dentro de los puertos de la vlan .

VLANS BASADAS EN PUERTOS.

Es una colección de puertos basadas entre uno o más switches que son configurados como miembros de una misma vlan.

Por Puerto Se configura por una cantidad "n" de puertos en el cual podemos indicar que puertos pertenecen a cada VLAN. Por ejemplo en el Switch se configuran los puertos de los cuales el 1,5 y 7 pertenecen a la VLAN 1; el 2, 3 y 8 a la VLAN 2 y los puertos 4, 6 y 9 a la VLAN 3.

VLANS BASADAS POR DIRECCION IP.

Mediante la dirección IP de cada dispositivo de la red se puede seleccionar y configurar una vlans en base a esos dispositivos

En algunos switches manejan el concepto de IP primaria y secundaria para determinar como el switch procesa el trafico de broadcast y multicast que recibe una vlan desde múltiples interfaces IP.

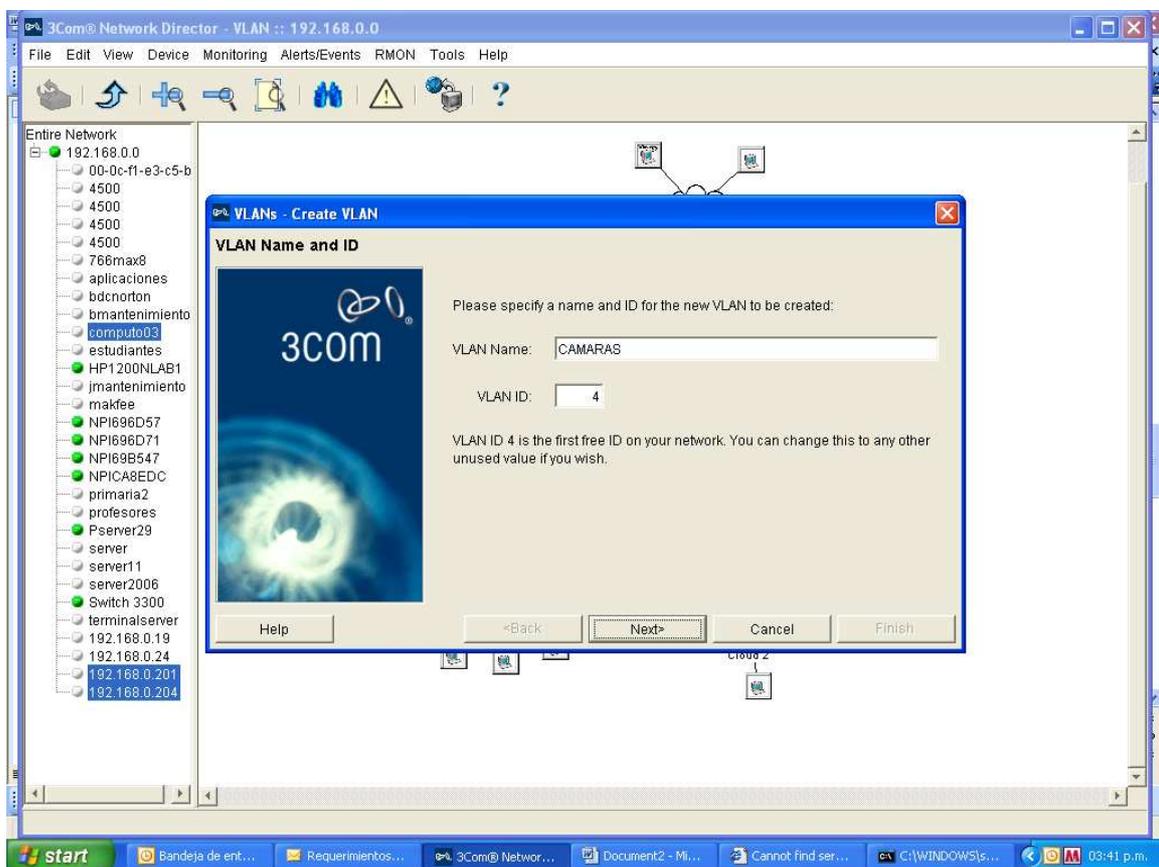
CREACION DE VLANS.

Se considera que no existe ninguna vlan creada, con ayuda del software de 3 com (Network Director) se empieza a realizar un descubrimiento de la red dando como resultado la siguiente información de soporte:

Descripción de la VLAN, en este caso toda la red como una sola vlan

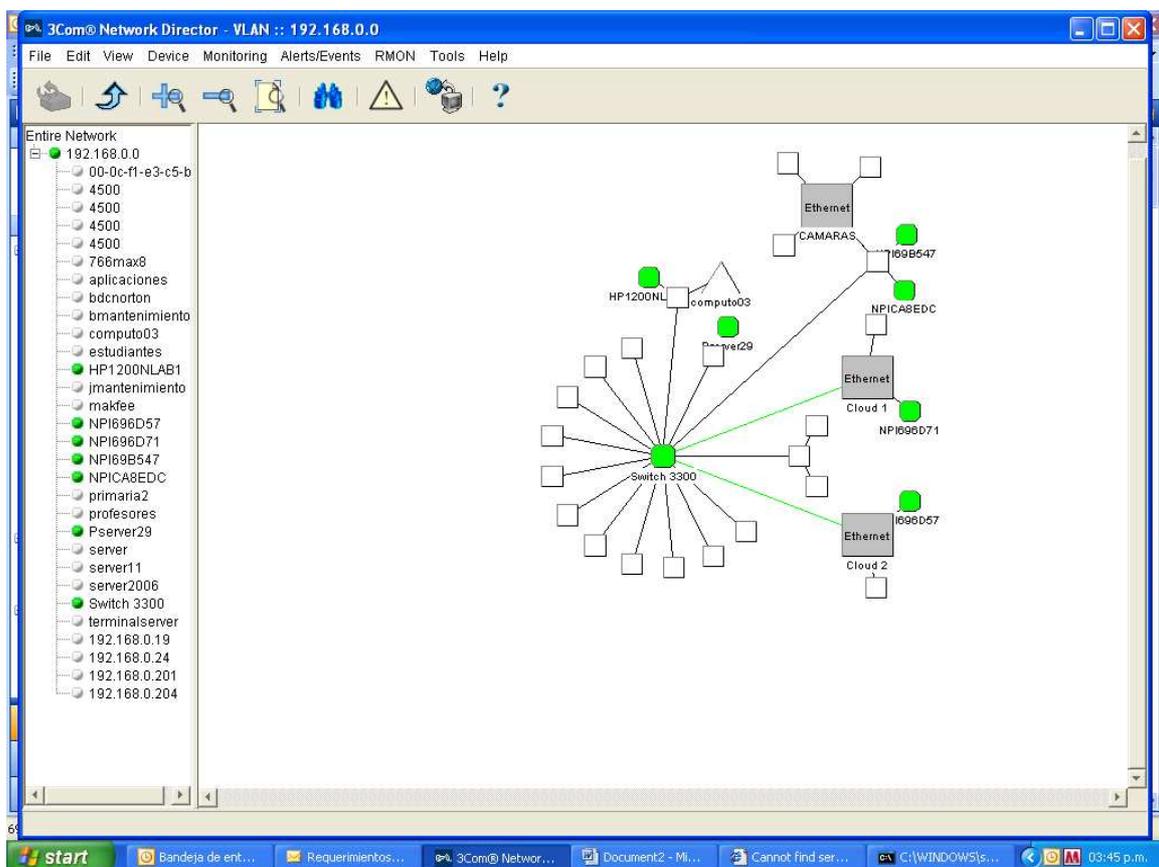
- Los tipos de switches
- Direcciones IP
- Los puertos de la vlans que la conforman.

En la pantalla siguiente se despliega una lista de switches que están instados en la red, cada switch consta de un número de puerto en los cuáles las vlans serán creadas, las siguientes reglas son usadas para decidir cuales puertos del switch son listados en esta opción.



- A cada switch le corresponde un número de puerto y todos los puertos conectados a otros switches son desplegados en la lista.
- 3com network director busca todos los puertos de los switches cercanos y los añade a lista.
- Para modificarlos nombres del switch el puerto seleccionar el botón CHANGE SELECTION.
- Una vez seleccionados todos los switches y los puertos requeridos seleccionar los dispositivos que formarán parte de la valan, antes de finalizar el asistente en el menú FILE salvar este proceso, 3 com network director realiza un chequeo de todos los puertos seleccionados e identificados en cada de los switches para evitar inconsistencias.

VISUALIZACION DE VLANS



CONECTIVIDAD DE LA VLAN.

En un ambiente IP la comunicación de la Vlan y entre Vlans se consigue definiendo vlans con las direcciones IP estableciendo comunicación entre los dispositivos asignados a la vlan y con dispositivos asignados a otras vlans. La mayoría de los switches actuales son de capa 3 que ayuda a un mejor rendimiento de la red y comunicación entre vlans.

La comunicación que se hace entre switches para interconectar VLANs utiliza un proceso llamado Trunking. El protocolo VLAN Trunk Protocol (VTP) es el que se utiliza para esta conexión, el VTP puede ser utilizado en todas las líneas de conexión incluyendo ISL, IEEE 810.10. IEEE 810.1Q y ATM LANE.

2.6 TECNOLOGIAS DE TRANSPORTE DE VIDEO

Para la transferencia de archivos de video se utilizan varias tecnologías, dos de las utilizadas son local caching y response spoofing.

File Caching. Esta operación proporciona almacenaje de información local, localización que puede ser usada como almacén temporal antes que los archivos sean enviados en la red. The caching hardware puede ser simplemente el uso de la memoria RAM, pero para archivos de video la opción es en discos de almacenamiento.

En el gráfico 2.8 muestra una operación básica del sistema caching, en este ejemplo el usuario A-1 necesita enviar un archivo al usuario B-1 sobre la red de área local.

Todas las estaciones de trabajo están a la red LAN a 100 Mbps, el dispositivo caching también está conectado a la misma red y a la misma velocidad.

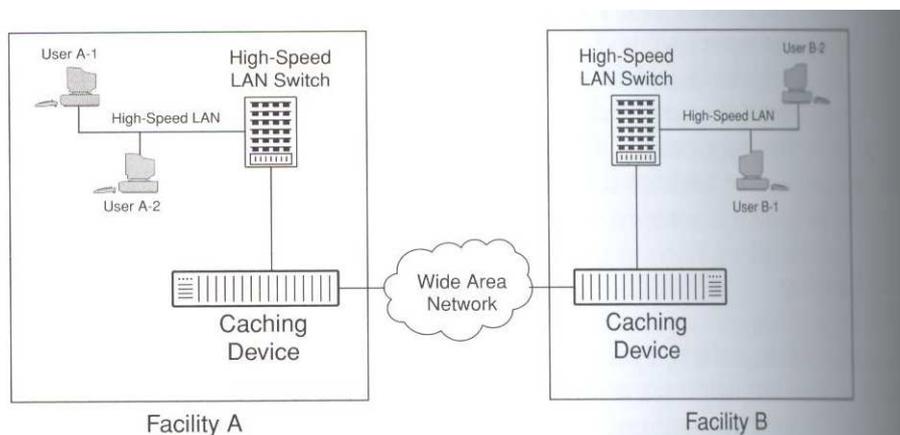
El primer paso para transferir el archivo de video es copiarlo desde la estación de trabajo del usuario A-1' al caché del dispositivo en la ubicación A.

A partir de esto este proceso toma lugar sobre la red de alta velocidad dentro de A, esto aumenta rápidamente, el caché del dispositivo A necesita tomar contacto con el caché del dispositivo B, una vez que la conexión se ha establecido entre las dos caché, entonces los datos comienzan a ser transmitidos, este proceso toma cierto tiempo dependiendo del ancho de banda disponible en la WAN entre los límites de velocidad de A y B de los datos a transferirse.

Después que la transferencia se ha completado, el archivo puede ser enviado desde el caché del dispositivo B al usuario de la estación de trabajo B-1 dentro de su propio espacio de red Facility B.

El dispositivo de caché no necesita ser un dispositivo especial de hardware, puede ser simplemente una estación de trabajo equipada con dos tarjetas de red y software especializado.

GRAFICO 2.8 Transporte de video



Simpson, Wes. Video Over IP [Practical Guide to Thecnology] S. Merril Weiss

Se debe tomar en cuenta que la mayoría de las tecnologías WAN son bidireccionales por tanto se podrá tener la transferencia de archivos desde el usuario B-2 al usuario A-2. mientras que los dispositivos cahing son un conjunto de manejadores, los datos a ser transmitidos en la WAN pueden ser

simultáneamente en ambas direcciones, mientras que el tiempo transmitido en la red ocurre debido al embotellamiento en la WAN, permitiendo a cada dispositivo caché enviar y recibir datos ayunado a mejorar la operación del sistema.

TCP SPOOFING.

Es una técnica utilizada para incrementar el throughput de las conexiones TCP debido al excesivo retardo en la red. Spoofing opera interceptando paquetes, que son transmitidos y enviando el acknowledgments⁷ al transmisor con anticipación, cuando los paquetes normalmente son enviados por el receptor. Esta es una técnica conveniente para el exceso de transmisión de gran cantidad de archivos de datos sobre la conexión que causa retardo.

Para obtener una apreciación de cómo spoofing trabaja, se necesita comprender como TCP crea un camino seguro para los datos que se obtienen desde los datos del remitente a los datos del receptor en una red IP.

TCP usa “handshaking” para permitir que en los dos extremos la comunicación sea un éxito o fracaso de los paquetes transferidos. Handshaking es el medio donde el emisor espera del receptor el acknowledge de la recepción de los datos periódicamente, el receptor usa estas respuestas rápidamente para enviar más datos.

Una buena analogía de esto pasa frecuentemente cuando una persona da cierta información a otra en una conversación telefónica como un número de teléfono o el número de la tarjeta de crédito, típicamente una persona comenzará diciendo los tres primeros dígitos o los cuatro dígitos del número en forma pausada mientras que el oyente construye una respuesta apropiada. En esta conversación las personas pudieran decir cualquier cosa para confirmar lo que se están diciendo el uno al otro, en estas circunstancias cuando una de las personas recibe la información es el turno de la otra persona para seguir enviando la siguiente parte de información en este caso los siguientes dígitos de la tarjeta pausado por otro acknowledgment y continua este

⁷ Es una señal de respuesta que indica que ciertos datos llegaron al destino sin errores

Proceso mientras se completa la información total y se cierre la comunicación. TCP handshaking es parecido a este proceso.

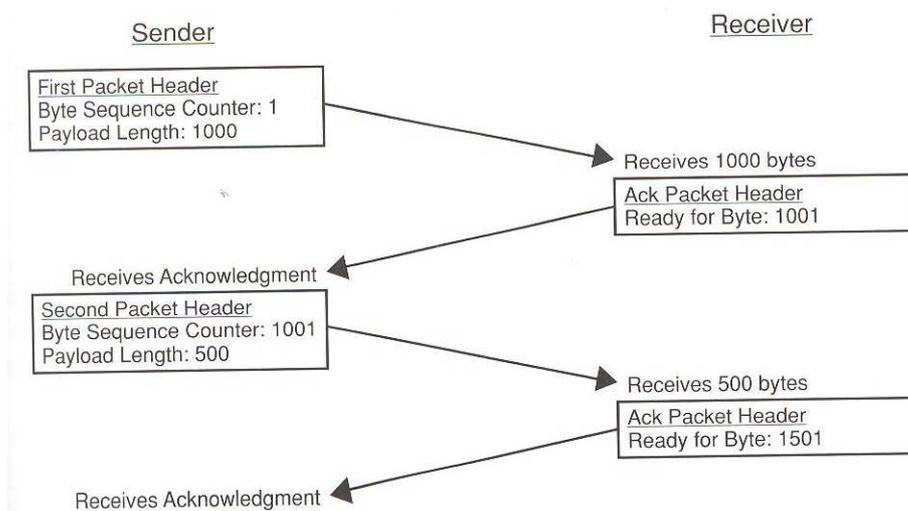
En TCP cada byte de datos se asigna a una secuencia de números para ser enviados, en cada transmisión de paquetes el número de secuencia es el primer byte de datos contenido en el paquete incluido en la cabecera, este soporte es una de las particularidades de TCP.

El receptor puede ordenar cualquier paquete de datos que tiene que ser entregados con el mismo número de secuencia.

El receptor puede detectar si cualquier paquete falta o está perdido mirando el número de secuencia del paquete.

El receptor puede indicar al remitente cuáles bytes de datos tienen que ser recibidos y cuál es el próximo byte de datos que el receptor está listo para recibir.

En handshaking cada paquete de datos enviados por el receptor al remitente contiene un acknowledgment en la secuencia de números. Este número representa el número de secuencia del próximo byte que el receptor está listo para aceptar, en la figura se indica esta acción.

Grafico 2.9 Transmisión TCP

Simpson, Wes. Video Over IP [Practical Guide to Thecnology] S. Merril Weiss

En el intercambio de paquetes como indica la figura el remitente comienza enviando 1000 bytes de datos, con un 1 de número de secuencia, para indicar que el primer byte está contenido en este paquete. El receptor procesa estos datos y determina si está recibiendo los 1000 bytes de datos pero que en realidad son 1001 bytes, el receptor envía un paquete al remitente con el acknowledgment. Cuando el remitente obtiene el acknowledgment este conoce que puede ahora enviar el próximo paquete de datos, ahora si se envía 500 bytes, el remitente usa el número 1001 como secuencia, porque es el primer byte del nuevo paquete, cuando el receptor obtiene el segundo paquete este calcula que está ahora listo para recibir el número 1501 como número de secuencia y envía un acknowledgment para empezar el proceso. Cuando el remitente recibe este segundo acknowledgment este conoce que el primero de los dos paquetes se ha recibido correctamente.

En realidad el remitente está autorizado a enviar algunos paquetes de datos en hilera sin recibir un acknowledgment, pero la cantidad de datos a enviar no puede exceder el límite establecido por el receptor cuando se ha establecido una

conexión TCP. Por ejemplo se quiere enviar 8000 bytes, el remitente puede transmitir 8 paquetes cada uno con 1000 bytes pero este tiene que esperar por un acknowledgment enviado por el receptor.

Acknowledgment Delay.

El retardo puede tener un gran impacto en la velocidad de transferencia de los datos, si el retardo en la red entre el remitente y el receptor es de 100 milisegundos, el viaje completo (ida y vuelta) demoraría 200 milisegundos, usando 8000 bytes el remitente podría transmitir solamente los 8000 bytes una vez, después tiene que esperar por el primer acknowledgment, el cual podría arribar por debajo de los 200 milisegundos. Después del cual podría volver a transmitir otra vez. Entonces después los 8000 bytes fueron transmitidos, el remitente tendría que esperar otros 200 milisegundos por el acknowledgment, Todo este proceso podría repetirse cinco veces en un segundo, permitiendo cinco grupos de datos para ser enviados. Entonces cada grupo está limitado a 8000 bytes por el límite de la ventana del receptor, el máximo throughput posible en este proceso sería de 40000 bytes por segundo. En contraste de esta situación el viaje completo podría demorar 10 milisegundos, en este caso 100 viajes completos por segundo sería la posibilidad de incrementar a 800 Kbytes/sec, de throughput total a un factor de mejoramiento de 20.

El papel del dispositivo spoofing es enviar un acknowledgment al remitente más rápidamente antes que exista retardo en la red, el dispositivo spoofing necesita inmediatamente pasar por el destino pero necesita guardar una copia de los datos en un buffer local, en el instante entre que los datos se pierdan entre el dispositivo spoofing y el receptor los datos faltantes pueden ser retransmitidos desde el buffer y enviados nuevamente.

Show Start Flow Control.

Otra de las funciones de TCP es proveer un control de flujo entre datos del remitente y datos del receptor, el flujo de control es un medio seguro para

controlar de forma segura los datos del remitente, es importante cuando existe demasiada carga en la red proveniente desde otras fuentes de datos.

Flujo control opera en los datos del remitente y usa un acknowledgment proveniente desde el receptor. TCP normalmente usa un proceso llamado "empieza despacio" donde el remitente transmite una pequeña cantidad de datos y espera por un acknowledgment desde el receptor, si el acknowledgment viene rápidamente, entonces el remitente prueba enviando una cantidad grande de datos y continua aumentando la velocidad mientras la cadena se transporta con mucho tráfico y de forma segura para enviar. Este proceso es llamado "empieza despacio" porque el porcentaje inicial de datos es baja y va incrementando solamente cuando se ha determinado que la cadena y el receptor son capaces de manejar un porcentaje rápido de flujo de datos.

Slow Start es una operación normal de Internet en el día a día, pero puede satisfacer la demanda de archivos de gran tamaño como video que se necesita ser transferidos en una red IP.

Sin embargo un problema en particular es cuando el tamaño de la red causa retardo entre el remitente y el receptor debido a la distancia.

Para comprender la transmisión con prolongado tiempo, se debe pensar que pasa con el tiempo transcurrido cuando los paquetes de datos son enviados y recibidos. Desde que se utiliza TCP el emisor necesita esperar por un acknowledgment desde el receptor para que los paquetes sean enviados. Cuando el acknowledgment llega después de un largo retraso, el emisor no tiene otra vía si el retardo es debido por congestión en la red o congestión en el receptor o debido a una demora desde el emisor al receptor. Porque de esta incertidumbre el emisor no prueba el incrementar el porcentaje de transmisión y empieza a enviar los datos muy despacio, esto no es normalmente un problema para transferir páginas WEB pero si es un gran problema para archivos de video que contienen miles de megabytes de información que se necesita ser transferidos.

El dispositivo spoofing previamente resuelve el problema con el comienzo lento por que envía rápidamente un acknowledgment para transmitir de esta manera trata de evitar el retardo.

Sí el canal de datos entre el emisor y receptor existe un error, los paquetes necesitaran ser retransmitidos periódicamente, esto es el beneficio de spoofing, adicionalmente spoofing introduce un camino complejo para transferir los archivos, con el cual podría crear incompatibilidad con otros software o dispositivos que son parte de una red IP. Spoofing podría ser utilizado después de realizar un testeo cuidadosamente del transporte de la red para reducir el porcentaje de error.

Jumbo Frames.

Una vía más eficiente para transmitir archivos de video es usar jumbo frames, especialmente para paquetes grandes. Los paquetes estándar Ethernet tienen una longitud límite de 1500 bytes, jumbo frames expande este límite a 9000+bytes, esta técnica provee dos vías para la transferencia de archivos.

Los paquetes de gran tamaño tienen gran porcentaje de datos en cada paquete, a partir la cantidad de datos fijos en la cabecera sin considerar la longitud del paquete.

En el protocolo TCP, el número de acknowledgment que se necesita para ser enviado es reducida, esto permite que la ventana de acknowledgment en el transmisor se expanda, de esta manera mejora el rendimiento entre los terminales de la red pero causa retardo en una comunicación completa es decir de ida y vuelta.

Desafortunadamente la mayoría de redes particularmente las WAN no soportan jumbo frames, esta tecnología puede ser utilizada en redes de área local o en redes privadas.

Después de haber analizado las tecnologías de transporte de video y contando con la estructura actual de la red tanto los dispositivos de hardware y software se adoptará la tecnología de TCP spoofin, utilizando dispositivos de hardware para almacenar la información para luego empezar la conexión y retransmitir.

2.7 ADMINISTRACION DE ALERTAS DE MONITOREO

El personal de seguridad son los principales usuarios del sistema, es decir son los encargados de monitorear y vigilar a través del sistema de video IP, con esta particularidad son los responsables de informar cualquier evento sospechoso a su inmediato superior en la línea de mando hasta el jefe de seguridad.

Según la gravedad del evento el personal de seguridad está en su responsabilidad de tomar dediciones oportunas a estos eventos y si la situación requiere de una instancia mayor será comunicada al jefe del de seguridad quien impartirá procedimientos oportunos.

Todos los reportes que requieran atención especial a más de ser informado al jefe de seguridad tienen que ser informados a la gerencia que es la instancia de mayor jerarquía dentro de la institución y la encargada en la toma de decisiones frente a estos eventos.

En cuanto a la vigilancia y monitoreo dentro de los bienes muebles, si se detecta algún evento sospechoso causado por estudiante o empleado dentro la institución el departamento de inspección general es el encargado de tomar decisiones oportunas en el caso de los estudiantes y la gerencia en el caso de un empleado.

2.8 USUARIOS DE MONITOREO.

Para el efecto se han identificado usuarios dentro del sistema, cada usuario pertenece a un grupo y cada uno se ha configurado un grupo de cámaras al cuál tienen acceso con sus respectivos niveles de acceso es decir se cuenta con un username y password y dependiendo de estos tienen asignados los permisos.

2.8.1 SEGURIDAD.

Tienen acceso a todas las cámaras instaladas, los cuales están dentro de un grupo y básicamente cuenta con todos los permisos excepto de revisar los eventos previamente grabados o registrados.

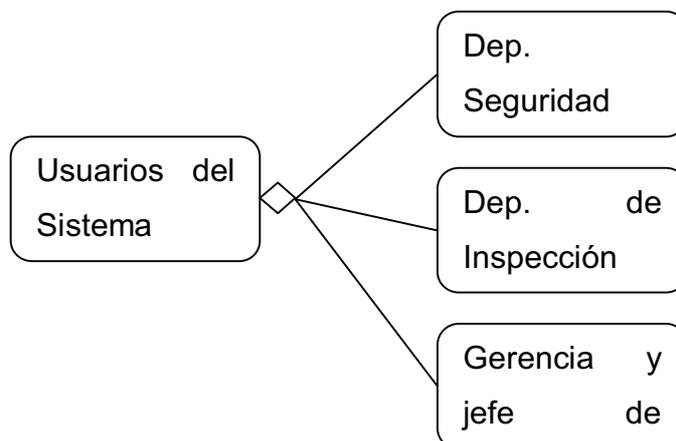
2.8.2 JEFE DE SEGURIDAD Y GERENCIA.

Son los usuarios que tienen acceso de igual forma a todas las cámaras y están ubicados en un grupo de administradores con todos los permisos y también con acceso a los eventos monitoreados.

2.8.3 INSPECCIÓN GENERAL.

Tiene acceso a las cámaras ubicadas en la entrada y salida de buses otorgándoles permisos de solo de monitoreo es decir solo podrán visualizar las cámaras.

GRAFICO 2.10 USUARIOS DEL SISTEMA



2.9 FORMAS DE ALMACENAMIENTO DE LOS EVENTOS MONITOREADOS

El software de monitoreo D3Data NETVM una de sus funciones es permitir configurar la carpeta donde se almacenará los eventos en cualquier servidor dentro de la LAN.

El almacenamiento dependiendo de la ubicación de la cámara y la importancia de los eventos monitoreados deberán realizar este proceso las 24 horas del día o ajustarse a un horario posible de grabación como se indica en la tabla 2.2

TABLA 2.2 HORARIO DE GRABACION DE CAMARAS

Cámara	Grab Horas por día
Parqueadero	12
Buses	12
Buses	12
Primaria	8
Secundaria	8
Prescolar	8
ESTADIO	12
Total	72

Para el almacenamiento de los eventos se cuenta con discos duros de tecnología SATA con 300 Gbytes instalados en el servidor de cámaras, los archivos de video almacenado tiene el formato MPG. Cada cámara cuenta con su propia carpeta de almacenamiento cuyos archivos tienen información de la fecha y hora de la grabación realizada.

El software de monitoreo permite realizar una grabación continua en cada espacio de almacenamiento dando la posibilidad de reutilización del disco es decir cuando detecta que no hay suficiente espacio en disco empieza a borrar los archivos los más antiguos conservando los más recientes en fechas de grabación.

2.10 POLITICAS DE BACKUP

Como se mencionó anteriormente toda la información que se genera se almacena en las carpetas de almacenamiento de cada cámara, esta información posteriormente se trasladará al servidor de respaldos donde solo tiene acceso el administrador de red.

Con ayuda de la herramienta de copia de seguridad propia de Windows se puede configurar el respaldo de la siguiente forma:

- El respaldo se lo debe realizar diariamente.
- Realizar un respaldo normal la primera vez
- Cada día realizar un respaldo normal y diferencial
- Verificar periódicamente la integridad de los respaldos
- Evaluar la información respaldada conjuntamente con el jefe de seguridad antes que los respaldos sean borrados físicamente teniendo en cuenta que los archivos de video generan gran espacio en disco.
- De igual forma realizar una restauración periódica con el fin de comprobar la integridad de la información.

CAPITULO 3: IMPLEMENTACION DEL PROTOTIPO

3.1 ANALISIS DE COSTOS

Una vez revisadas las demostraciones, explicación, característica de cámaras y proformas de las diferentes empresas, se sugiere realizar la compra inicial de al menos 4 cámaras, dos para interiores y dos para exteriores.

De acuerdo a lo revisado se tiene:

Tabla 3.1 Cotizaciones Cámaras

Opción 1

Cant	Descripción	Empres a	P. U.	P. Total
1	Cámara IP, FV-3100-I, color, para interiores, fija, sin zoom, varifocal, con soporte, 32° de cobertura, CON licencia Relay Server	Satcom	416.4	416.4
2	Cámara IP, MZ-3100, color, para Interiores, fija, zoom MANUAL, varifocal, con soporte, CON licencia Relay Server para una cámara	Satcom	850.8	1701.6
	Total sin IVA			2118

Tabla 3.2 Cotizaciones Cámaras Axis

Opción 2

Cant	Descripción	Empresa	P. U.	P. Total
1	Axis 207 Indoor Network Camera	Asecuador	332.35	332.35
2	Axis 210 Network Camera	Asecuador	527.85	1055.7
	Total sin IVA			1388.05

Nota:

- 1.- Estos precios no incluyen el 12% de IVA
- 2.- Los costos solo representan el valor del equipo.
- 3.- En las opciones no se incluye el valor del software de monitoreo

De acuerdo con el presupuesto destinado para el proyecto de cámaras para la inicialización del presente proyecto se cuenta con el visto bueno de la gerencia y se procede a la compra de 4 cámaras Axis, dos cámaras correspondiente al modelo 207 y dos cámaras correspondientes al modelo 210.

Costos del Sistema:

Descripción	Cantidad	Precio Unitario	Precio Total
Cámara Axis 207	2	332.25	664.5
Cámara Axis 210	2	527.85	1055.7
Computador (servidor)	1	950	840
Licencia Windows	1	100	100
Cables	200 m.	200	200
Puntos Eléctricos	4	150	150
Costo Parcial			3010.2
IVA			361.22
Costo Total			3371.42

Costo Remuneración Mensual (Guardia)

Ítem	Valor
Sueldo Mensual	250
IESS	30
Décimos	25
Seguro Médico	35
Uniformes	10
Costo Total Mensual	350

Período de Recuperación del Capital

Mes	Ahorro	Acumulado	Inversión Inicial
1	350	350	3372
2	350	700	3372
3	350	1050	3372
4	350	1400	3372
5	350	1750	3372
6	350	2100	3372
7	350	2450	3372
8	350	2800	3372
9	350	3150	3372
10	350	3500	3372

La vida útil del sistema de cámaras está proyectada para tres años, con los cuadros anteriores el costo anual de un guardia de seguridad es de 4200 dólares en dos años son 8400 dólares, reemplazando un guardia con el sistema propuesto el período de recuperación del capital es a partir de los 10 meses tiempo en se cubre los costos empleados para la implementación del proyecto.

3.2 ANALISIS TECNICO Y DE FACTIBILIDAD

3.2.1 ANALISIS TECNICO

De acuerdo con las características descritas de la infraestructura actual del establecimiento, cuenta con los recursos necesarios tanto en hardware como en software para poder llevar a cabo este proyecto, al cuál se incluirá nuevos equipos para lograr el incremento de la seguridad deseada.

Con este proyecto se logrará mejorar la deficiencia en la vigilancia y seguridad de los bienes muebles e inmuebles de la institución, también la del estudiantado y personal en general.

3.2.2 ANALISIS DE FACTIBILIDAD

Evidenciados los procedimientos de seguridad y la necesidad de incrementar y mejorar estos procesos conlleva a buscar una alternativa que permita obtener un mejor control sobre los bienes muebles e inmuebles del establecimiento, como también el proceso de seguridad de los estudiantes.

Es decisión de la gerencia del establecimiento llevar a cabo este tipo de proyecto, el cual se requiere que no involucre costos altos en esta primera etapa, con la sencilla razón de realizar todas las pruebas posibles y en base a estas tomar la decisión en un sistema completo, porque conlleva a utilizar con lo que cuenta la infraestructura actual y adquirir los equipos e implementos justamente lo necesario y que los mismos formen parte del sistema final.

Con los resultados obtenidos y evaluados en esta parte del proyecto se preverá la posibilidad de adquirir mejor infraestructura en hardware y software para implementar un sistema completo con el número de cámaras necesarias en las zonas críticas.

Para este proyecto inicialmente se adquirirán los siguientes equipos:

- Un servidor de Cámaras
- Dos Cámaras IP
- Protectores y pedestales (soportes) para las cámaras
- Software de Monitoreo
- Sistema Operativo Windows 2003 Server
- Dirección Web para acceso externo

3.2.3 SELECCION DE CAMARAS IP.

Para el efecto de este proyecto se adquirió cámaras de tecnología IP AXIS en los modelos 207 y 210 cuyas características se detallan a continuación:

- Excelente calidad de imagen gracias al uso de un sensor CCD de exploración progresiva y procesamiento de vídeo avanzado.
- Cámara de red con funcionalidad completa y servidor Web incorporado
- Realiza detección de movimiento en la imagen e incluye memorias pre y post alarma.
- Amplia gama de resoluciones: hasta 640 x 480 en diferentes niveles de calidad a frecuencias de hasta 25 imágenes por segundo.
- Posibilidad de insertar máscara, logotipo personalizado o imagen superpuesta en las secuencias de vídeo.

3.2.4 SELECCIÓN DEL SOFTWARE DE MONITOREO

En este proyecto se probó varios software de monitoreo de versión trial es decir con versiones solo de prueba en los cabe mencionar el software Active Web Cam, Mailstone y el D3Data NETVW.

El software de monitoreo que originalmente viene con las cámaras Axis no se lo adquirió por el precio razón por la cual para el presente proyecto se realizó con software de fabricantes bajados del Internet.

El software D3Data NETVW en su implementación ofrece algunas opciones interesantes que se las puede mencionar como ventajas frente a los demás

software de monitoreo que se probó previamente. Permitiendo gestionar, potencializar las aplicaciones y beneficios de la administración de video.

Una de las principales ventajas es la opción de poder crear usuarios y grupos de acceso, también la posibilidad de crear vistas para cada grupo y usuario y poder relacionarlos.

3.3 ANALISIS LEGAL

Para el presente proyecto se realizó la compra de las cámaras con su respectivo software que legalmente son propiedad de la institución.

En Internet existe gran variedad de software que puede ser bajado gratuitamente por cualquier usuario, la mayoría de software que se ofrece viene con licencias de prueba que expiran en 30 días, este tipo de licencia son autorizadas por las mismas empresas desarrolladoras de software con la finalidad de probar el producto y si el mismo cumple con las expectativas esperadas sin lugar a dudas las licencias serán adquiridas y pasaran a ser propiedad de la institución en términos legales.

Las áreas de monitoreo que específicamente involucra actos sospechosos por parte de los estudiantes es pedido estricto y autorizado por el consejo de disciplina del plantel debido actos vandálicos ocasionados en los casilleros y en los laboratorios de computación.

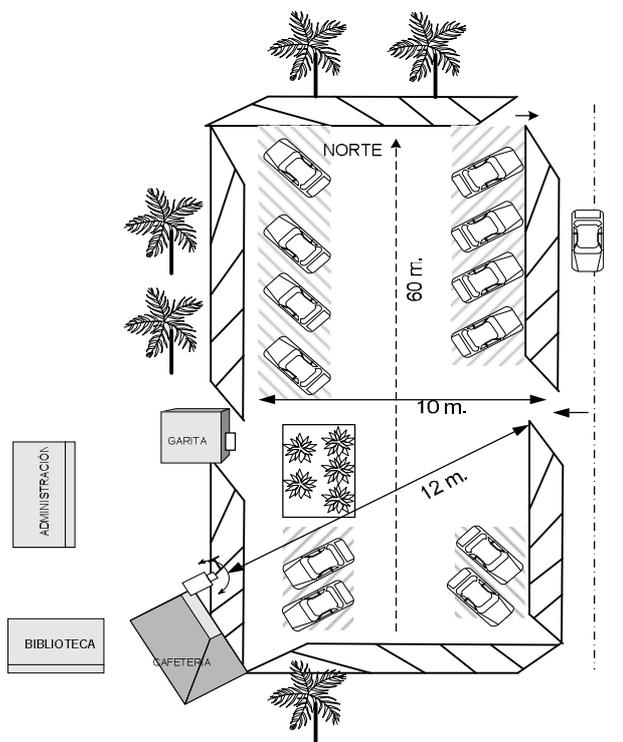
En el caso de la cafetería que involucra a estudiantes y personal del colegio es solicitud expresa por las autoridades de la institución y quien fuere encontrado en cualquier acto de sospecha tendrá que atenerse al reglamento de disciplina y sanciones correspondientes.

3.4 IMPLANTACION DEL PROTOTIPO.

3.4.1 INSTALCIÓN DE CAMARAS

Una vez analizado la ubicación de cámaras y el sitio donde se colocan las mismas se procede con la instalación física del equipo, se debe tomar en consideración que para proceder con esta tarea no se realizó ningún estudio técnico acerca de la distancia, altura y ángulos de visualización para instalar las cámaras, el trabajo más bien consistió en ir buscando y probando un punto de ubicación óptimo y luego realizar la obra civil para su ubicación, en la figura se indica la ubicación de la cámara para el área de parqueaderos instalada en la parte superior de la cafetería, la altura de esta cámara tiene una altura de 3.10 m con un ángulo 35 grados noreste.

Gráfico 3.1 Ubicación cámara parqueadero



3.4.2 INSTALACION DEL SERVIDOR DE CAMARAS

En el servidor de cámaras a nivel de software consta con las siguientes características:

Software

- Sistema Operativo Windows 2003 Server
- Service Pack actualizados
- Sistema Antivirus
- IP privada 192.168.0.15
- Software de monitoreo y administración de cámaras D3Data NETVW

Hardware

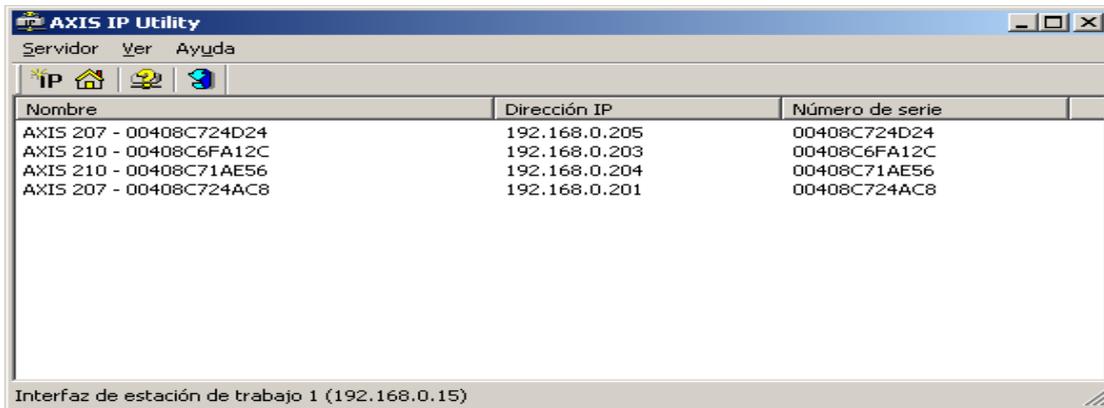
- Procesador Intel Pentium 4 de 2.8 Ghz.
- RAM de 1 Gb.
- Hard Disk de 120 Gb. y 200 Gb.
- Tarjeta Gráfica
- Main Board

Estas características de hardware que se menciona para la instalación del software de monitoreo son las características de los servidores que están en producción en el centro de cómputo de la institución y se cuenta con uno de ellos para el servidor de cámaras, es decir que se cuenta con el equipo y cumple con los requerimientos que se citan.

3.4.3 INSTALACION DE SOFTWARE DE CAMARAS.

Cada cámara Axis viene con su software de instalación con información del MacAdress, el número de serie correspondiente, el modelo y con la configuración de la dirección IP, como se indica en la figura.

Gráfico 3.2 configuración cámaras Axis

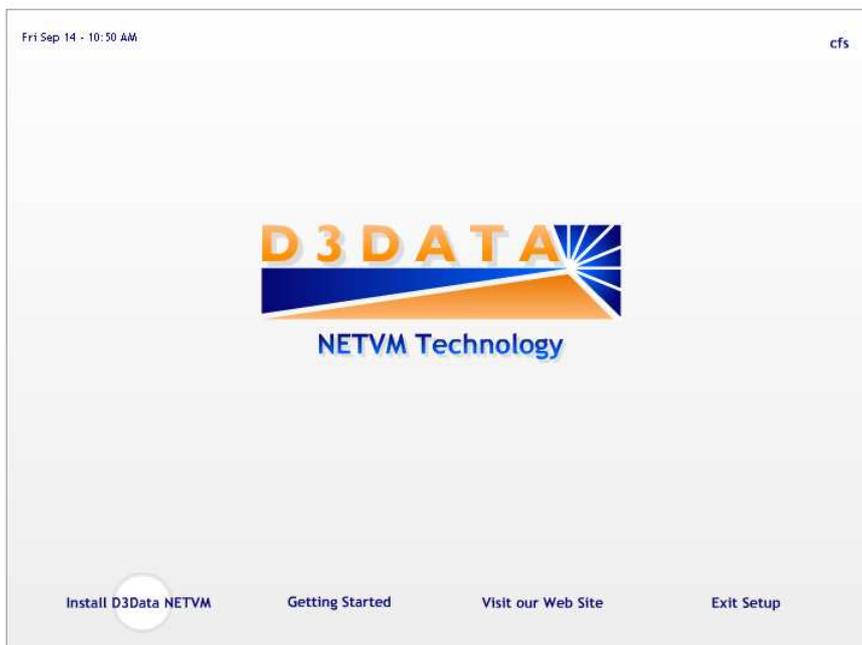


Nombre	Dirección IP	Número de serie
AXIS 207 - 00408C724D24	192.168.0.205	00408C724D24
AXIS 210 - 00408C6FA12C	192.168.0.203	00408C6FA12C
AXIS 210 - 00408C71AE56	192.168.0.204	00408C71AE56
AXIS 207 - 00408C724AC8	192.168.0.201	00408C724AC8

3.4.4 INSTALACION DEL SOFTWARE DE MONITOREO

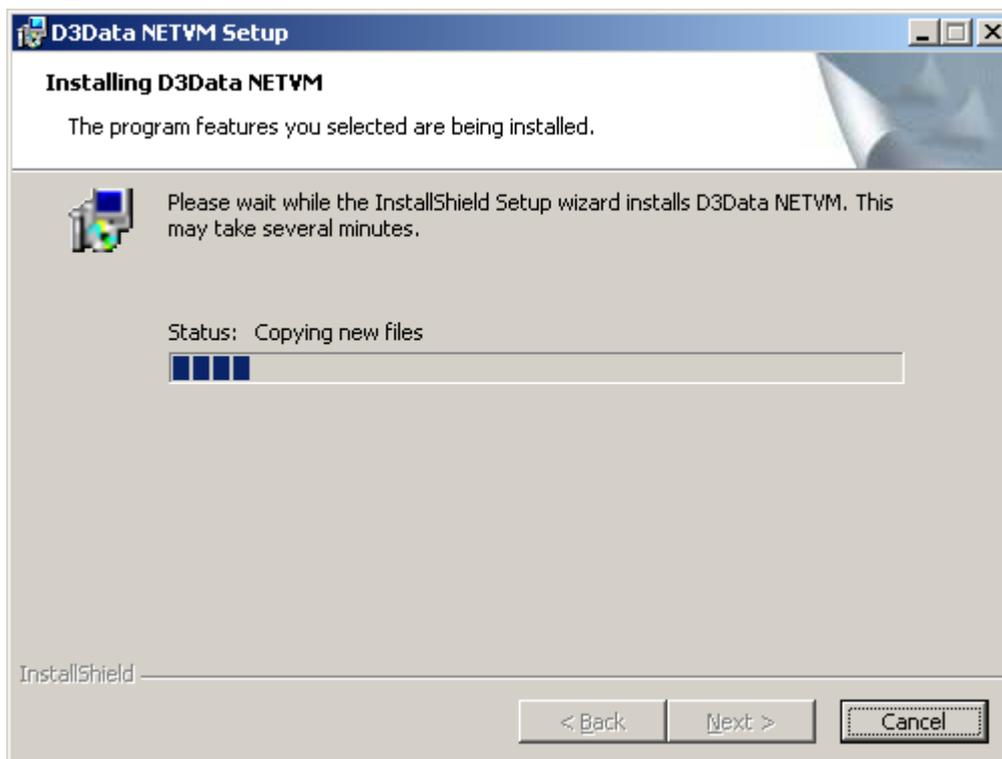
Una vez instalado y configurado el servidor de cámaras se procede con la instalación del software de monitoreo como se indica en las figuras siguientes:

Gráfico 3.3 Pantalla Principal instalación software de monitoreo



En este gráfico empieza el asistente para instalar el software de monitoreo que permitirá agregar las cámaras IP anteriormente instaladas en base a los datos obtenidos de la Mac Adress y la dirección IP asigna, seleccionar la opción de instalación del D3Data NETVM.

Gráfico 3.4 Instalación del Software de monitoreo D3Data NETVM



Cuando se ha completado el asiste de instalación del software de monitoreo, se procede a con las opciones de configuraciones para poder añadir las cámaras y poder crear:

- Los usuarios del sistema
- Los grupos de usuarios

- Permisos de los usuarios
- Asignación e vista de cámaras
- Grabación de cámaras
- Creación de carpetas para grabación de cámaras

En el gráfico 3.5 indica las opciones de configuración que se requiere para llevar a cabo este proceso.

Gráfico 3.5 Pantalla de opciones de configuración D3Data NETVM

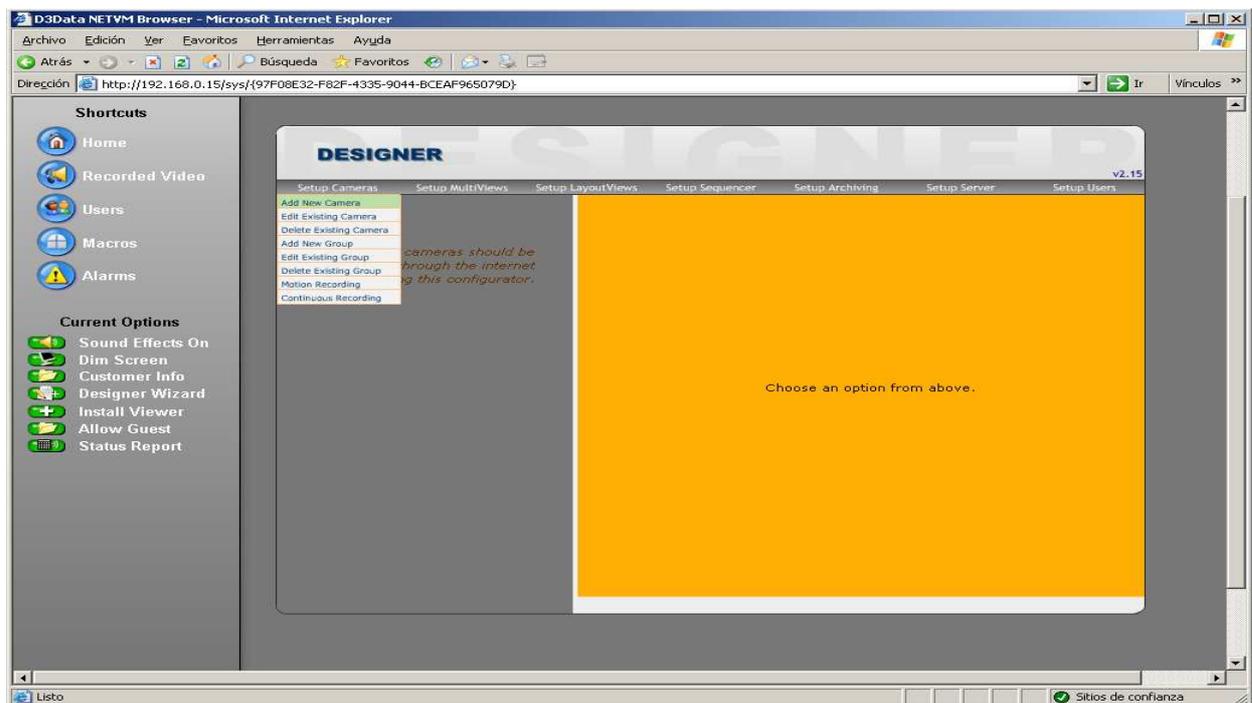
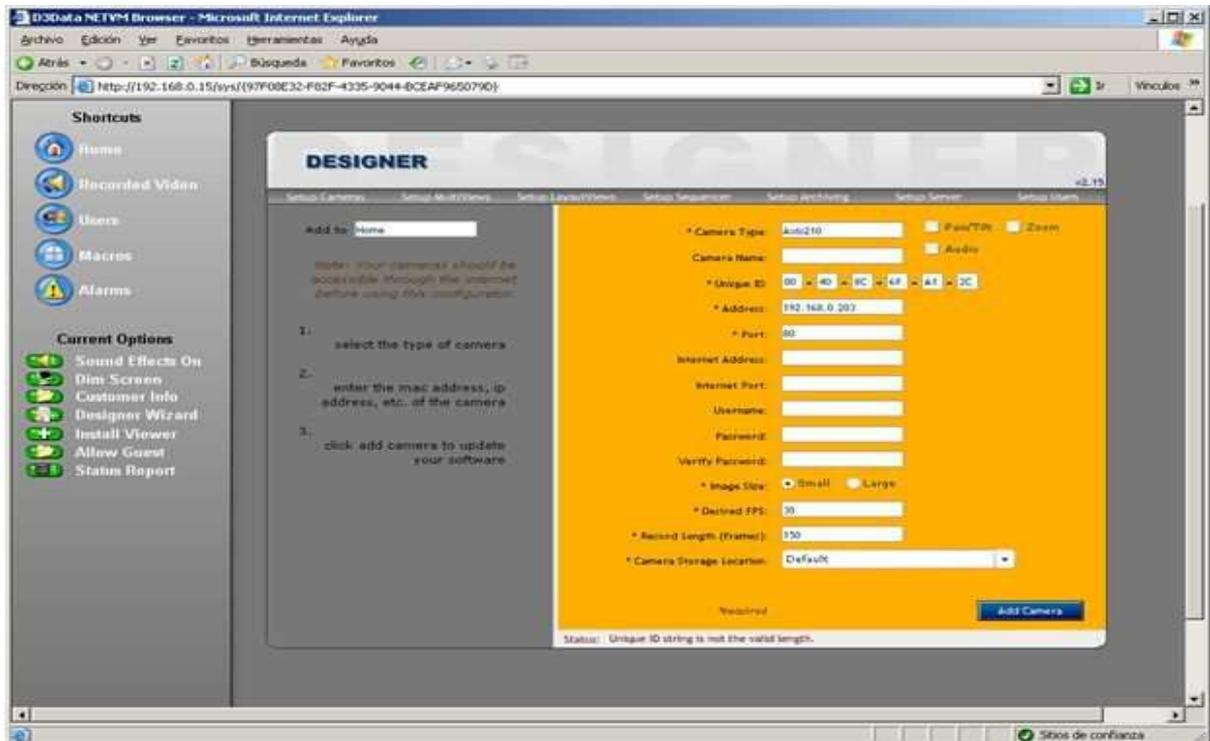


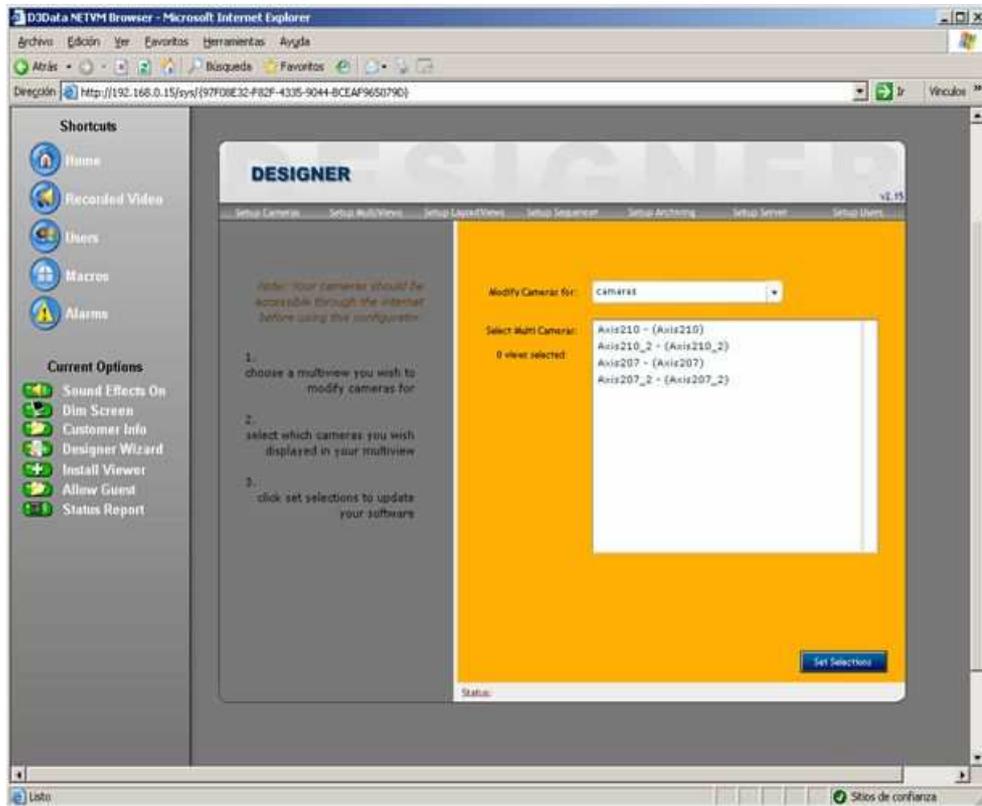
Gráfico 3.6 Pantalla para añadir las cámaras al software de monitoreo



En el pantalla anterior seleccionar la opción setup camera, empieza el los parámetros de configuración en base a las características de la cámara como:

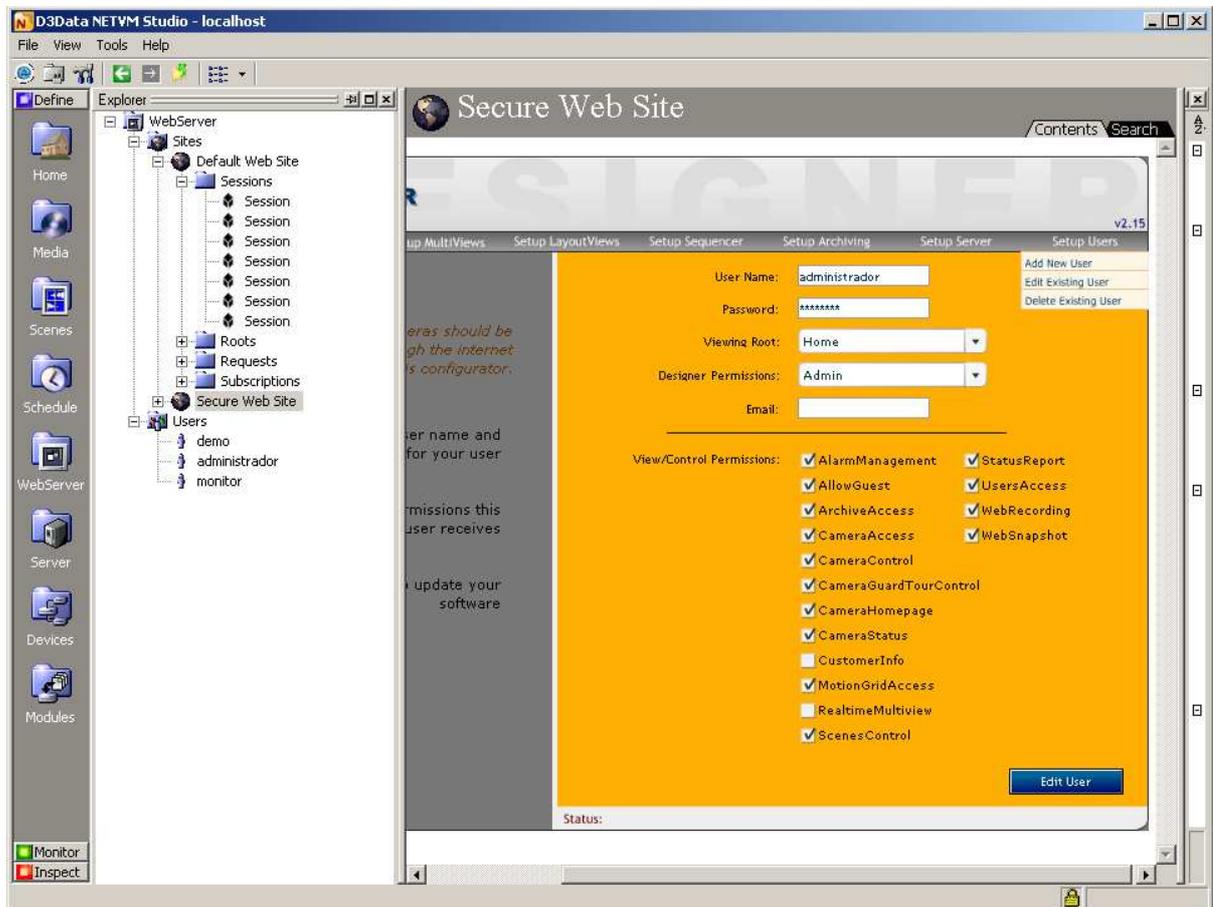
- El modelo de la cámara
- El nombre de la cámara por ejemplo preescolar
- Dirección Mac Adress
- Dirección IP
- El puerto

En el gráfico 3.7 indica el número de cámaras total que se han añadido en esta opción.

Gráfico 3.7 número de cámaras totales configuradas

En el gráfico 3.8 se procede a la opción de crear los usuarios del sistema en base a los perfiles correspondientes.

Gráfico 3.8 Pantalla creación de usuarios y permisos de acceso.



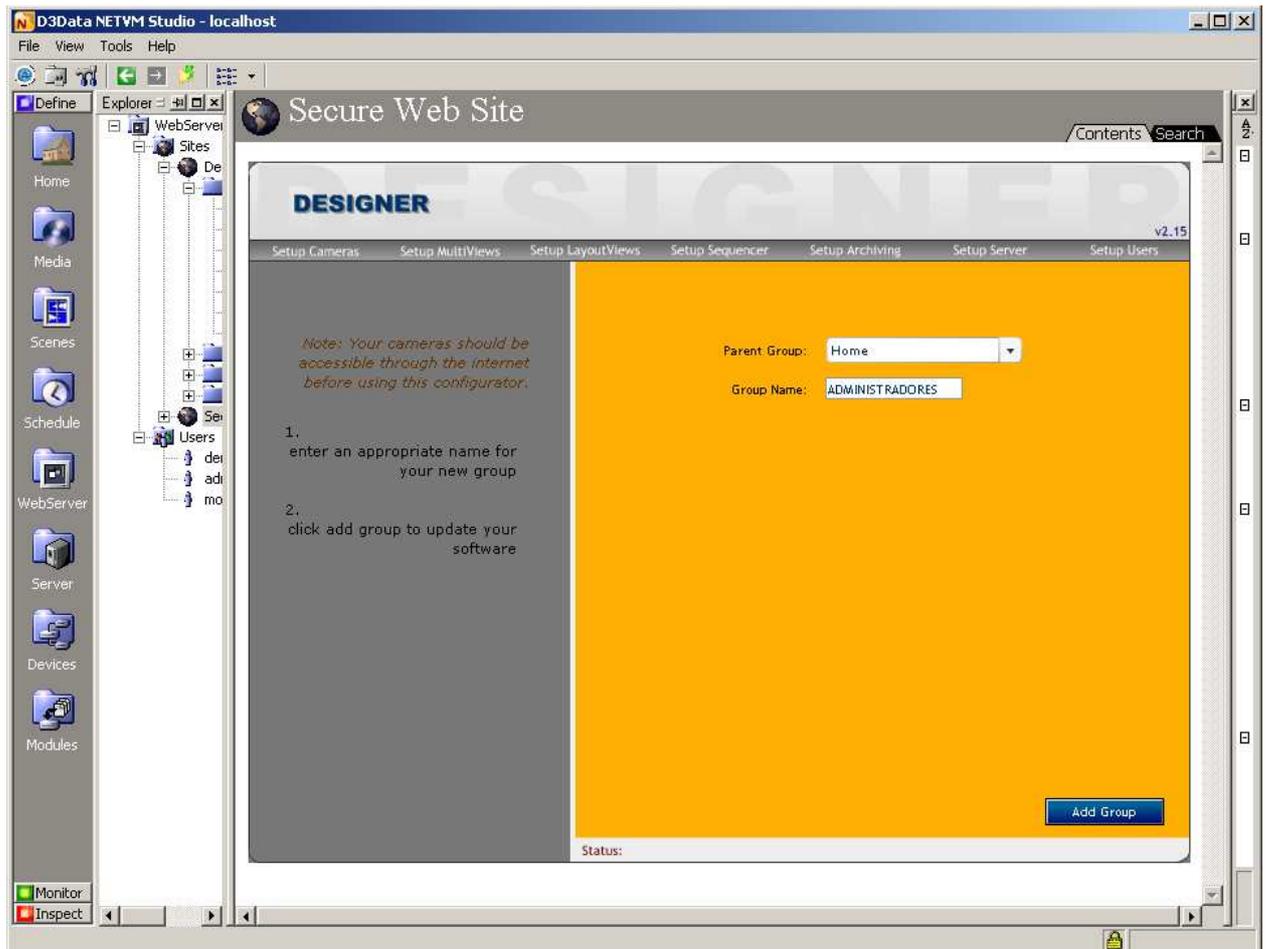
Los usuarios creados para el uso del sistema del sistema son:

- El administrador del sistema, tiene todos los permisos para poder administrar y configurar el sistema.
- Usuarios de inspección general, tendrán solo la posibilidad de visualización de cámaras
- Usuarios de seguridad, tienen los permisos de administrar el sistema
- Jefe de seguridad y gerencia, poseen los permisos de administración y grabación.

En la pantalla siguiente gráfico 3.9 permite la opción de crear los grupos de usuarios de acuerdo a los perfiles seleccionados es decir a los permisos

administrados, con esta opción permite a grupos de usuarios definir las vistas cámaras es decir crear varios conjuntos de cámaras y asignar a un grupo.

Gráfico 3.9 Pantalla para creación de grupos de usuarios

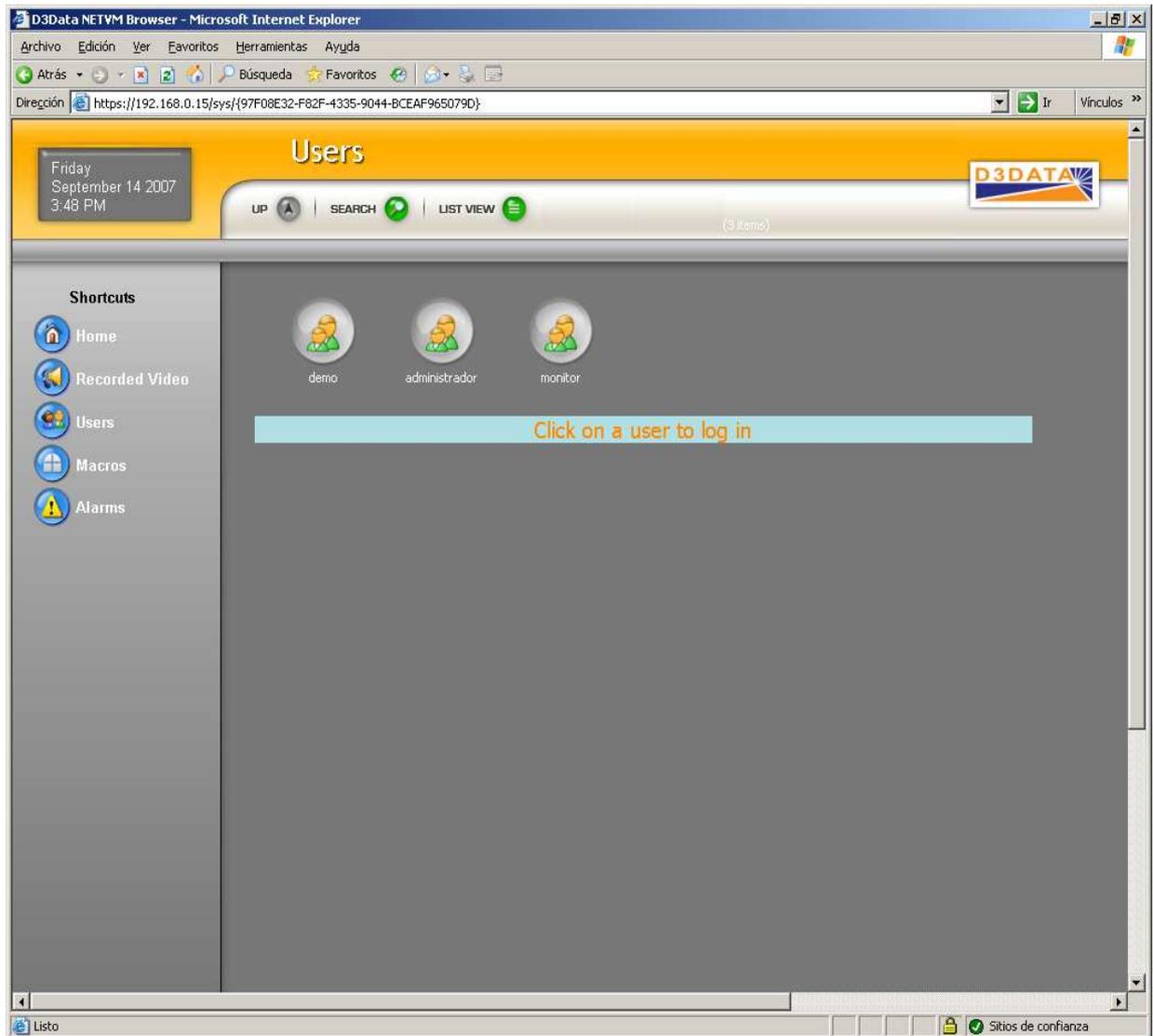


Los grupos de usuarios creados son:

- Administradores
- Seguridad
- Jefe de seguridad y gerencia
- Inspección general

La siguiente pantalla gráfico 2.10 se indica un ejemplo de los usuarios creados para el ingreso al sistema de cámaras.

Gráfico 3.10 Pantalla autenticación para el ingreso al sistema de cámaras

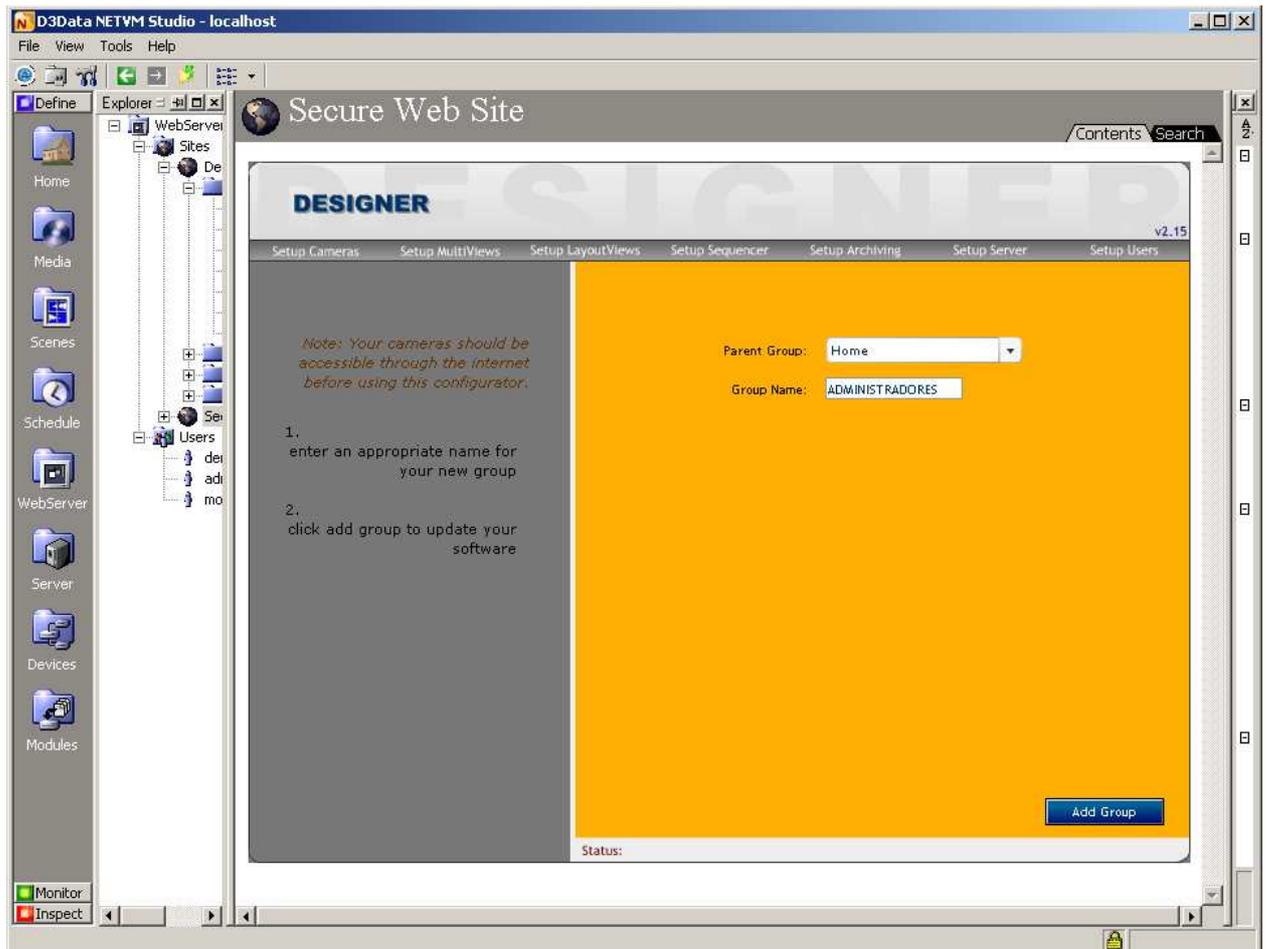


Dependiendo de los permisos asignados los usuarios podrán tener acceso a las cámaras y que vista fueron asignados

En el gráfico 3.11 se configura la creación de vistas de cámaras, se crea una vista a la cual se agregan cámaras, por ejemplo a inspección general necesita

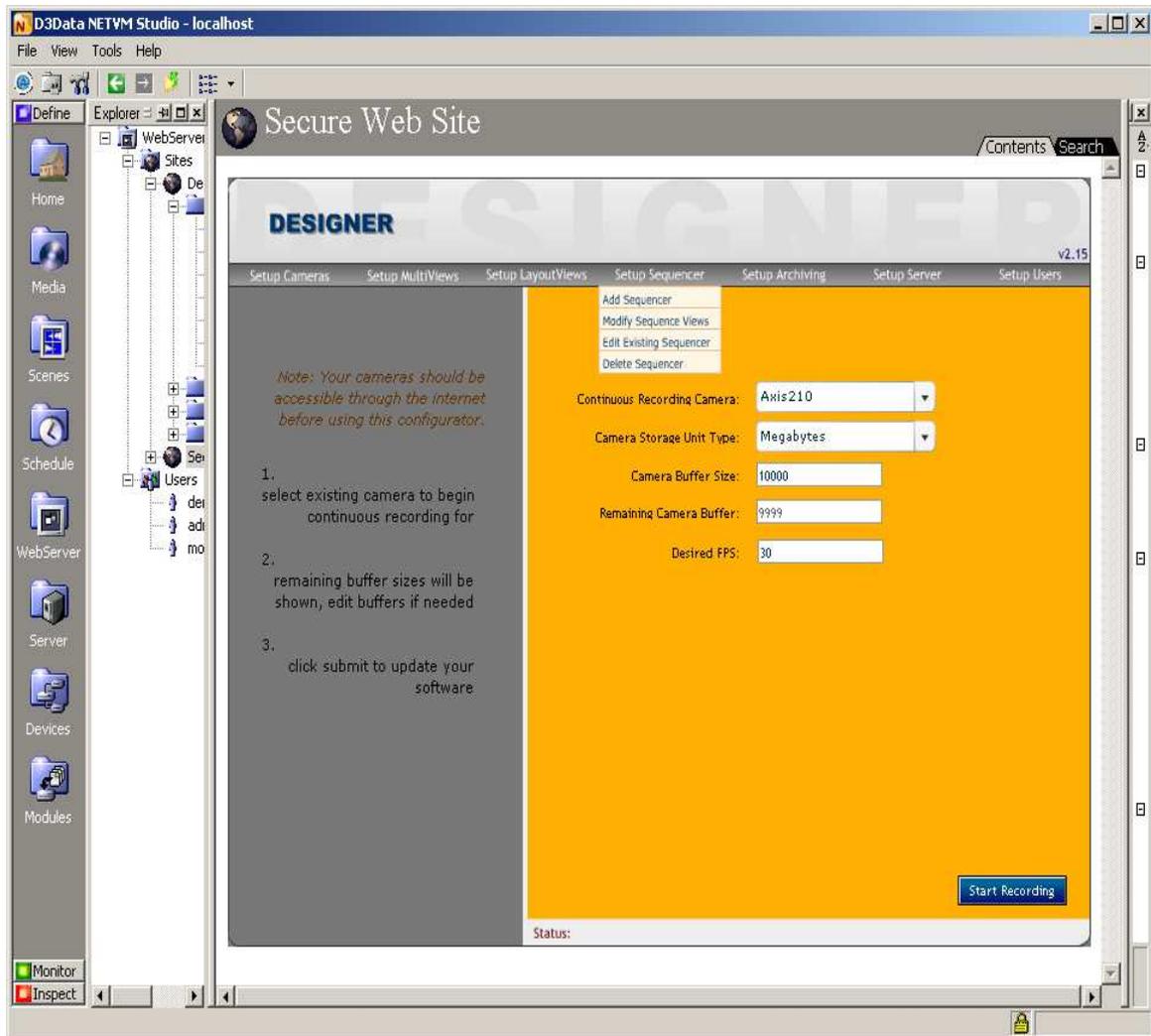
monitorear la entrada salida de buses y solo tendrá acceso a este conjunto de cámaras.

Gráfico 3.11 Pantalla de creación vista de cámaras



en el gráfico 3.12 se procede a la configuración y creación del directorio donde se almacenará toda la información de los eventos monitoreados, para el efecto se configuró que las cámaras graben en forma continua.

Gráfico 3.12 DIRECTORIO D:\GRABACION\CAMARA1

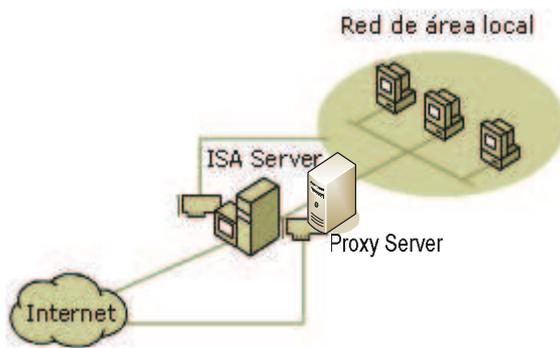


A cada cámara se le debe asignar su propia carpeta con su respectiva identificación donde se almacena toda información registrada correspondiente a la fecha del suceso.

Completado todo el proceso de configuración de cámaras y usuarios se procede con la administración del sistema, en el gráfico 3.13 se obtiene el resultado de todo el proceso realizado y donde empieza la visualización de las cámaras es decir con el monitoreo.

3.4.6 CONFIGURACION DEL ACCESO REMOTO

Para poder acceder al servidor de cámaras o de monitoreo vía Internet se lo realiza configurando una regla de publicación en el servidor ISA Server esto es utilizando la dirección IP pública y direccionando a la dirección IP privada a este proceso se lo conoce como NAT.



Para el acceso remoto se tendrá que digitar la dirección IP pública en el browser desde cualquier computador con acceso a Internet.

3.4.7 PRUEBAS DE MONITOREO

Instaladas las cámaras, el servidor de cámaras y el software de monitoreo se procede a realizar pruebas de funcionamiento del sistema dando como resultado:

Las cámaras cumplen las especificaciones y características del fabricante y se puede observar las imágenes en movimiento en base a estos parámetros.

El software de monitoreo cumple con las expectativas antes planteadas y ejecuta los requerimientos de los usuarios.

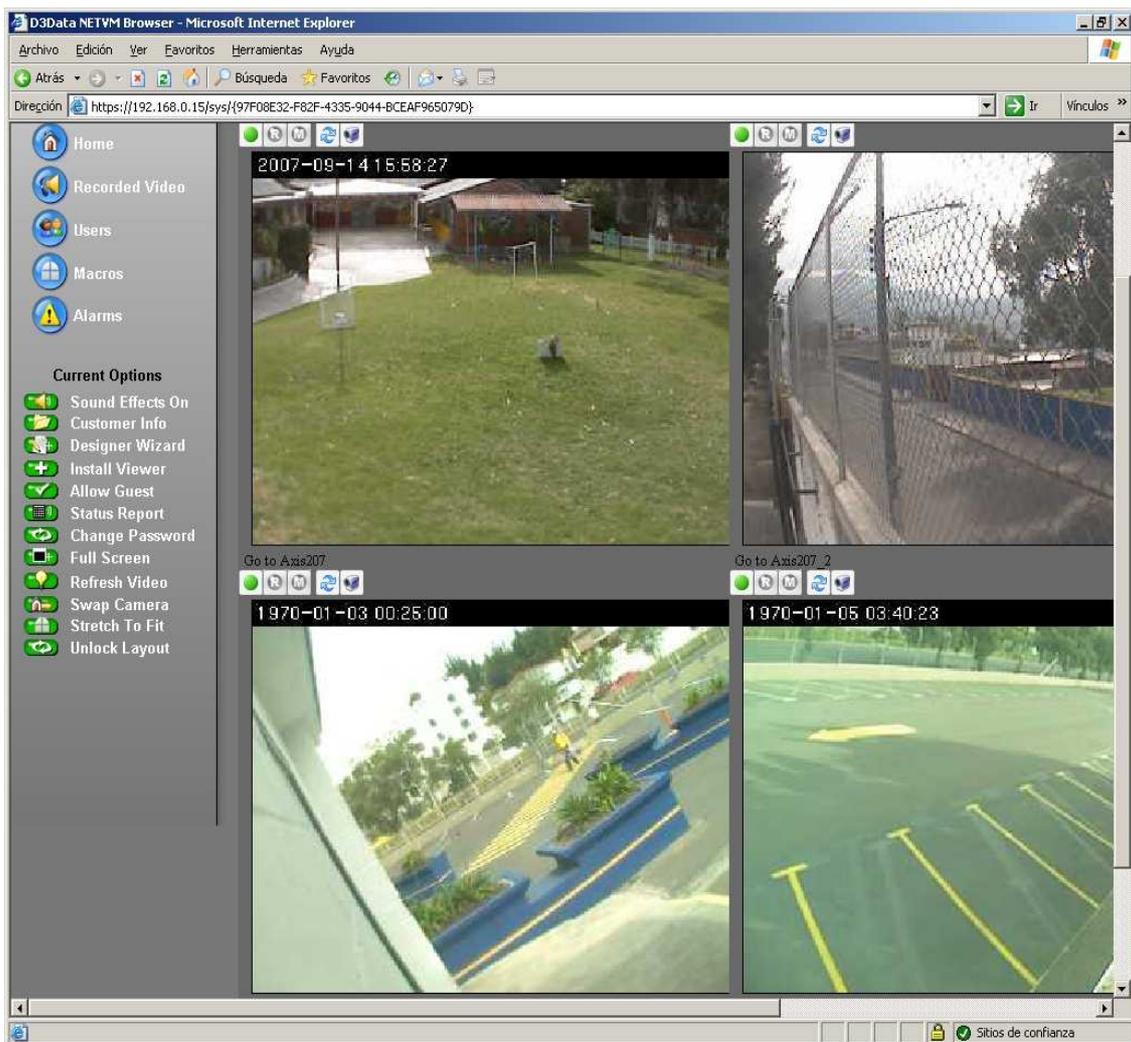
Después de realizar algunas pruebas de ubicación de las cámaras se llegó a determinar el sitio correcto en cuanto a la distancia, ángulo de visualización y altura correcta.

El sistema puesta en marcha cumple con las expectativas requeridas por el personal de seguridad y demás usuarios.

El proceso de grabación de cámaras utiliza los recursos propios del servidor de respaldos en discos duros sin necesidad de utilizar otros dispositivos para este evento.

Este proyecto está en producción y forma parte de la solución final que se requiere alcanzar y está en pleno funcionamiento.

Gráfico 3.13 Pantalla de visualización de cámaras



CAPITULO 4: CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- En base al diagnóstico realizado previamente La infraestructura actual se presta para la elaboración de este proyecto en cuanto a la plataforma de red, hardware y sistemas operativos.
- Con el apoyo de la gerencia y el presupuesto destinado al sistema cámaras fue posible la adquisición de equipos e instalación de las mismas.
- Al momento de elegir el software monitoreo hay que verificar que su programación sea abierta es decir que permita añadir cámaras de distinta tecnología y que su funcionalidad sea adaptable.
- Las cámaras IP tienen la ventaja de conectarse en cualquier lugar de la red de datos y la posibilidad de ir incrementándose según la necesidad.
- Este tipo de tecnología hace que la gestión sea más sencilla y económica ya que no requiere de cableado adicional.
- Los proveedores de soluciones de seguridad en IP se limitan solo a vender el hardware y software de la firma a cuál representan, cuando se trata de una solución completa que involucren hardware de diferente tecnología no ofrecen garantía en la integridad del sistema.
- El software de monitoreo tiene la particularidad de generar vistas de un conjunto de cámaras dando la posibilidad de generar monitoreo personalizado, si a futuro se incrementa el número de cámaras va ser mas difícil visualizar todas en una misma pantalla.
- Los beneficios de la implantación de este proyecto son satisfactorios dando la posibilidad de incrementar la vigilancia desde cualquier estación de trabajo.

- La utilización de software de monitoreo con licencia trial no permite dimensionar al máximo la funcionalidad de sus aplicaciones ya que muchas de sus opciones son restringidas.

4.2 RECOMENDACIONES

- Dado que la red cuenta con switch de capa 2 y es un modelo discontinuado, tiene opciones mínimas de administración y no posee calidad de servicio QoS se recomienda el reemplazo de estos dispositivos para controlar y asegurar la correcta entrega de la información.
- La energía eléctrica que requieren las cámaras para su funcionamiento debe ser una energía regularizada e instalación a tierra para proteger a los dispositivos de descargas ocasionados por la misma red eléctrica o rayos.
- El sistema de cámaras propuesto será un complemento a la vigilancia, por ello necesita el monitoreo del personal de seguridad.
- La mayoría de cámaras serán instaladas a la intemperie es necesario buscar las protecciones para proteger las cámaras del agua, polvo y sol, además tienen que estar en un lugar que no sea de fácil acceso o alcance y sean desconectadas, manipuladas o sustraídas fácilmente.
- Una vez configurado y probado el software de monitoreo D3Data NETVM se recomienda la adquisición del producto y poder trabajar con toda la potencialidad del software.
- El número de cámaras no debe ser excesivo y cause redundancia de monitoreo, tener más 8 cámaras en una pantalla se hace difícil la tarea de monitoreo.
- En sitios sensibles se debería revisar la posibilidad de adquisición e instalación de cámaras de mejores características para gestión de eventos que permiten a la cámara tomar dediciones, y permita la entrada de sensores para robustecer la vigilancia.

ANEXOS**ANEXO 1 DETALLE DE USUARIOS DE LA RED DE LA INSTITUCIÓN**

Tabla A1.1: Número de estudiantes por grado / paralelo		
Grado	Paralelo	
	A	B
Prebásica	25	25
01 EGB	24	23
02 EGB	24	25
03 EGB	22	23
04 EGB	20	20
05 EGB	22	21
06 EGB	19	20
07 EGB	16	16
08 EGB	18	19
09 EGB	19	18
10 EGB	18	19
01 Complementaria	18	19
02 Complementaria	18	17
03 Complementaria	19	20

Tabla A1.2: Distribución personal docente por departamento o área	
Departamento / Área	# Docentes
Arte	08
Ciencias Experimentales	10

Tabla A1.2: Distribución personal docente por departamento o área

Departamento / Área	# Docentes
Matemática	08
Ciencias Sociales	05
Cultura Física	05
Cultura Judía	04
Letras	06
Idiomas	15
Asesoría Universitaria	01
Biblioteca	02
Computación y Multimedia	02
Preescolar	07
Psicología	04
Recuperación Psicopedagógica	02

Tabla A1.3: Distribución del personal administrativo

Área	# Administrativos
Rectorado	02
Vicerrectorado	02
Gerencia	05
Comunicación y admisiones	02
Inspección General	03
Centro de cómputo	03
Secretaría Académica	01
Mantenimiento	12
Seguridad	10

ANEXO 2. DETALLE DE ESTACIONES DE TRABAJO

Anexo A2.1: Distribución de estaciones de trabajo		
#	Equipo	Ubicación - Ambiente
1	Compaq Armada 1500c	Centro de cómputo
2	Compaq NX 9010	Centro de cómputo
3	Compaq NX 9010	Centro de cómputo
4	Compaq NX 9010	Gerencia
5	Estación de Trabajo (Clon 2)	Ciencias Sociales
6	Estación de Trabajo (Clon 2)	Dep. Cultura Física
7	Estación de Trabajo (Clon 2)	Garita
8	Estación de Trabajo (Clon 2)	Lab Biología
9	Estación de Trabajo (Clon 2)	Lab CCNN
10	Estación de Trabajo (Clon 2)	Lab Física
11	Estación de Trabajo (Clon 2)	Lab Química
12	Estación de Trabajo (Clon 2)	Mantenimiento
13	Estación de Trabajo (Clon 2)	Mantenimiento
14	Estación de Trabajo (Clon 2)	Psicología
15	Estación de Trabajo (Clon INTEL 1)	Arte
16	Estación de Trabajo (Clon Intel 1)	Asesoría Universitaria
17	Estación de Trabajo (Clon INTEL 1)	Biblioteca
18	Estación de Trabajo (Clon Intel 1)	Ciencias Experimentales
19	Estación de Trabajo (Clon Intel 1)	Ciencias Experimentales
20	Estación de Trabajo (Clon Intel 1)	Contabilidad
21	Estación de Trabajo (Clon Intel 1)	Dep. Cultura Física
22	Estación de Trabajo (Clon Intel 1)	Hebreo
23	Estación de Trabajo (Clon Intel 1)	Idiomas
24	Estación de Trabajo (Clon Intel 1)	Idiomas
25	Estación de Trabajo (Clon INTEL 1)	Inspección General
26	Estación de Trabajo (Clon Intel 1)	Letras
27	Estación de Trabajo (Clon Intel 1)	Letras

Anexo A2.1: Distribución de estaciones de trabajo		
#	Equipo	Ubicación - Ambiente
28	Estación de Trabajo (Clon Intel 1)	Oficina de Suministros
29	Estación de Trabajo (Clon Intel 1)	Psicología
30	Estación de Trabajo (Clon Intel 1)	Oficina Preescolar
31	Estación de Trabajo (Clon INTEL 2)	Asistente Contabilidad
32	Estación de Trabajo (Clon INTEL 2)	Biblioteca
33	Estación de Trabajo (Clon INTEL 2)	Contabilidad
34	Estación de Trabajo (Clon Intel 2)	Idiomas
35	Estación de Trabajo (Clon Intel 2)	Letras
36	Estación de Trabajo (Clon INTEL 2)	Rectorado
37	Estación de Trabajo (Clon INTEL 2)	Relaciones Públicas
38	Estación de Trabajo (Clon INTEL 2)	Secretaria Académica
39	Estación de Trabajo (Clon INTEL 2)	Secretaria Gerencia
40	Estación de Trabajo (Clon INTEL 2)	Secretaria Rectorado
41	Estación de Trabajo (Clon INTEL 3)	Arte
42	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
43	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
44	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
45	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
46	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
47	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
48	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
49	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
50	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
51	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
52	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
53	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
54	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
55	Estación de Trabajo (Clon INTEL 3)	Laboratorio Génesis
56	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2

Anexo A2.1: Distribución de estaciones de trabajo		
#	Equipo	Ubicación - Ambiente
57	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
58	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
59	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
60	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
61	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
62	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
63	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
64	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
65	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
66	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
67	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
68	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
69	Estación de Trabajo (Clon INTEL 3)	Laboratorio PC2
70	Estación de Trabajo (Clon INTEL 3)	Recup. Psicopedagógica
71	Estación de Trabajo (Clon Intel 4)	Biblioteca
72	Estación de Trabajo (Clon Intel 4)	Centro de cómputo
73	Estación de Trabajo (Clon Intel 4)	Centro de cómputo
74	Estación de Trabajo (Clon INTEL 4)	Centro de cómputo
75	Estación de Trabajo (Clon Intel 4)	Ciencias Sociales
76	Estación de Trabajo (Clon INTEL 4)	Colecturía
77	Estación de Trabajo (Clon Intel 4)	Coordinación BI
78	Estación de Trabajo (Clon Intel 4)	Experimentación
79	Estación de Trabajo (Clon Intel 4)	Hebreo
80	Estación de Trabajo (Clon INTEL 4)	Inspección General
81	Estación de Trabajo (Clon Intel 4)	Multimedia
82	Estación de Trabajo (Clon Intel 4)	Oficina de Suministros
83	Estación de Trabajo (Clon INTEL 4)	Recepción
84	Estación de Trabajo (Clon INTEL 4)	Secretaría Vicerrectorado
85	Estación de Trabajo (Clon Intel 4)	Seguridad

Anexo A2.1: Distribución de estaciones de trabajo		
#	Equipo	Ubicación - Ambiente
86	Estación de Trabajo (Clon INTEL 4)	Subinspección General
87	Estación de Trabajo (Clon INTEL 4)	Subinspección General
88	Estación de Trabajo (Clon Intel 4)	Vicerrectorado
89	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
90	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
91	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
92	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
93	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
94	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
95	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
96	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
97	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
98	Estación de Trabajo (Imac G3)	Laboratorio Preescolar
99	Estación de trabajo (Power MAC G3)	Laboratorio Preescolar
100	Estación de trabajo (Power MAC G3)	Laboratorio Preescolar

ANEXO 3. DIRECCIONAMIENTO IP

Tabla A3.1 Distribución de direcciones IP		
Dispositivo	Dirección IP	Ubicación
Servidor ISA Server (SRVDMZ02)	192.168.0.1	Sala de servidores
Firewall	192.168.0.2	Sala de servidores
Servidor de correo (Server)	192.168.0.4	Sala de servidores
Servidor de aplicaciones, archivos (BDCNorton)	192.168.0.5	Sala de servidores
Servidor de base de datos	192.168.0.6	Sala de servidores

Tabla A3.1 Distribución de direcciones IP		
Dispositivo	Dirección IP	Ubicación
(Server11)		
Servidor de archivos estudiantes (Estudiantes)	192.168.0.8	Sala de servidores
Servidor de archivos profesores (Profesores)	192.168.0.9	Sala de servidores
Servidor de aplicaciones (TerminalServer)	192.168.0.10	Sala de servidores
Servidor Directorio activo (Server 2000)	192.168.0.11	Sala de servidores
HP Láser Jet 1200n	192.168.0.26	Laboratorio Génesis
HP Láser Jet 1200n	192.168.0.27	Laboratorio PC2
HP Láser Jet 1300n	192.168.0.28	Colecturía
HP Láser Jet 1300n	192.168.0.29	Vicerrectorado
HP Láser Jet 1300n	192.168.0.30	Subinspección General
HP Láser Jet 1300n	192.168.0.31	Inspección General
HP Láser Jet 2300dn	192.168.0.32	Recepción
HP Láser Color Jet 2500	192.168.0.33	Oficina Suministros
Xerox Work Centre 315 /320	192.168.0.34	Colecturía
Xerox Document Centre 332/340	192.168.0.35	Oficina Suministros
Estación de Trabajo (Clon INTEL 1)	192.168.0.51	Arte
Estación de Trabajo (Clon INTEL 3)	192.168.0.52	Arte
Estación de Trabajo (Clon Intel 1)	192.168.0.53	Asesoría Universitaria
Estación de Trabajo (Clon INTEL 2)	192.168.0.54	Asistente Contabilidad
Estación de Trabajo (Clon INTEL 1)	192.168.0.55	Biblioteca
Estación de Trabajo (Clon INTEL 2)	192.168.0.56	Biblioteca
Estación de Trabajo (Clon Intel 4)	192.168.0.57	Biblioteca
Compaq Armada 1500c	192.168.0.58	Centro de cómputo
Compaq NX 9010	192.168.0.59	Centro de cómputo
Compaq NX 9010	192.168.0.60	Centro de cómputo

Tabla A3.1 Distribución de direcciones IP		
Dispositivo	Dirección IP	Ubicación
Estación de Trabajo (Clon Intel 4)	192.168.0.61	Centro de cómputo
Estación de Trabajo (Clon Intel 4)	192.168.0.62	Centro de cómputo
Estación de Trabajo (Clon INTEL 4)	192.168.0.63	Centro de cómputo
Estación de Trabajo (Clon Intel 1)	192.168.0.64	Ciencias Experimentales
Estación de Trabajo (Clon Intel 1)	192.168.0.65	Ciencias Experimentales
Estación de Trabajo (Clon 2)	192.168.0.66	Ciencias Sociales
Estación de Trabajo (Clon Intel 4)	192.168.0.67	Ciencias Sociales
Estación de Trabajo (Clon INTEL 4)	192.168.0.68	Colecturía
Estación de Trabajo (Clon Intel 1)	192.168.0.69	Contabilidad
Estación de Trabajo (Clon INTEL 2)	192.168.0.70	Contabilidad
Estación de Trabajo (Clon Intel 4)	192.168.0.71	Coordinación BI
Estación de Trabajo (Clon 2)	192.168.0.72	Dep. Cultura Física
Estación de Trabajo (Clon Intel 1)	192.168.0.73	Dep. Cultura Física
Estación de Trabajo (Clon Intel 4)	192.168.0.74	Experimentación
Estación de Trabajo (Clon 2)	192.168.0.75	Garita
Compaq NX 9010	192.168.0.76	Gerencia
Estación de Trabajo (Clon Intel 1)	192.168.0.77	Hebreo
Estación de Trabajo (Clon Intel 4)	192.168.0.78	Hebreo
Estación de Trabajo (Clon Intel 1)	192.168.0.79	Idiomas
Estación de Trabajo (Clon Intel 1)	192.168.0.80	Idiomas
Estación de Trabajo (Clon Intel 2)	192.168.0.81	Idiomas
Estación de Trabajo (Clon INTEL 1)	192.168.0.82	Inspección General
Estación de Trabajo (Clon INTEL 4)	192.168.0.83	Inspección General
Estación de Trabajo (Clon 2)	192.168.0.84	Lab Biología
Estación de Trabajo (Clon 2)	192.168.0.85	Lab CCNN
Estación de Trabajo (Clon 2)	192.168.0.86	Lab Física
Estación de Trabajo (Clon 2)	192.168.0.87	Lab Química
Estación de Trabajo (Clon Intel 1)	192.168.0.128	Letras
Estación de Trabajo (Clon Intel 1)	192.168.0.129	Letras

Tabla A3.1 Distribución de direcciones IP		
Dispositivo	Dirección IP	Ubicación
Estación de Trabajo (Clon Intel 2)	192.168.0.130	Letras
Estación de Trabajo (Clon 2)	192.168.0.131	Mantenimiento
Estación de Trabajo (Clon 2)	192.168.0.132	Mantenimiento
Estación de Trabajo (Clon Intel 4)	192.168.0.133	Multimedia
Estación de Trabajo (Clon Intel 1)	192.168.0.134	Oficina de Suministros
Estación de Trabajo (Clon Intel 4)	192.168.0.135	Oficina de Suministros
Estación de Trabajo (Clon Intel 1)	192.168.0.136	Oficina Preescolar
Estación de Trabajo (Clon 2)	192.168.0.137	Psicología
Estación de Trabajo (Clon Intel 1)	192.168.0.138	Psicología
Estación de Trabajo (Clon INTEL 4)	192.168.0.139	Recepción
Estación de Trabajo (Clon INTEL 2)	192.168.0.140	Rectorado
Estación de Trabajo (Clon INTEL 3)	192.168.0.141	Recup. Psicopedagógica
Estación de Trabajo (Clon INTEL 2)	192.168.0.142	Relaciones Públicas
Estación de Trabajo (Clon INTEL 2)	192.168.0.143	Secretaria Académica
Estación de Trabajo (Clon INTEL 2)	192.168.0.144	Secretaria Gerencia
Estación de Trabajo (Clon INTEL 2)	192.168.0.145	Secretaria Rectorado
Estación de Trabajo (Clon INTEL 4)	192.168.0.146	Secretaría
		Vicerrectorado
Estación de Trabajo (Clon Intel 4)	192.168.0.147	Seguridad
Estación de Trabajo (Clon INTEL 4)	192.168.0.148	Subinspección General
Estación de Trabajo (Clon INTEL 4)	192.168.0.149	Subinspección General
Estación de Trabajo (Clon Intel 4)	192.168.0.150	Vicerrectorado
Estación de Trabajo (Clon INTEL 3)	192.168.0.201	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.202	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.203	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.204	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.205	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.206	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.207	Laboratorio Génesis

Tabla A3.1 Distribución de direcciones IP		
Dispositivo	Dirección IP	Ubicación
Estación de Trabajo (Clon INTEL 3)	192.168.0.208	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.209	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.210	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.211	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.212	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.213	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.214	Laboratorio Génesis
Estación de Trabajo (Clon INTEL 3)	192.168.0.215	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.216	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.217	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.218	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.219	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.220	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.221	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.222	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.223	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.224	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.225	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.226	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.227	Laboratorio PC2
Estación de Trabajo (Clon INTEL 3)	192.168.0.228	Laboratorio PC2
Estación de Trabajo (Imac G3)	192.168.0.229	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.230	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.231	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.232	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.233	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.234	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.235	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.236	Laboratorio Preescolar

Tabla A3.1 Distribución de direcciones IP		
Dispositivo	Dirección IP	Ubicación
Estación de Trabajo (Imac G3)	192.168.0.237	Laboratorio Preescolar
Estación de Trabajo (Imac G3)	192.168.0.238	Laboratorio Preescolar
Estación de trabajo (Power MAC G3)	192.168.0.239	Laboratorio Preescolar
Estación de trabajo (Power MAC G3)	192.168.0.240	Laboratorio Preescolar

ANEXO 4. CARACTERISTICAS DE LOS SWITCH 3COM

TABLA 4.1 SuperStack® 3 Switch 3300	
Dimensiones	Alto 76mm. Ancho 483 mm. Peso 4Kg.
Temperatura Operacional	0° to 50°C (32° to 122°F)
Temperatura Ambiente	-10° to +70°C (14° to 158°F)
Humedad	10–95% relative humidity
Características Eléctricas	Línea de Frecuencia AC 50/60 Hz Voltaje de Entrada 90 – 240 VAC Current Rating 3 amperios como máximo
Estándares	SNMP SNMP protocol (RFC 1157) MIB-II (RFC 1213) Bridge MIB (RFC 1493) Repeater MIB (RFC 1516) VLAN MIB (RFC 1573) RMON MIB (RFC 1271) BOOTP (RFC 951) Terminal Emulation Telnet (RFC 854)

	Protocols Used for Administration UDP (RFC 768) IP (RFC 791) ICMP (RFC 792) TCP (RFC 793) ARP (RFC 826) TFTP
Certificación	UL 1950, EN60950, CSA 22.2 No. 950, IEC 950
Modulo de Expansion	100BASE-FX para mayor velocidad

TABLA 4.1 SuperStack® II Baseline 10/100	
Dimensiones	Alto 70mm. Ancho 440 mm.Peso 4Kg.
Temperatura Operacional	0° to 50°C (32° to 122°F)
Temperatura Ambiente	-10° to +70°C (14° to 158°F)
Humedad	10-95% relative humidity
Características Eléctricas	Línea de Frecuencia AC 50/60 Hz Voltaje de Entrada 90 – 240 V AC Current Rating 3 amperios como máximo
Funcionalidad	ISO 8802-3, IEEE 802.3 (Ethernet), IEEE 802.3u (Fast Ethernet), IEEE 802.3x (Flow Control) Height 70mm (2.75in.) or 1.5U
Máximo poder de Disipación	628 BTU/hr

MDF: LABORATORIOS

Existen 49 enlaces de cable UTP categoría 5e que parten desde la sala de servidores a las áreas de trabajo. Todos los enlaces son internos en el edificio y pasan a través de canaleta decorativa de 2" empotrada en la pared a 40cm del piso, el detalle de los mismos se describe en la tabla 2.5.

Tabla 2.5: Detalle de enlaces edificio Laboratorios			
Enlace	Longitud (m)	Ubicación	Piso
# 01	09.30	Laboratorio iMac	PB
# 02	10.90	Laboratorio iMac	PB
# 03	10.90	Laboratorio iMac	PB
# 04	13.40	Laboratorio iMac	PB
# 05	13.60	Laboratorio iMac	PB
# 06	16.90	Laboratorio iMac	PB
# 07	18.20	Laboratorio iMac	PB
# 08	18.20	Laboratorio iMac	PB
# 09	23.30	Laboratorio iMac	PB
# 10	23.30	Laboratorio iMac	PB
# 11	13.00	Laboratorio iMac	PB
# 12	13.20	Laboratorio iMac	PB
# 13	26.90	Laboratorio iMac	PB
# 14	26.90	Laboratorio iMac	PB
# 15	07.40	Sala de servidores	PB
# 16	07.40	Sala de servidores	PB
# 17	29.30	Oficina Cómputo	PB
# 18	30.60	Oficina Cómputo	PB
# 19	27.10	Oficina Cómputo	PB
# 20	21.10	Oficina Cómputo	PB
# 21	21.10	Oficina Cómputo	PB
# 22	07.60	Laboratorio Génesis	PB
# 23	09.70	Laboratorio Génesis	PB

Tabla 2.5: Detalle de enlaces edificio Laboratorios			
Enlace	Longitud (m)	Ubicación	Piso
# 24	09.70	Laboratorio Génesis	PB
# 25	11.60	Laboratorio Génesis	PB
# 26	11.80	Laboratorio Génesis	PB
# 27	16.50	Laboratorio Génesis	PB
# 28	13.60	Laboratorio Génesis	PB
# 29	16.50	Laboratorio Génesis	PB
# 30	18.80	Laboratorio Génesis	PB
# 31	18.60	Laboratorio Génesis	PB
# 32	23.10	Laboratorio Génesis	PB
# 33	21.70	Laboratorio Génesis	PB
# 34	11.20	Laboratorio iMac	PB
# 35	24.80	Laboratorio Génesis	PB
# 36	26.90	Laboratorio Génesis	PB
# 37	26.90	Laboratorio Génesis	PB
# 38	24.00	Laboratorio de Física	PB
# 39	36.60	Laboratorio de Química	PB
# 40	46.30	Departamento médico	PB
# 41	53.10	Oficina de Mantenimiento	PB
# 42	14.00	Sala de servidores	PB
# 43	11.60	Sala de servidores	PB
# 44	11.60	Sala de servidores	PB
# 45	10.90	Sala de servidores	PB
# 46	16.90	Sala de servidores	PB
# 47	16.90	Sala de servidores	PB
# 48	12.60	Sala de servidores	PB
# 49	10.70	Sala de servidores	PB

IDF: INSPECCIÓN GENERAL

Existen 16 enlaces que parten de la oficina de inspección general y se distribuyen en las oficinas de los edificios Inspección General y Oficinas Departamentos. Los enlaces del edificio Inspección General pasan a través de canaleta decorativa de 2" empotrada en la pared a 40cm del piso; mientras que los enlaces que van hacia el edificio Oficinas Departamentos van por canaleta desde el origen hasta la Oficina de Letras, luego pasan por tubería de 1" enterrada a 80cm entre los dos edificios y finalmente pasan por canaleta decorativa hasta llegar a su destino. El detalle de los enlaces de esta zona se muestra en las tablas 2.6 y 2.7.

Enlace	Longitud (m)	Ubicación	Piso
# 01	05.60	Inspección general	PB
# 02	05.80	Inspección general	PB
# 03	05.80	Inspección general	PB
# 04	07.00	Consejo estudiantil	PB
# 05	08.00	Departamento de Ciencias Sociales	PB
# 06	09.70	Departamento de Ciencias Sociales	PB
# 07	11.40	Departamento de Letras	PB
# 08	11.60	Departamento de Letras	PB
# 09	14.00	Departamento de Cultura Judía	PB
# 10	14.00	Departamento de Cultura Judía	PB

Enlace	Longitud (m)	Ubicación	Piso
# 11	39.20	Departamento de Idiomas	PB
# 12	39.90	Departamento de Idiomas	PB
# 13	40.70	Departamento de Idiomas	PB
# 14	46.70	Departamento de Ciencias Experimentales	PB

# 15	46.70	Departamento de Ciencias Experimentales	PB
# 16	48.30	Departamento de Ciencias Experimentales	PB

SDF 1: PRIMARIA 1

Existen 7 enlaces que parten de la oficina de Subinspección en el edificio Primaria 1, 4 enlaces se distribuyen en las oficinas de este edificio, 2 en el edificio Cafetería y 1 en el edificio Primaria 2. Los enlaces del edificio Primaria 1 pasan a través de canaleta decorativa de 2" empotrada en la pared a 40cm del piso; mientras que los enlaces que van hacia los otros edificios van por canaleta hasta salir del edificio Primaria 1, luego pasan por tubería de 1" enterrada a 80cm entre los edificios y finalmente pasan por canaleta decorativa hasta llegar a su destino. El detalle de los enlaces de esta zona se muestra en las tablas 2.8.

Tabla 2.8: Detalle de enlaces edificios Primaria 1, Primaria 2 y Cafetería			
Enlace	Longitud (m)	Ubicación	Piso
# 01	54.50	Cafetería – Cafetería	PB
# 02	54.10	Aula de recursos – Primaria 2	PB
# 03	51.80	Aula de música – Cafetería	PB
# 04	21.50	Recuperación Psicopedagógica – Primaria 1	PB
# 05	12.60	Subinspección – Primaria 1	PB
# 06	10.90	Subinspección – Primaria 1	PB
# 07	07.00	Subinspección – Primaria 1	PB

SDF 2: BIBLIOTECA

Existen 8 enlaces de cable UTP categoría 5e que parten desde la sala de audiovisuales a las áreas de trabajo. Todos los enlaces son internos en el edificio y pasan a través de canaleta decorativa de 2" empotrada en la pared, el detalle de los mismos se describe en la tabla 2.9.

Tabla 2.9: Detalle de enlaces edificio Biblioteca			
Enlace	Longitud (m)	Ubicación	Piso

# 01	08.30	Sala de audiovisuales	PB
# 02	10.50	Sala de audiovisuales	PB
# 03	26.40	Sala de audiovisuales	PB
# 04	34.90	Oficina Biblioteca	PB
# 05	37.80	Oficina Biblioteca	PB
# 06	38.00	Sala de lectura	PB
# 07	40.90	Sala de lectura	PB
# 08	40.90	Sala de lectura	PB

SDF 3: ADMINISTRACIÓN

Existen 18 enlaces de cable UTP categoría 5e que parten desde el rack de pared ubicado junto a la cafetería hacia cada una de las áreas de trabajo del edificio. Existen 16 enlaces que son internos en el edificio y pasan a través de canaleta decorativa de 2" empotrada en la pared y dos enlaces ubicados en garita y que pasan por canaleta hasta salir del edificio, luego pasan a través de ducto de manguera de 1" hasta llegar a la garita y finalmente por canaleta hasta llegar a su destino, el detalle de cada enlace se describe en la tabla 2.10.

Enlace	Longitud (m)	Ubicación	Piso
# 01	20.70	Recepción	PB
# 02	24.20	Recepción	PB
# 03	29.70	Secretaría General	PB
# 04	43.20	Operaciones	PB
# 05	48.50	Operaciones	PB
# 06	53.70	Garita	PB
# 07	47.30	Operaciones	PB
# 08	45.00	Operaciones	PB
# 09	54.50	Garita	PB
# 10	17.80	Secretaría General	PB
# 11	30.80	Secretaría Rectorado	PB

# 12	26.90	Rectorado	PB
# 13	42.30	Departamento de Comunicación	PB
# 14	41.50	Secretaría Gerencia	PB
# 15	38.40	Gerencia	PB
# 16	40.10	Gerencia	PB
# 17	28.10	Rectorado	PB
# 18	43.00	Operaciones	PB
# 19	20.00	Mantenimiento	PA
# 20	28.00	Seguridad	PA
# 21	43.00	Suministros	PA

SDF 4: SECUNDARIA

Existen 13 enlaces de cable UTP categoría 5e que parten desde el rack de pared ubicado junto a la Sala de sesiones de Vicerrectorado hacia las áreas de trabajo del bloque 3 del edificio Secundaria y del edificio Gimnasio. Existen 10 enlaces que son internos en el edificio y pasan a través de canaleta decorativa de 2" empotrada en la pared y dos enlaces ubicados en garita y que pasan por canaleta hasta salir del edificio, luego pasan a través de ducto de manguera de 1" hasta llegar a la oficina de Deportes en el edificio Gimnasio y finalmente por canaleta hasta llegar a su destino, el detalle de cada enlace se describe en la tabla 2.11.

Enlace	Longitud (m)	Ubicación	Piso
# 01	08.00	Asesoría universitaria	PA
# 02	12.00	Secretaria vicerrectorado	PA
# 03	13.80	Secretaria vicerrectorado	PA
# 04	15.50	Vicerrectorado	PA
# 05	15.70	Experimentación	PA
# 06	18.20	Psicología	PB
# 07	21.10	Departamento de Arte	PB
# 08	22.70	Departamento de Arte	PB

# 09	25.60	Audiovisuales	PB
# 10	31.20	Audiovisuales	PB
# 11	81.40	Departamento de Deportes - Gimnasio	PB
# 12	82.40	Departamento de Deportes - Gimnasio	PB
# 13	89.00	Departamento de Deportes - Gimnasio	PB

SDF 5: PREESCOLAR

Existen 16 enlaces de cable UTP categoría 5e que parten desde la el laboratorio de computadoras iMac a las áreas de trabajo. Todos los enlaces son internos en el edificio y pasan a través de canaleta decorativa de 2" empotrada en la pared, el detalle de los mismos se describe en la tabla 2.12.

Tabla 2.12: Detalle de enlaces edificio Laboratorio Preescolar			
Enlace	Longitud (m)	Ubicación	Piso
# 01	11.60	Laboratorio Preescolar	PB
# 02	09.10	Laboratorio Preescolar	PB
# 03	08.90	Laboratorio Preescolar	PB
# 04	07.80	Laboratorio Preescolar	PB
# 05	07.80	Laboratorio Preescolar	PB
# 06	06.60	Laboratorio Preescolar	PB
# 07	10.10	Laboratorio Preescolar	PB
# 08	09.50	Laboratorio Preescolar	PB
# 09	09.50	Laboratorio Preescolar	PB
# 10	25.60	Coordinación Sección Inicial	PB
# 11	11.60	Laboratorio Preescolar	PB
# 12	11.60	Laboratorio Preescolar	PB
# 13	30.00	Coordinación Sección Inicial	PB
# 14	10.50	Laboratorio Preescolar	PB
# 15	26.20	Coordinación Sección Inicial	PB

Enlace	Longitud (m)	Ubicación	Piso
# 16	10.50	Laboratorio Preescolar	PB