



**UNIVERSIDAD NACIONAL  
PEDRO RUIZ GALLO**



**FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS  
ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA**

## **TESIS**

---

**“SISTEMA INTEGRADO DE VIDEOVIGILANCIA IP Y  
CONTROL DE ACCESO PARA MEJORAR LA SEGURIDAD  
EN LAS INSTALACIONES DEL MERCADO CENTRAL DE  
CHICLAYO”**

---

PARA OPTAR POR EL TÍTULO PROFESIONAL DE:

**INGENIERO ELECTRÓNICO**

### **AUTORES:**

Bach. FERNÁNDEZ CUSMA, Jorge Artemio

Bach. GAMARRA FIESTAS, Luis Angel

### **ASESORA:**

Ing. CHAMÁN CABRERA, Lucía Isabel

LAMBAYEQUE – PERU  
2015



UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO  
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS  
ESCUELA PROFESIONAL DE INGENIERIA ELECTRONICA



## **SISTEMA INTEGRADO DE VIDEOVIGILANCIA IP Y CONTROL DE ACCESO PARA MEJORAR LA SEGURIDAD EN LAS INSTALACIONES DEL MERCADO CENTRAL DE CHICLAYO**

### **Por:**

Bach. FERNÁNDEZ CUSMA, Jorge Artemio

Bach. GAMARRA FIESTAS, Luis Angel

### **Aprobado por:**

---

Ing. Ramírez Castro, Manuel Javier  
**Presidente del Jurado**

---

Ing. Chiclayo Padilla, Hugo Javier  
**Secretario**

---

Ing. Nombera Lossio, Martín Augusto  
**Vocal**

### **Asesora:**

---

Ing. CHAMÁN CABRERA, Lucía Isabel



## DEDICATORIA

A ti mi Dios que me diste la vida y me regalaste una familia maravillosa.

A mis padres Jorge y Angélica, quienes con su sacrificio y esfuerzo, han logrado guiarme por un camino de rectitud, respeto, orden y dedicación.

A mis hermanas, quienes con su paciencia, sus palabras y apoyo incondicional, supieron elevar mis perspectivas y aspiraciones que en su momento se vieron limitadas.

A mis pequeños sobrinos, quienes con ternura y cariño han sido una gran motivación emocional.

Ellos, mi familia, han sido y serán el motor y motivo de cada cosa que logre en mi vida. Siempre creyeron en mí y lo seguirán haciendo.

"Hay hombres que luchan un día y son buenos. Hay otros que luchan un año y son mejores. Hay quienes luchan muchos años, y son muy buenos. Pero hay los que luchan toda la vida, esos son los imprescindibles".

**Bertolt Brecht**

*Jorge Artemio*



## DEDICATORIA

A Dios, por darme salud cada día de mi vida.

A mis padres Walter y María, porque gracias a ellos puedo obtener este logro.

A mis hermanos, Walter y Victoria, porque ambos siempre me han brindado su apoyo cuando más lo necesitaba.

*Luis Angel*



## AGRADECIMIENTO

Al creador de todas las cosas, ser maravilloso que nos dio fuerzas y fe para creer en lo que parecía imposible terminar.

A nuestra familia por su confianza, apoyo y comprensión.

A nuestros compañeros y amigos, presentes y del pasado quienes sin esperar nada a cambio compartieron sus conocimientos, tiempo y nos brindaron su ayuda cuando se necesitaba.

A la Ing. Lucía Isabel Chamán Cabrera por su asesoramiento, tolerancia y amistad desde que se puso en marcha la elaboración de nuestra tesis.

A nuestros mentores de la UNPRG. Ellos han servido de base en nuestra formación profesional y futuros logros.

*Los Autores*



## INTRODUCCIÓN

En la actualidad la inseguridad en el mundo ha pasado de ser un problema y se ha convertido en una de las principales características de todas las sociedades modernas. En Perú, como en toda Latinoamérica, la violencia y la delincuencia, experimenta en los últimos años un aumento en gran proporción, que más haya de solo dejar en la población una percepción de inseguridad, traducida en temor y zozobra, obstaculizan el crecimiento económico y la reducción de la pobreza.

En este contexto y con la reducción de la brecha tecnológica entre países del primer mundo y los países en desarrollo, es posible contar con modernos equipos que hacen posible implementar sistemas de seguridad que proporcionen un medio de disuasión, prevención y detección de actos delictivos.

En la zona norte del país, Chiclayo es una de las ciudades con un aumento demográfico y económico significativo, esto a su vez ha conllevado paralelamente a elevar el índice de inseguridad. Es así, el caso de “El Mercado Central de Chiclayo”, que por muchos años ha sido un centro comercial minorista, con una ubicación en pleno centro de Chiclayo, así pues cuenta con 4 puertas de acceso, por importantes calles y avenidas, de Chiclayo (Av. José Balta, Calle Lora y Cordero, Av. Vicente de la Vega, Calle Alfredo Lapoint), lo que ha hecho posible se convierta en un centro comercial de gran importancia en la adquisición de bienes y servicios por parte de un gran sector de la población chiclayana, esto ha contribuido significativamente al desarrollo económico chiclayano.



Dada la importancia, ubicación y magnitud del “Mercado Central de Chiclayo”, hace posible se realice un comercio sostenible, con la afluencia de personas, tanto chiclayanos, como foráneos; pero no todos llegan a sus instalaciones a realizar actividades económicas, es sabido que este comercio diario, resulta atractivo para quienes de manera ilícita (delinquiendo), buscan beneficiarse del movimiento económico que se da a diario, por lo tanto existe la percepción de inseguridad, alterando el normal desenvolvimiento de las actividades dentro de sus instalaciones.

Se ha podido observar, la carencia de sistemas de seguridad que proporcionen un medio de disuasión, prevención y detección de actos delictivos contra los compradores, consumidores, trabajadores y bienes del “Mercado Central de Chiclayo”. En tal medida esta situación ha motivado a la realización del presente proyecto de tesis que tiene como objetivo el diseño de un Sistema Integrado de Videovigilancia IP y control de acceso, como base propuesta para una futura implementación.



## RESUMEN

En la actualidad existen dos conceptos que se están desarrollando ampliamente en el área de las comunicaciones: la tecnología de información y la seguridad, encontrándose los dos en proceso de convergencia. Estos dos desarrollos han creado el interés de soluciones basadas en la utilización de una red IP, que hace posible se diseñe un sistema de seguridad integrado, con un sistema de control de acceso.

En el presente proyecto de tesis se desarrolla el diseño de un sistema de seguridad integrado: Videovigilancia IP y Control de Acceso; utilizando una red muy difundida como es la red IP y la transmisión por cable, como red troncal para transportar video y audio digital, y otros datos. Así también aplicaremos la tecnología de alimentación a través de Ethernet (POE), permitiéndonos utilizar la red para transportar alimentación a los equipos que se consideran distribuir en las instalaciones del “Mercado Central de Chiclayo” y forman parte del proyecto.

Como todo proyecto, se realiza un estudio previo del grado de inseguridad percibida en el mercado, el cual sustenta el desarrollo de nuestro trabajo. Por otra parte se analiza la infraestructura, distribución eléctrica y demás factores a tener en consideración antes de la elaboración del diseño de seguridad integrado.

Se tendrá en consideración los diferentes equipos de TI estándar y el sistema en red, como son las cámaras IP, unidades de acceso, routers, switches, NVR, patch panel, rack, así también software de gestión de video y de la unidad de control de acceso. Software que permitirá el monitoreo interno (LAN) o un monitoreo remoto en un navegador web (WAN), de las incidencias ocurridas.

Asimismo este estudio servirá para la posterior implementación en cualquier otra aplicación que se requiera.





## ABSTRACT

Nowadays, there are two concepts that are being widely developed in the area of communications: information technology and security, being both in the process of convergence. These two developments have created interest based on the use of an IP network solutions that enables an integrated security system is designed with an access control system.

In this thesis project which is designed an integrated security system : IP CCTV and Access Control ; using a widespread network like the IP network , cable transmission , the backbone for transporting digital video and audio, and other data. We will apply technology power over Ethernet (POE), allowing us to use the network to transport food to the equipment that is considered to distribute facilities to the Central Market of Chiclayo as a part of the project.

Like any project, a previous study of the degree of perceived uncertainty in the market, which supports the development of our work. Moreover infrastructure, electrical distribution and other factors are analyzed in order to take them into consideration before developing integrated design safety.

We will take into consideration different equipment of IT standard and network system, such as IP cameras, access units, routers, switches, NVR, patch panel, rack, video management software and control unit access. Software that will allow internal monitoring (LAN) or remote monitoring in a web browser (WAN), of the occurred incidents.

Also, this study will help to improve further implementation in other applications required.



# ÍNDICE GENERAL

DEDICATORIA.....	I
AGRADECIMIENTO.....	III
INTRODUCCION.....	IV
RESUMEN.....	VI
ABSTRACT.....	VII
<b>1 CAPÍTULO 1 .....</b>	<b>1</b>
<b>ASPECTOS GENERALES DEL PROYECTO .....</b>	<b>1</b>
1.1 SITUACIÓN PROBLEMÁTICA .....	1
1.2 FORMULACIÓN DEL PROBLEMA CIENTÍFICO .....	2
1.3 HIPÓTESIS .....	2
1.4 JUSTIFICACIÓN .....	2
1.5 OBJETIVOS .....	3
1.5.1 OBJETIVO GENERAL .....	3
1.5.2 OBJETIVOS ESPECIFICOS .....	3
<b>2 CAPITULO 2 .....</b>	<b>4</b>
<b>MARCO TEORICO.....</b>	<b>4</b>
2.1 ANTECEDENTES .....	4
2.2 BASES TEÓRICAS .....	10
2.2.1 REDES Y DISPOSITIVOS DE RED .....	11
2.2.1.1 RED DE DATOS .....	11
2.2.1.2 CARACTERISTICAS DE LAS REDES.....	12
2.2.1.3 REDES DE AREA LOCAL (LAN) .....	15
2.2.1.4 TOPOLOGIA DE RED .....	19
2.2.1.5 MODELO OSI .....	22
2.2.1.6 MODELO TCP/IP .....	23
2.2.1.7 MEDIO DE RED:.....	24
2.2.1.8 VIDEOVIGILANCIA IP .....	34
2.2.1.8.1 VENTAJAS DE LA VIDEOVIGILANCIA IP .....	34
2.2.1.8.2 COMPONENTES DE UN SISTEMA DE VIDEOVIGILANCIA IP .....	37
2.2.1.9 SISTEMA DE CONTROL DE ACCESO .....	45
2.2.1.9.1 BENEFICIOS DEL CONTROL DE ACCESO .....	46
2.2.1.9.2 PRINCIPALES DISPOSITIVOS PARA CONTROL DE ACCESO Y CONTROL DE ASISTENCIA. ....	47
2.2.1.10 SISTEMA DE CABLEADO ESTRUCTURADO.....	48
2.2.1.10.1 SISTEMA DE CABLEADO ESTRUCTURADO DE LAS LAN .....	48
2.2.1.10.2 SUBSISTEMAS DE CABLEADO ESTRUCTURADO .....	49



<b>3</b>	<b>CAPITULO 3 .....</b>	<b>51</b>
	<b>PROPUESTA DE DISEÑO .....</b>	<b>51</b>
3.1	HIPOTESIS DE LA SOLUCIÓN PROPUESTA.....	51
3.2	OBJETIVOS DE LA SOLUCIÓN PROPUESTA.....	52
3.3	ZONA DE DISEÑO. ....	53
3.4	CONSIDERACIONES PARA EL DISEÑO.....	54
3.4.1	SISTEMA DE VIDEOVIGILANCIA IP. ....	54
3.4.2	CÁMARA DE RED. ....	54
3.4.3	USO DE ANCHO DE BANDA. ....	55
3.4.4	SEGURIDAD.....	56
3.4.5	PROTECCIÓN FÍSICA DE LAS CÁMARAS.....	57
3.4.5.1	DISEÑO DE LA CÁMARA/CARACA.....	57
3.4.5.2	CUBIERTA TRANSPARENTE .....	58
3.4.5.3	MONTAJE.....	58
3.4.5.4	TIPOS DE MONTAJE .....	59
3.4.5.5	COLOCACIÓN DE CÁMARAS.....	61
3.4.5.6	VIDEO INTELIGENTE. ....	61
3.4.6	COMPRESIÓN. ....	62
3.4.6.1	H264 .....	62
3.4.6.2	MJPEG .....	62
3.4.6.3	MPEG4 .....	63
3.4.7	ALMACENAMIENTO. ....	63
3.4.7.1	CÁLCULO EN H.264.....	64
3.4.7.2	CÁLCULO EN MPEG-4 .....	64
3.4.7.3	CÁLCULO EN MOTION JPEG.....	65
3.4.8	SISTEMA DE CONTROL DE ACCESO .....	66
3.4.8.1	BENEFICIOS DE UN SISTEMA DE CONTROL DE ACCESOS:.....	67
3.4.8.2	CONTROL DE PERSONAL .....	67
3.5	PRESENTACION DE DISEÑO. ....	68
3.5.1	ENTORNO DEL SISTEMA.....	70
3.5.1.1	ELECCIÓN DEL FORMATO DE COMPRESIÓN .....	70
3.5.1.2	PARÁMETROS DE LAS CÁMARAS.....	70
3.5.1.2.1	SENSOR DE IMAGEN. ....	71
3.5.1.2.2	TAMAÑO DEL SENSOR.....	74
3.5.1.2.3	SELECCIÓN DEL TIPO DE LENTE. ....	75
3.5.1.2.4	CÁLCULOS DEL DISEÑO.....	79
3.5.1.3	CAPACIDAD DE ALMACENAMIENTO.....	89
3.5.1.4	DISTRIBUCIÓN DE LAS CÁMARAS IP Y UNIDAD DE CONTROL DE ACCESO.....	91
3.5.1.4.1	MEDIDAS .....	92
3.5.1.4.2	DISTRIBUCIÓN.....	95
3.5.1.5	CÁLCULO DEL ANCHO DE BANDA. ....	100
3.5.2	ENTORNO DE LA RED. ....	102
3.5.2.1	CABLEADO .....	103



3.5.2.1.1 CABLE UTP .....	104
3.5.2.1.2 CONECTOR RJ-45 .....	105
3.5.2.1.3 CABLE COAXIAL RG-6 .....	105
3.5.2.1.4 CONECTOR BNC .....	106
3.5.2.1.5 PoE ETHERNET EXTENDER SET OVER COAXIAL .....	107
3.5.2.2 ELEMENTOS DEL SISTEMA .....	108
3.5.2.2.1 CÁMARAS IP. ....	108
3.5.2.2.2 GRABADORA DE VIDEO (NVR).....	112
3.5.2.2.3 UNIDAD DE ACCESO POR HUELLA DIGITAL.....	114
3.5.2.2.4 COMPUTADORA .....	115
3.5.2.2.5 MONITOR PARA VISUALIZACIÓN DE LAS .....	116
3.5.2.2.6 ROUTER .....	123
3.5.2.2.7 CONMUTADOR .....	124
<b>4 CAPITULO 4 .....</b>	<b>127</b>
<b>PRESUPUESTO.....</b>	<b>127</b>
<b>5 CAPITULO 5 .....</b>	<b>131</b>
<b>CONCLUSIONES Y RECOMENDACIONES.....</b>	<b>131</b>
5.1 CONCLUSIONES.....	131
5.2 RECOMENDACIONES.....	132
<b>6 CAPITULO 6 .....</b>	<b>133</b>
<b>FUENTES DE REFERENCIA .....</b>	<b>133</b>
<b>7 CAPITULO 7 .....</b>	<b>138</b>
<b>ANEXOS .....</b>	<b>138</b>
7.1 ANEXO A:.....	138
PLANO DEL SISTEMA DE VIDEOVIGILANCIA IP Y CONTROL DE ACCESO.....	138
7.2 ANEXO B:.....	138
PLANO DE SECTORIZACION .....	138
7.3 ANEXO C: .....	138
DATASHEET .....	138



## ÍNDICE TABLAS

Tabla 1.Norma T568A: Orden de colores .....	27
Tabla 2.Norma T568B: Orden de colores .....	27
Tabla 3.Capacidad de almacenamiento: Formato H.264 .....	64
Tabla 4.Capacidad de almacenamiento: Formato MPEG-4.....	65
Tabla 5.Capacidad de almacenamiento: Formato JPEG .....	66
Tabla 6.Relación entre lente y el tamaño del sensor. ....	78
Tabla 7.Consumo eléctrico de los elementos del Sistema.....	120
Tabla 8.Modelo, cantidad de equipos y materiales a utilizar.....	128
Tabla 9.Precio de equipos y accesorios a utilizar (incluyen IGV).....	130



## ÍNDICE GRAFICOS

Figura 1.Eschema de una Red de Datos.....	11
Figura 2.Distribución de una Red LAN.....	18
Figura 3.Topología Físicas de Redes de Computadoras.....	20
Figura 4.Capas que componen el Modelo OSI.....	22
Figura 5.Capas que componen el Modelo TCP/IP.....	24
Figura 6.Cable UTP.....	25
Figura 7.Normas de Ponchado.....	28
Figura 8.Conector RJ45.....	28
Figura 9.Cable directo y cruzado.....	29
Figura 10.Cable Coaxial.....	30
Figura 11.Conectores para cable Coaxial.....	33
Figura 12.Conectores Machos.....	33
Figura 13.Conectores Hembra.....	33
Figura 14.Un sistema que utiliza la Alimentación a través de Ethernet.....	37
Figura 15.Tipos de cámaras IP.....	41
Figura 16.Sistema NVR.....	42
Figura 17.Switch de 24 puertos CISCO.....	43
Figura 18.Router CISCO 2801.....	44
Figura 19.Patch Panel.....	45
Figura 20.Sistema de seguridad con Control de Acceso.....	46
Figura 21.Reconocimiento facial y lector dactilar.....	47
Figura 22.Dispositivos para Control de Acceso.....	48
Figura 23.Subsistemas de Cableado Estructurado.....	50
Figura 24.Tipos de carcasa.....	57
Figura 25.Carcasas para cámaras de red fijas montadas a ras del techo.....	59
Figura 26.Montaje en superficie (izquierda), un montaje empotrado (centro) y un montaje colgante (derecha).....	60
Figura 27.Montaje en parapeto.....	61
Figura 28.Unidad de Control de Acceso.....	68
Figura 29.Arquitectura de una cámara IP.....	71
Figura 30.Relacion de tamaños entre el lente y sensor.....	74
Figura 31.Lente Fijo.....	76
Figura 32.Lente Varifocal.....	76
Figura 33.Apertura del lente.....	77
Figura 34.Apertura Relativa.....	79
Figura 35.Dibujo de instalación de Cámaras (Relación de aspecto 3:4).....	81
Figura 36.Vista 3D – Relación de aspectos 3:4.....	82



Figura 37.Relación de aspectos 4:3.....	82
Figura 38.Visión con una distancia focal de 12mm.....	83
Figura 39.Dibujo de instalación de Cámaras (Relación de aspecto 3:4).....	84
Figura 40.Vista 3D – Relación de aspecto 3:4 (Cámara 1).....	85
Figura 41.Vista 3D – Relación de aspecto 3:4 (Cámara 2).....	85
Figura 42.Vista NVR- Relación de aspecto 3:4.....	86
Figura 43.Dibujo de instalación de Cámaras (Relación de aspecto 4:3).....	87
Figura 44.Vista 3D- Relación de aspecto 4:3.....	88
Figura 45.Vista en el plano del Área de administración. ....	89
Figura 46.Almacenamiento-Cámara HKDS2CD2732 F – I. ....	90
Figura 47.Almacenamiento-Cámara HKDS2CD2132 - I. ....	90
Figura 48.Almacenamiento-Cámara HKDS2CD8253F – EI.....	91
Figura 49.Plano sectorizado en AutoCAD del “Mercado Central de Chiclayo”. ....	92
Figura 50.Primer Sector: Medidas de referencia para la colocación de las cámaras IP.....	93
Figura 51.Segundo Sector: Medidas de referencia para la colocación de las cámaras IP.....	94
Figura 52.Tercer Sector: Medidas de referencia para la colocación de las cámaras IP.....	94
Figura 53.Cuarto Sector: Medidas de referencia para la colocación de las cámaras IP.....	95
Figura 54.Sector 1 – Mercado Central de Chiclayo. ....	96
Figura 55.Sector 2 – Mercado Central de Chiclayo. ....	97
Figura 56.Sector 3 – Mercado Central de Chiclayo. ....	98
Figura 57.Sector 4 – Mercado Central de Chiclayo. ....	99
Figura 58.Unidad de control de acceso ubicada en el Sector 1 Administración.....	100
Figura 59.Ancho de Banda - HKDS2CD2732 F – I.....	101
Figura 60.Ancho de Banda - HKDS2CD2132 - I.....	101
Figura 61.Ancho de Banda - HKDS2CD8253F – EI.....	101
Figura 62.Red del Sistema integrado de Videovigilancia IP y.....	103
Figura 63.Cable UTP Cat. 6.....	104
Figura 64.Conector RJ-45.....	105
Figura 65.Cable coaxial RG6.....	106
Figura 66.Conector BNC macho.....	106
Figura 67.Elementos extensores PoE.....	107
Figura 68.Conexión de los elementos extensores con el RG6. ....	108
Figura 69.Cámara IP HIKVISION.....	110
Figura 70.Cámara IP HIKVISION.....	111
Figura 71.Cámara IP HIKVISION.....	112
Figura 72. NVR QNAP.....	113
Figura 73. Unidad de Control de Acceso ZKSoftware.....	115
Figura 74. Computadora Core i3 ADVANCE .....	116



Figura 75. Monitor SANSUNG. ....	119
Figura 76. Sistema de alimentación ininterrumpida. ....	122
Figura 77. 5PORT GIGA ETHERNET.....	124
Figura 78. Conmutador HP. ....	126





# 1 CAPÍTULO 1

## ASPECTOS GENERALES DEL PROYECTO

### 1.1 SITUACIÓN PROBLEMÁTICA

En Chiclayo uno de los principales centros de abastos minoristas es “El Mercado Central de Chiclayo”, aquí el comercio diario y la afluencia de personas, han hecho que se mantenga vigente por muchos años y estos últimos años no han sido la excepción frente a los grandes supermercados que pretenden acaparar el comercio chiclayano. También es la ubicación, un factor que ha contribuido para que “El Mercado Central de Chiclayo” sea concurrido por un gran sector de la población chiclayana e incluso foránea.

La importancia del “Mercado Central de Chiclayo” obliga a contar con medios que garanticen el desarrollo normal de las actividades económicas realizadas. Es así que, para evitar los actos delictivos, se cuenta con un servicio de guardianía, pero a resultado no ser suficiente para disminuir el índice de inseguridad percibida.

La carencia de medidas disuasivas y de detección, ponen en riesgo el comercio que se desarrolla en sus instalaciones. Esta problemática ha sido solucionada en otros centros comerciales, como los supermercados.

En este contexto conlleva a plantear el diseño de un sistema de seguridad integrado, que brinde una Videovigilancia IP y un control de acceso en el ingreso tanto al mercado, como en áreas para personal autorizado. De esta manera la sensación de seguridad percibida, permitirá que la actividad económica realizada en “El Mercado Central de Chiclayo”, no se vea afectada.



## **1.2 FORMULACIÓN DEL PROBLEMA CIENTÍFICO**

¿De qué manera el diseño de un Sistema Integrado de Videovigilancia IP y Control de Acceso como base mejoraría la seguridad en las instalaciones del Mercado Central de Chiclayo?

## **1.3 HIPÓTESIS**

Si se diseña un Sistema Integrado de Videovigilancia IP y Control de Acceso entonces mejoraría la seguridad en las instalaciones del Mercado Central de Chiclayo.

## **1.4 JUSTIFICACIÓN**

El desarrollo de esta investigación, permitirá establecer las bases necesarias para la posterior implementación de un Sistema Integrado de Videovigilancia IP, con un control de acceso. Empleando la tecnología actual, es posible mejorar la seguridad en las instalaciones del mercado central de Chiclayo: contar con un control de acceso a las instalaciones y/o áreas específicas para el personal autorizado y el monitoreo por medio de cámaras IP, estratégicamente distribuidas, permitirán disuadir, prevenir y detectar actos delictivos. Se hace necesario emplear medios de seguridad, debido a que en estos momentos la ciudad de Chiclayo -como otras ciudades de nuestro país- presenta un aumento exponencial en el índice de inseguridad percibida y esta se ve reflejada en los lugares de gran afluencia de personas como es “El Mercado Central de Chiclayo”. En tal contexto, resulta necesario plantear un proyecto, como medida atenuante a un problema social latente en estos días.



## **1.5 OBJETIVOS**

### **1.5.1 OBJETIVO GENERAL**

Diseñar un Sistema Integrado de Videovigilancia IP y Control de Acceso como base para mejorar la seguridad en las instalaciones del Mercado Central de Chiclayo.

### **1.5.2 OBJETIVOS ESPECIFICOS**

- Estudiar las diferentes tecnologías aplicadas a la videovigilancia y control de acceso.
- Examinar la estructura de las instalaciones del mercado, los puntos de alimentación eléctrica disponibles, ductería y la manera óptima de interconectar los diferentes tipos de cámaras IP a emplear, así como la disposición de la unidad de control de acceso.
- Diseñar la red lógica fundada sobre una plataforma IP con servidores para la grabación de cámaras full HD.
- Diseñar un sistema de Control de Accesos, basada en el reconocimiento de huella digital. Permitirá restringir el acceso a personal no autorizado, al área que será, el centro de monitoreo. A la vez se realizara un control diario, que se almacenara en su base de datos; permitirá precisar el ingreso y salida del personal.
- Plantear una disposición óptima de los equipos de seguridad en las instalaciones del Mercado Central de Chiclayo.



## 2 CAPITULO 2

### MARCO TEORICO

#### 2.1 ANTECEDENTES

Se citan algunos trabajos profesionales, que se relacionan con nuestra investigación.

##### ❖ ANTECEDENTE 01:

TÍTULO: DISEÑO DE UN SISTEMA DE VIDEO VIGILANCIA IP PARA LA CORTE SUPERIOR DE JUSTICIA. - LA LIBERTAD” – LA LIBERTAD-PERU (2013).

AUTOR: PELÁEZ SALVADOR, JUAN ALEXANDER

OBJETIVO GENERAL:

**Mejorar la seguridad de los activos de la Corte Superior de Justicia - La Libertad, diseñando un sistema de video vigilancia IP.**

El presente proyecto se enfoca en el diseño e implementación de un Sistema de Videovigilancia para la corte superior de justicia en la libertad, dicho sistema se basa en la tecnología IP, con medios cableados distribuidos en las instalaciones de la institución, el mismo que interconectan las cámaras sensibles al movimiento y las cámaras nocturnas, tenidas en cuenta para el proyecto. El cableado se concentra en una sala de control y monitoreo que se ubica dentro del departamento de informática. En esta sala se con el equipo de backup, que almacenara la grabación de una semana, las 24 horas del día, previstas en el diseño, así como un UPS que garantiza 2 horas de fluido eléctrico en caso de apagones.



## CONCLUSIONES:

- Se logró atenuar la pérdida de activos e incluso expedientes de gran valor, también disuadir la manipulación de datos de vital importancia para la institución, como también la desconfiguración de equipos en horarios cuándo el local se encuentra cerrado.
- Se Redujo el costo de horas-hombre para la actividad del control de activos de 6.24% mensualmente.
- Se redujo en un 87.45% el tiempo de respuesta de consulta de acceso remoto en tiempo real, disminuyendo la relación en la cantidad de activos y de la emisión de reportes por pérdida de activos al 64.01% mensual.

## ❖ ANTECEDENTE 02:

**TÍTULO:** DISEÑO DE UN SISTEMA DE CCTV BASADO EN RED IP INALÁMBRICA PARA SEGURIDAD ES ESTACIONAMIENTOS VEHICULARES. – LIMA-PERU (2011).

**AUTOR:** FERNANDO RAÚL REY MANRIQUE

## OBJETIVO GENERAL:

La obtención de un sistema de vigilancia IP que tenga la posibilidad de monitorear localmente y a distancia (tele vigilancia), transmitiendo la información por medio inalámbrico, para la aplicación en estacionamientos vehiculares de gran extensión.

Se plantea utilizar la red IP, la cual es ampliamente conocida como base del sistema de vigilancia digital. El diseño propone la transmisión de información



Inalámbricamente, a fin de cubrir toda el área determinada de un estacionamiento, brindando un monitoreo local y remoto. De esta manera se prescinde del cableado que tendría que hacerse por cada cámara a utilizar, así la instalación y el cambio de cámara podría hacerse en cualquier lugar. Otro factor que se tiene en cuenta es el ancho de banda utilizado por los elementos que conforman el sistema de vigilancia IP, el cual no solo dependerá de su configuración y características, sino también de factores como el tamaño de la imagen, la compresión, la frecuencia de imagen (fotogramas por segundo) y la complejidad de la imagen.

## CONCLUSIONES:

- Se hace posible evitar los delitos e identificar a los autores de un robo o conducta indebida. Así también, se desarrolló los beneficios de la aplicación misma, como las avanzadas capacidades de búsqueda, y la posibilidad de estar grabando y revisando los archivos en forma simultánea.
- Se cumplió con cubrir todas las zonas del estacionamiento, con la instalación de 10 cámaras de red en tres zonas en las que se dividió el establecimiento, obteniendo una buena cobertura, transmisión y recepción de la información.
- Se demostró que un sistema de vigilancia basado en red IP puede resolver los problemas que ocurren en un sistema con tecnología analógica o DVR (Digital Video Recording), como lo son la calidad de imagen, medio de transmisión, tecnología de los equipos y el costo de manutención del sistema, sin implicar un alto costo sino, por el contrario, crear una alternativa económica.



- El sistema de vigilancia propuesto, utilizando en una red IP inalámbrica, a pesar de tener un costo mayor a la propuesta de un sistema inalámbrico, resulta beneficioso para un crecimiento del sistema cuando se requiera, debido a su escalabilidad que permite aumentar un equipo nuevo (dispositivo final), sin la necesidad de otros equipos adicionales, sino solo con la configuración necesaria, esto se traduce en una reducción de costo en consideración a un sistema analógico el cual requiere una reestructuración si se pretende adicionar elementos.

### ❖ ANTECEDENTE 03:

TÍTULO: SISTEMA DE CONTROL DE ACCESO CON RFID. –  
D.F.-MÉXICO (2008).

AUTOR: JORGE ALBERTO ALVARADO SÁNCHEZ

OBJETIVO GENERAL:

**Desarrollar un Sistema de control de acceso utilizando la tecnología RFID.**

El sistema de acceso que se planteó en este proyecto, se basa en el uso de la tecnología RFID, buscando definir las ventajas y desventajas de dicha tecnología para la realización del control de acceso de personal en múltiples puntos, así también definir una arquitectura que permita la integración de esta aplicación –control de acceso- con otros sistemas.



## CONCLUSIONES:

- La tecnología RFID, presenta características de adaptabilidad, las cuales resultaron idóneas para el proyecto desarrollado y ventajas frente a otras tecnologías que aún se encuentran en proceso de maduración, ya que les falta terminar de definir estándares. Existen limitantes en esta tecnología, como son las limitantes de lectura en medios líquidos y metales, regulaciones no definidas del impacto en la sociedad, en cuanto a la privacidad y seguridad. Resulta complicado que RFID remplace a otras tecnologías, por lo que resulta más factible es que RFID sirva de complemento y que en un futuro tal vez remplace algunas tecnologías de autoidentificación.
- Se logró un sistema funcional, que permite controlar el acceso en determinados puntos y una fácil configuración del sistema, esto hace posible agregar, quitar o modificar puntos de acceso, hasta donde el hardware lo permite. Por ventajas en cuanto a distancia se seleccionó el protocolo RS-485 (más de 1km), pensando en controlar lectores y/o actuadores a distancia. Este protocolo presenta limitantes con respecto a la conexión en red de 32 dispositivos, por lo que resulta necesario agregar una tarjeta RS232 al host, si se requiere agregar más dispositivos. La utilización de componentes RFID interconectados en redes Ethernet y Wifi, tiene la ventaja de no tener un limitante en el número de dispositivos en la red (cantidad de trafico soportado por los equipos de la red), esto también permite basarse en los esquemas de verificación de errores TCP/IP, permitiendo la retransmisión de paquetes si es necesario, lo que no sucede en una red RS-485, ya que este control debe ser hecho en capas más altas por la aplicación.





#### ❖ ANTECEDENTE 04:

**TÍTULO:** DISEÑO E IMPLEMENTACIÓN DE SISTEMA BIOMÉTRICO BASADO EN HUELLA DACTILAR PARA EL CONTROL DE ASISTENCIA EN LA DIRECCIÓN DE INFORMÁTICA Y SISTEMAS DEL LA GOBERNACIÓN DEL ESTADO BOLÍVAR. – BOLÍVAR-VENEZUELA (2011)

**AUTOR:** FABIOLA GONZÁLEZ N.

#### OBJETIVO GENERAL:

**Diseñar e Implementar Sistema Biométrico basado en Huella Dactilar para el Control de Asistencia en la Dirección de Informática y Sistemas del a Gobernación del Estado Bolívar.**

El presente trabajo plantea un sistema biométrico de huella dactilar que se orienta a mejorar y automatizar el control de asistencia en la dirección de informática y sistemas de la gobernación del estado de bolívar. El control de acceso basado en un sistema biométrico, hace posible contar con un módulo que permita contar con registros de entrada y salida, retrasos, ausencias, horas extras trabajadas, trabajadores con permiso, de vacaciones o reposos, con su respectivo reporte de cada empleado. El control de acceso y asistencia al personal, dado por este sistema biométrico es posible a través de una combinación de patrones de líneas, arcos, lazos, y círculos que está establecido por una huella digital humana como principal identificador de seguridad y precisión, que el equipo biométrico empleado es capaz de identificar y procesar.



## CONCLUSIONES:

- Se estableció que el sistema biométrico es una de las mejores medidas de seguridad en la autenticación de usuario, ya que se basa en características inherentes y que resultan inconfundibles a un usuario distinto.
- Una reducción en el tiempo y costo que implica los reportes, historial y procesamiento de datos referentes a las asistencias, retardo y faltas de los usuarios. Esto reportes permite que se haga un análisis estadísticos, los cuales fácilmente pueden llevarse a tablas comparativas y gráficos.
- Se observó una flexibilidad en la configuración del sistema frente a las necesidades establecidas.

## 2.2 BASES TEÓRICAS

A lo largo de los años han surgido diferentes propuestas destinadas a brindar seguridad en oficinas, residencias, industrias, mercados, etc., tales propuestas han sido desde sistemas de seguridad independientes, hasta los sistemas integrados, que con la tecnología actual, es posible contar con videovigilancia y unidades de control de acceso, convergentes en una misma red.

Para el desarrollo del presente estudio se necesita conocer las características de los elementos que conforman un sistema de seguridad integrado, tales como las cámaras IP, las unidades de control de acceso, medios de transmisión, protocolos, software y la tecnología actual.

## 2.2.1 REDES Y DISPOSITIVOS DE RED

### 2.2.1.1 RED DE DATOS

Las redes de datos nacen por una necesidad empresarial de transmitir información, modificarla y actualizarla de manera rápida y eficaz. Antes de que existieran las redes de datos los usuarios tenían que utilizar medios rígidos de almacenamiento de información y precisamente el desplazamiento de este medio lo hacía más complejo.

Debido a estos inconvenientes se llegó a la necesidad de desarrollar estándares para las tecnologías networking, estas traen tres soluciones principales.

1. Compartir información.
2. Compartir Hardware y Software.
3. Centralizando Administración y el soporte. [1]

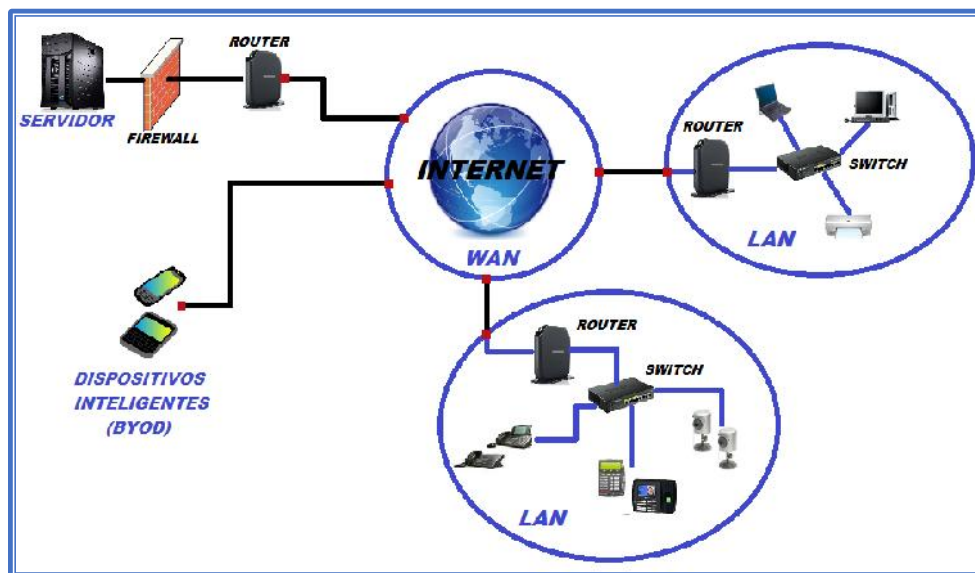


Figura 1. Esquema de una Red de Datos.  
Fuente: [Elaboración propia]



### 2.2.1.2 CARACTERISTICAS DE LAS REDES

- ❖ **Compartición de archivos:** La compartición de archivos requiere un directorio compartido o controlador de disco que pueda ser accesado por muchos usuarios de la red, junto con la lógica de programación asociada que se necesita para asegurarse de que más de una persona no realice cambios conflictivos a un archivo al mismo tiempo (llamado bloqueo de archivos)
- ❖ **Compartición de impresora:** Ésta puede llevarse a cabo de muchas maneras en una red. La más común es utilizar *colas de impresión* en un servidor. Una cola de impresión maneja trabajos de impresión hasta que se terminen de llevar a cabo y después, de forma automática, envía los trabajos en espera a la impresora.

Otra forma de compartir impresoras en una red es permitir que cada estación de trabajo acceda a la impresora directamente pero, generalmente, cada una deberá esperar su turno si muchas estaciones de trabajo quieren usar la impresora al mismo tiempo.
- ❖ **Servicio de aplicación:** De la misma forma en que usted puede compartir archivos en una red, con frecuencia también puede compartir aplicaciones. Por ejemplo, si posee el tipo de licencia de software, puede tener una copia compartida de Microsoft Office, o alguna otra aplicación, y conservarla en el servidor de la red, desde donde también puede trabajar con dicha copia. Cuando una estación de trabajo desea correr el programa, carga los archivos desde la red en su propia memoria, de la misma manera que lo haría desde un disco local y corre el programa como de costumbre. Mantener las aplicaciones en un punto central reduce la cantidad de espacio en disco necesario en cada estación de trabajo y facilita la administración de la aplicación.



❖ **Correo electrónico:** A grosso modo, los sistemas de correo electrónico se dividen en dos tipos: basados en archivos y cliente/servidor. El primero consiste en un conjunto de archivos que residen en una ubicación compartida en un servidor tipo el cual, en realidad, no hace nada más que proporcionar acceso a los archivos.

Un sistema de correo cliente/servidor consta de un servidor de correo electrónico que contiene el mensaje y maneja todas las interconexiones de correo electrónico, tanto dentro de la compañía como fuera de ella. Estos sistemas, como Microsoft Exchange o Lotus Notes, son más seguros y mucho más poderosos que los basados en archivos.

❖ **Acceso remoto:** Otro servicio importante para la mayoría de las redes es el acceso remoto a los recursos de éstas. Los usuarios utilizan esta característica para acceder a sus archivos y a su correo electrónico cuando se encuentran de viaje o trabajan desde una ubicación remota, como un hotel o sus casas. Existen muchos tipos de sistemas de acceso remoto. Algunos de los métodos que se utilizan para proporcionar acceso remoto se basan en:

- Establecer una conexión simple de servicio de acceso remoto (RAS) en un Windows Server, que pueda variar desde utilizar un solo módem hasta un banco de módems.
- Utilizar un sistema de acceso remoto dedicado, que maneje muchos módems y que generalmente incluya muchas computadoras, cada una en su propia tarjeta independiente.
- Emplear una estación de trabajo en la red y hacer que los usuarios marquen a ella mediante un programa de control remoto como PC Anywhere.



- Establecer una conexión de red privada virtual (VPN) a Internet, mediante la cual los usuarios pueden acceder a los recursos de la red de la compañía de manera confiable mediante internet.
- Instalar Windows Terminal Services (sobre Windows Servers) o Citrix MetaFrame, los cuales permiten que un solo Windows Server administre múltiples sesiones de cliente, cada uno de los cuales aparenta ser una computadora independiente para el usuario final.

❖ **Redes de área amplia:** Usted debe pensar en una red de área amplia (WAN) como un tipo de “metarred”. Una WAN es simplemente la conexión de varias redes de área local (LAN) entre sí. Este megasistema puede construirse de muchas formas en función de la frecuencia con que sea necesario conectar las LAN entre sí, cuánta capacidad de datos (ancho de banda) se requiere y cuál es la distancia entre las LAN.

Las WAN se instalan cuando los usuarios de una LAN necesitan acceder con mucha frecuencia a los recursos de otra LAN. Por ejemplo, un sistema para la planeación de recursos de una compañía (ERP) puede operar en las oficinas centrales de ella, pero la ubicación de la bodega necesita acceder a él a fin de poder utilizar sus funciones de inventario y embarque.

❖ **Internet e intranet:** Una conexión a Internet de una red consiste en una conexión de una red de telecomunicaciones a un ISP mediante una conexión como una línea privada DSL, una línea ISDN o una conexión DS1 (T-1) fraccional o total. Esta línea entra al edificio y se conecta a una caja llamada CSU/DSU (unidad de servicio de canal/unidad de servicio de datos), la cual convierte los datos de la forma en que se transportan por medio de la compañía telefónica local a una forma que pueda utilizar la LAN. La CSU/DSU, a su vez, se conecta a un ruteador que direcciona los paquetes de datos entre la red local e Internet.



Una intranet, como su nombre lo sugiere, es una red con enfoque interno que imita a una red Internet. En general, las intranets no se pueden acceder desde un punto fuera de la LAN (aunque sí es posible) y sólo son una versión mucho más pequeña de la Internet que una compañía instala para su propio uso.

- ❖ **Seguridad de la red:** La seguridad de la red se brinda por medio de una combinación de factores, dentro de los que se incluyen las características del NOS, la planta física del cableado, cómo se conecta la red a otras redes, las características de las estaciones de trabajo cliente, las acciones de los usuarios, las políticas de seguridad de la dirección y con qué eficiencia se deben implantar y administrar las características de seguridad. Todos estos aspectos forman una cadena, por lo cual una falla en cualquier enlace de la misma puede provocar que falle la red en su totalidad. Dependiendo de la compañía, cualquier falla en la seguridad de la red puede tener consecuencias severas, por lo que la seguridad es, en general, una parte extremadamente importante de cualquier red. [2]

### 2.2.1.3 REDES DE AREA LOCAL (LAN)

Son redes ubicadas en un área restringida, cuya propiedad es privada; pueden estar situadas en una oficina o en el edificio de la empresa. Las hogareñas también se consideran LAN siempre y cuando tengan, al menos, dos computadoras.

Los medios utilizados para conectarlas son los cables y/o el aire (el más común es el sistema WiFi, a través de un Access point), y los dispositivos de enlace (networking): hub, switch o router. Recordemos que estos componentes se explicarán con profundidad a lo largo de toda la obra.



La infraestructura varía según el tamaño del área por cubrir, la cantidad de usuarios que se pueden conectar, y el número y los tipos de servicios disponibles. Las características clave de las redes de área local para tener en cuenta son:

- Permiten impulsar tecnologías para compartir localmente archivos y hardware de manera eficiente y, así, permitir las comunicaciones internas.
- Son redes de propiedad privada, por ejemplo, una red hogareña, una oficina, una empresa o una pyme, entre otras.
- Se usan para conectar computadoras personales, con el objeto de compartir recursos e intercambiar información, y así facilitar el trabajo.
- Están restringidas en tamaño.
- Suelen emplear tecnología Ethernet (broadcast) mediante un cable sencillo (por ejemplo, UTP), a través del cual todas las computadoras se conectan a un nodo central (hub o switch).

Normalmente, las redes locales operan a velocidades que se encuentran entre 10 y 100 Mbps (megabits por segundo). En la actualidad, se manejan velocidades superiores, que van desde 1 Gb hasta 10 Gb, aunque estas últimas aún no se aplican en forma masiva; se planea su implementación a medida que aumente el tráfico de datos con el agregado de voz y video. Las redes de área local se destacan por tener bajo retardo y generar mínimos márgenes de error.

Los requerimientos que tienen hoy las redes LAN, de acuerdo con la demanda y las necesidades cotidianas, son:





- **Escalabilidad:** La red LAN debe poder absorber el crecimiento futuro, sobre la nueva red que se cree. Este detalle resulta clave, dado que una red no siempre se arma desde cero, sino que se pueden realizar mejoras sobre las ya implementadas.
- **Administración:** Es un término poco aplicado; sin embargo, las redes deben ser administradas a través de programas o de aplicaciones que permitan relevar los problemas surgidos a diario, analizarlos y darles una solución.
- **Costo-beneficio:** Es un tema no menor, dado que siempre que se impulsa una nueva red o una modificación de la actual, debe primar este aspecto.
- **Alta disponibilidad:** La red debe estar siempre operativa. Un factor importante para que esto suceda es contar con ambientes redundantes, tanto en las conexiones como en los dispositivos.
- **Servicios:** La red debe tener la capacidad de soportar diferentes tipos de tráfico, como datos, voz y video, por lo que se requiere QoS (calidad de servicio). También exige ambientes con desarrollo de multicast (multidifusión de datos entre usuario) y, en especial, que sea segura, con buenas prácticas de resguardo.
- **Multiprotocolo:** La red debe tener capacidad a través de los dispositivos de networking y permitir el trabajo en ambientes cerrados, con protocolos propietarios, como también en ambientes con estándares, bajo normas comunes, para diferentes fabricantes.

- **Movilidad:** Las redes actuales, por el continuo movimiento de las personas que conforman una empresa, deben tener la capacidad de implementar tecnología wireless.

Para cubrir las necesidades de todos los usuarios, hay que prestar atención a la convergencia de múltiples servicios, a la mayor movilidad de los usuarios, al aumento en las velocidades de conexión y a un mayor número de parámetros de seguridad ante nuevos peligros emergentes. [3]

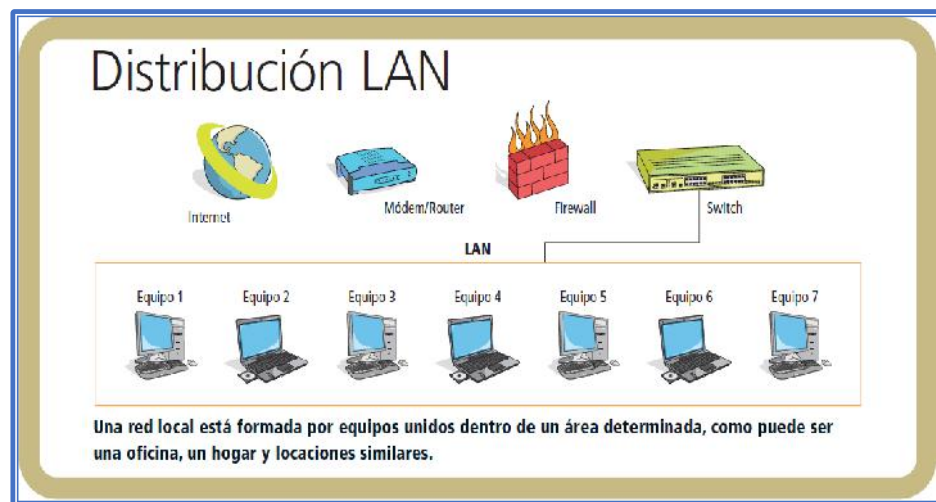


Figura 2. Distribución de una Red LAN.  
Fuente: [Revista USERS]

#### 2.2.1.4 TOPOLOGIA DE RED

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cuál topología es la más apropiada para una situación dada. La topología en una red es la configuración adoptada por las estaciones de trabajo para conectarse entre sí.

Las redes también se pueden clasificar de acuerdo a su topología física. La topología física define la representación geométrica de todos los enlaces de una red y los dispositivos físicos que se enlazan entre sí. Las topologías más conocidas son: bus, anillo, estrella y malla.

- **Una topología en bus** es una configuración donde un único enlace conecta todos los dispositivos de la red constituyendo una red en forma de tronco.
- **Una topología en anillo** es una topología de red donde cada dispositivo tiene una línea de conexión con todos los dispositivos de la red constituyendo una red en forma de anillo.
- **Una topología en estrella** es aquella en la que cada dispositivo solo tiene un enlace dedicado con un controlador central habitualmente llamado concentrador.
- **Una topología en malla** es una configuración en la que cada dispositivo tiene un enlace punto a punto dedicado con cualquier otro dispositivo. El término dedicado indica que el enlace sólo conduce el flujo de datos entre los dispositivos que interconecta. En la topología en malla, los dispositivos que forman la red pueden ser nodos de reenvío y enrutamiento (router) o equipos finales (PC).

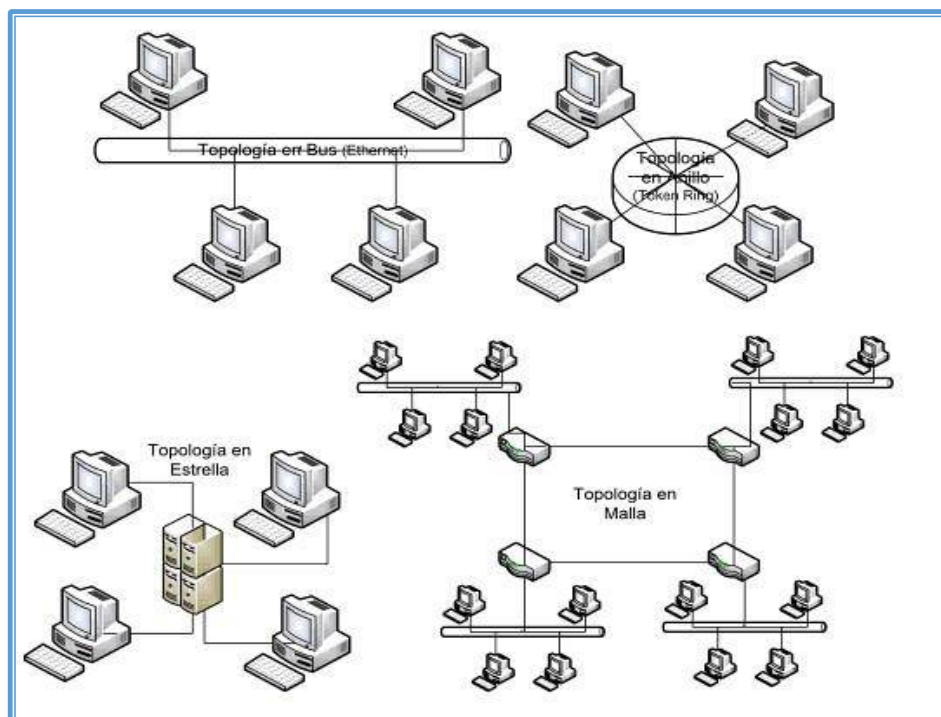


Figura 3. Topología Físicas de Redes de Computadoras.  
Fuente: [Redes y Transmisión de Datos]

La topología en malla ofrece varias ventajas respecto al resto de topologías de red. Así, la topología en malla proporciona una mayor tolerancia a fallos y fiabilidad. El uso de enlaces dedicados garantiza que cada conexión transporte únicamente los mensajes entre los dispositivos que interconecta, eliminando el problema de que en caso de fallo se pierdan todos los datos que transporta la red, ya que sólo se perderán los que transporta ese enlace. Además, se puede evitar los enlaces que han tenido fallos o problemas de tráfico y, por otro lado, es fácil para el administrador de la red localizar y detectar las causas de la pérdida y dar soluciones a éstas. También cabe destacar que estas redes, por su topología, tienen la ventaja de la privacidad y seguridad ya que únicamente pueden acceder a un mensaje, que es transportado por un enlace determinado, los dispositivos conectados a él. Pero no obstante, la topología en malla también sufre de ciertas desventajas relacionadas principalmente con la cantidad de cable y el número de dispositivos de interconexión (puertos de entrada y salida



necesarios). Esto obliga a costes monetarios elevados, a limitaciones de espacio disponible y a dificultades en la instalación y reconfiguración de la red.

Para evitar estos problemas, se hace más adecuado en algunas ocasiones la instalación de redes estrellas cuyo coste es más barato que la red en malla. En una topología en estrella, cada dispositivo necesita sólo de un enlace de un puerto de entrada y salida para conectarse a un nodo concentrador, por lo tanto esto hace que se facilite la instalación y reconfiguración de la red, además de reducir el número de cables y conexiones. La red en estrella también se caracteriza por la robustez y tolerancia a fallos, ya que si falla un enlace solamente afecta a los dispositivos conectados a ese enlace, permaneciendo todos los demás enlaces activos. El principal problema radica en caso de que falle el concentrador, en cuyo caso todos los enlaces de la red fallarán. Además, el número de dispositivos conectados al concentrador determina la capacidad de proceso de éste.

Al igual que en la topología en malla, la topología en estrella requiere gran cantidad de cableado. Otras topologías como el bus o el anillo reducen la cantidad de éste. Por ejemplo, la topología en bus tiene la principal ventaja de la sencillez de instalación. Sin embargo, se caracteriza también por su dificultad para su reconfiguración (añadir o quitar equipos) o localizar y detectar fallos. Además, en topologías en bus, la rotura del cable del bus provoca la imposibilidad de transmisión entre cualquier dispositivo de la red.

Finalmente, cabe comentar de la topología en anillo que es fácil de instalar y de reconfigurar si se compara con una topología en bus mediante cable coaxial. No obstante, sigue siendo más difícil de instalar y reconfigurar si se compara con una topología en bus implementada con dispositivos HUB. También destaca porque los fallos son localizables fácilmente, aunque no tanto como en un bus con HUBs. Siendo su principal desventaja, el tráfico que es del tipo unidireccional siempre en un sentido del anillo. [4]

### 2.2.1.5 MODELO OSI

El modelo OSI divide el funcionamiento de una red en siete capas bien definidas. En cada una de ellas se preparan los datos para viajar y ser entregados a su destino de manera satisfactoria.



Figura 4. Capas que componen el Modelo OSI.  
Fuente: [Revista USERS]

Debemos tener en cuenta que, en la actualidad, existen protocolos de comunicación mucho más flexibles y que, por lo tanto, nos entregan capas de comunicación que no están demarcadas en forma precisa.

A pesar de esto, el modelo OSI se sigue empleando para explicar de modo sencillo el funcionamiento real de las comunicaciones en red. Por este motivo, puede ser correcto hablar de modelo de referencia OSI. [5]



### **2.2.1.6 MODELO TCP/IP**

El modelo de capas TCP/IP es paralelo al OSI; se trata de dos modelos muy similares en los cuales podemos darnos cuenta de que las capas que los componen se entremezclan.

#### **Capas del modelo TCP/IP**

Las capas jerarquizadas del modelo TCP/IP solo son cuatro, a diferencia de las siete que componen el modelo OSI. Pero debemos tener en cuenta que cada una de estas capas se corresponde con las capas del modelo OSI; de esta forma, podemos identificar sus correspondencias de una manera sencilla.

#### **Capa 1: Capa de enlace**

Combina la capa física y la capa de enlace de datos correspondiente al modelo OSI. Enruta los datos entre dispositivos y maneja el intercambio de datos.

#### **Capa 2: Capa de red**

Se asimila a la capa 3 del modelo OSI, y se encarga de determinar la dirección del dispositivo al cual debe dirigirse la información.

#### **Capa 3: Capa de transporte**

Se corresponde en forma directa con la capa de transporte del modelo OSI. Aquí encontramos el protocolo TCP, encargado de averiguar si un dispositivo de la red está esperando la información que se transmite.

#### **Capa 4: Capa de aplicación**

Esta capa combina las capas de sesión, presentación y aplicación del modelo OSI. En este nivel encontramos protocolos específicos relacionados con el correo electrónico o la transferencia de archivos, entre otros. [5]



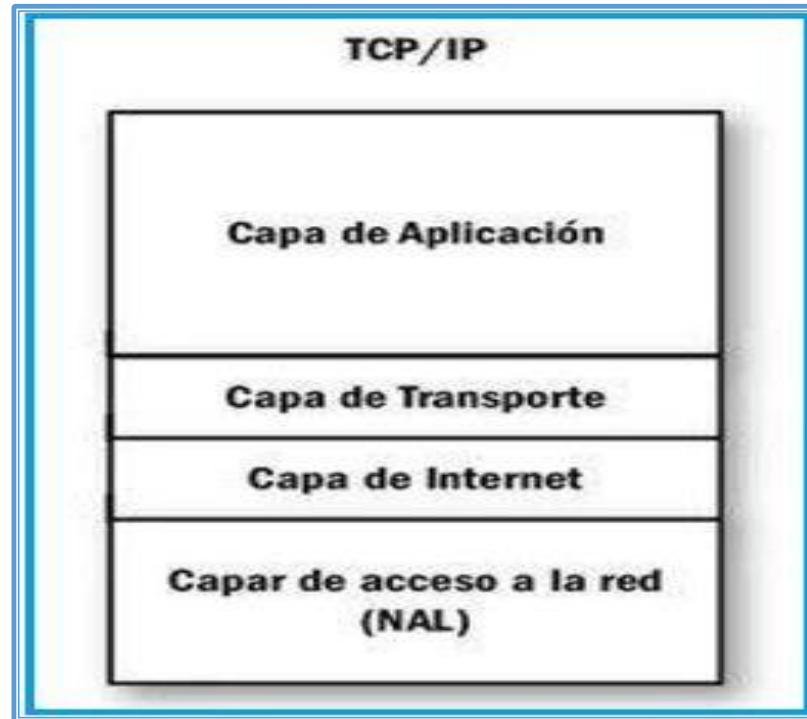


Figura 5. Capas que componen el Modelo TCP/IP.  
Fuente: [Revista USERS]

### 2.2.1.7 MEDIO DE RED:

#### ➤ CABLE UTP

Unshielded Twisted Pair (UTP), es un tipo de cableado utilizado principalmente para comunicaciones.

Es un cable de pares trenzados y sin recubrimiento metálico externo, de modo que es sensible a las interferencias; sin embargo, al estar trenzado compensa las inducciones electromagnéticas producidas por las líneas del mismo cable. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz, disminuyendo sensiblemente, o incluso impidiendo, la capacidad de transmisión. Es un



cable barato, flexible y sencillo de instalar. La impedancia de un cable UTP es de 100 ohmios.

Como el nombre lo indica, "unshielded twisted pair" (UTP), es un cable que no tiene revestimiento o blindaje entre la cubierta exterior y los cables. El UTP se utiliza comúnmente para aplicaciones de REDES Ethernet, el término UTP generalmente se refiere a los cables categoría 3, 4 y 5 especificados por el estándar TIA/EIA 568-A standard. [6]

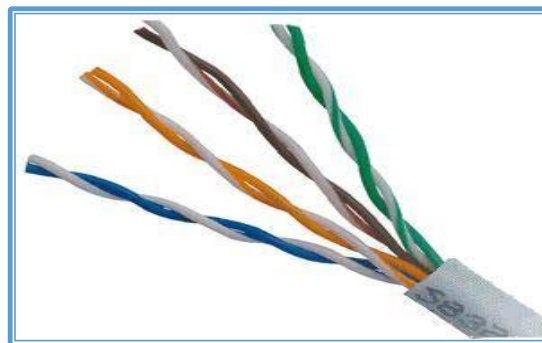


Figura 6. Cable UTP.  
Fuente: [6]

## TIPOS DE CABLE UTP

- **Categoría 1:** El cable CAT 1 o categoría 1, es el más adecuado para las comunicaciones telefónicas. No es adecuado para transmitir datos o para trabajarlos en una red. Se utiliza sobre todo en instalaciones de cableado.
- **Categoría 2:** El cable categoría 2, o CAT 2, es capaz de transmitir datos de hasta 4 Mbps. Se trata de cable nivel 2 y se usó en las redes ARCnet (arco de red) y Token Ring (configuración de anillo) hace algún tiempo. El CAT 2 al igual que el CAT 1, no es adecuado para la transmisión de datos en una red.



- **Categoría 3:** El cable categoría 3, o CAT 3, es un par trenzado, sin blindar, capaz de llevar a la creación de redes 100BASE-T y puede ayudar a la transmisión de datos de hasta 16MHz con una velocidad de hasta 10 Mbps. No se recomienda su uso con las instalaciones nuevas de redes.
- **Categoría 4:** El cable categoría 4, o CAT 4, es un par trenzado sin blindar que soporta transmisiones de hasta 20MHz. Es confiable para la transmisión de datos por encima del CAT 3 y puede transmitir datos a una velocidad de 16 Mbps. Se utiliza sobre todo en las redes Token Ring.
- **Categoría 5:** El cable categoría 5, o CAT 5, ayuda a la transmisión de hasta 100 MHz con velocidades de hasta 1000 Mbps. Es un cable UTP muy común y adecuado para el rendimiento 100BASE T. Se puede utilizar para redes ATM, 1000BASE T, 10BASE T, 100BASE T y token ring. Estos cables se utilizan para la conexión de computadoras conectadas a redes de área local.
- **Categoría 5e:** El cable categoría 5e o CAT 5e, es una versión mejorada sobre el de nivel 5. Sus características son similares al CAT 5 y es compatible con transmisión de hasta 10MHz. Es más adecuado para operaciones con Gigabit Ethernet y es una excelente opción para red 1000BASE T.
- **Categoría 6:** El cable Categoría 6, o CAT 6, es una propuesta de par trenzado sin blindar que puede soportar hasta 250 MHz de transmisión. Se trata de la sexta generación del cable Ethernet. Este cable con alambres de cobre puede soportar velocidades de 1 GB. CAT 6 es compatible con el CAT 5e, CAT 6 y CAT 3. Es adecuado para redes 1000BASE T, 100BASE T y 10BASE T y posee estrictas reglas acerca del ruido del sistema y la diafonía.

- **Categoría 7:** El cable categoría 7, CAT 7, es otro proyecto de norma que admite la transmisión de hasta 600MHz. CAT 7 es un estándar Ethernet de cable de cobre 10G que mide más de 100 metros. Es compatible con CAT 5 y CAT 6 y tiene reglas más estrictas que CAT 6 sobre el ruido del sistema y la diafonía. [7]

## PONCHADO DE CABLES

El cableado estructurado para redes de computadores nombran dos tipos de normas o configuraciones a seguir, estas son: La EIA/TIA-568A (T568A) y la EIA/TIA-568B (T568B). La diferencia entre ellas es el orden de los colores de los pares a seguir para el conector RJ45.

### NORMAS DE PONCHADO

• Blanco - Verde	• Blanco – Azul
• Verde	• Naranja
• Blanco - Naranja	• Blanco - Café
• Azul	• Café

Tabla 1.Norma T568A: Orden de colores  
Fuente: [6]

• Blanco - Naranja	• Blanco - Azul
• Naranja	• Verde
• Blanco - Verde	• Blanco - Café
• Azul	• Café

Tabla 2.Norma T568B: Orden de colores  
Fuente: [6]

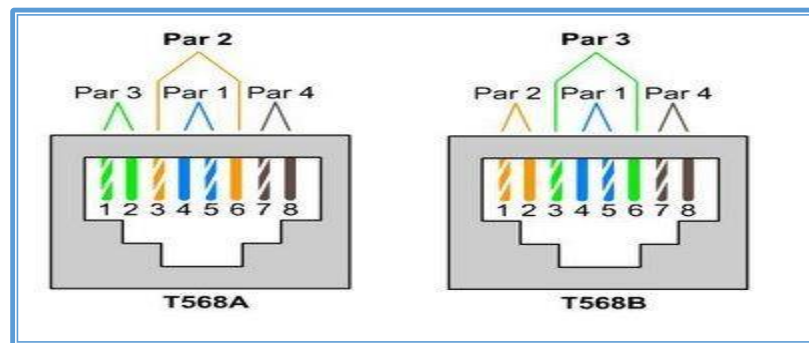


Figura 7. Normas de Ponchado.  
Fuente: [6]

### RJ45:

Es una interfaz física comúnmente usada para conectar redes de cableado estructurado, (categorías 4, 5, 5e y 6). RJ es un acrónimo inglés de Registered Jack que a su vez es parte del Código Federal de Regulaciones de Estados Unidos.



Figura 8. Conector RJ45.  
Fuente: [6]

Posee ocho "pines" o conexiones eléctricas, que normalmente se usan como extremos de cables de par trenzado. Es utilizada comúnmente con estándares como TIA/EIA-568-B, que define la disposición de los pines o wiring pinout. Una aplicación común es su uso en cables de red Ethernet, donde suelen usarse 8 pines (4 pares).

Al utilizar estas normas podemos utilizar el cable UTP de manera Directa o Cruzada. [6]

## El Cable de Red Directo

El cable directo sirve para conectar dispositivos diferentes, como una computadora con switch o router, por ejemplo nuestra PC al modem/router de internet.

En este caso ambos extremos del cable deben de tener la misma distribución. No existe diferencia alguna en la conectividad entre la distribución 568B y la distribución 568A siempre y cuando en ambos extremos se use la misma.

## El Cable de Red Cruzado

Es aquel donde en los extremos la configuración es diferente. El cable cruzado, como su nombre lo dice, cruza las terminales de transmisión de un lado para que llegue a recepción del otro, y la recepción del origen a transmisión del final. Para crear el cable de red cruzado, lo único que se debe hacer es ponchar un extremo del cable con la norma T568A y el otro extremo con la norma T568B. Es utilizado para conectar dos PCs directamente o equipos activos entre si, como hub con hub, con switch, router, etc. [6]

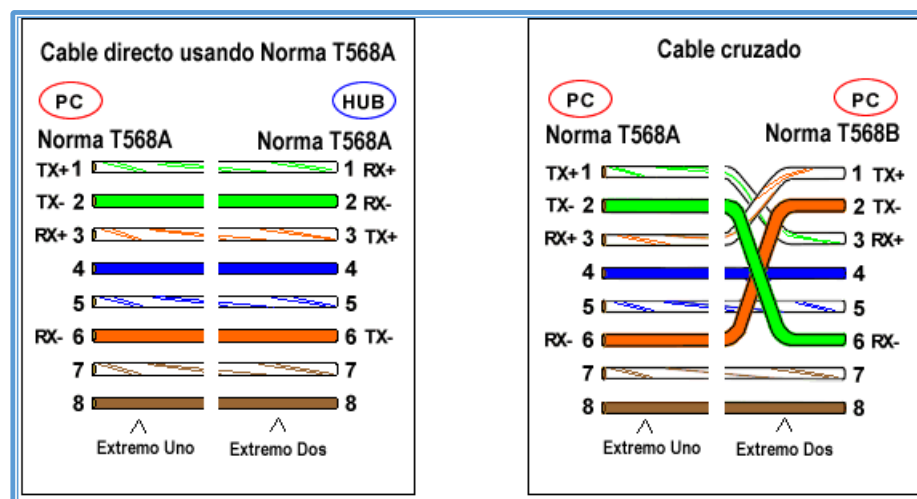


Figura 9.Cable directo y cruzado.  
Fuente: [6]

### ➤ CABLE COAXIAL

Este tipo de cable está compuesto de un hilo conductor central de cobre rodeado por una malla de hilos de cobre. El espacio entre el hilo y la malla lo ocupa un conducto de plástico que separa los dos conductores y mantiene las propiedades eléctricas. Todo el cable está cubierto por un aislamiento de protección para reducir las emisiones eléctricas.

Originalmente fue el cable más utilizado en las redes locales debido a su alta capacidad y resistencia a las interferencias, pero en la actualidad su uso está en declive. Su mayor defecto es su grosor, el cual limita su utilización en pequeños conductos eléctricos y en ángulos muy agudos.

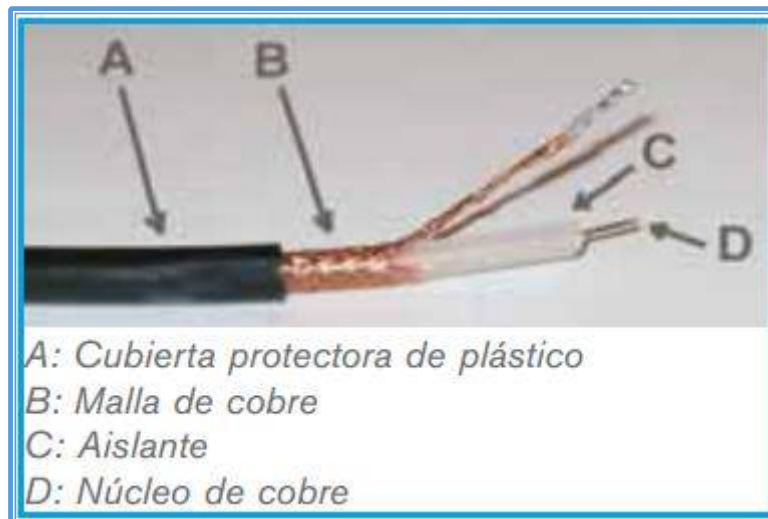


Figura 10.Cable Coaxial

Fuente: [8]

### TIPOS DE CABLE COAXIAL

**THINCK:** (grueso). Este cable se conoce normalmente como “cable amarillo”, fue el cable coaxial utilizado en la mayoría de redes. Su capacidad en términos de velocidad y distancia es grande, pero el coste del cableado es alto y su grosor no permite su utilización en canalizaciones con demasiados cables. Este cable es empleado en las redes de área local conformando con la norma 10 Base 2.



**THIN:** (fino). Este cable se empezó a utilizar para reducir el coste de cableado de la redes. Su limitación está en la distancia máxima que puede alcanzar un tramo de red sin regeneración de la señal. Sin embargo el cable es mucho más barato y fino que el thick y, por lo tanto, solventa algunas de las desventajas del cable grueso. Este cable es empleado en las redes de área local conformando con la norma 10 Base 5. El cable coaxial en general solo se puede utilizar en conexiones Punto a Punto o dentro de los racks. **[9]**

### **ELECCIÓN DEL COAXIAL**

Los cables coaxiales se eligen en base a los siguientes parámetros, que son impuestos por el circuito al que deberán ser conectados:

- Impedancia característica (50, 75 o 93 Ohm)
- Frecuencia de trabajo (de 100 kHz a 3000 MHz)
- Atenuación máxima (de 1 a varios cientos de dB/100 m.) y/o potencia máxima (de unos pocos W hasta algún kW, referido a una frecuencia de trabajo).
- Capacidad (de 30 a 100 pF/m)
- Máxima tensión de señal
- Aunque de menor importancia, en ciertas aplicaciones se requiere considerar también la velocidad de propagación y la impedancia de transferencia. Una vez definida la impedancia se puede elegir el cable operando sobre el correspondiente gráfico de los cables normalizados; con el valor de la frecuencia de trabajo se individualiza el punto de intersección correspondiente a la atenuación o potencia. Es suficiente adoptar el valor del diámetro D inmediatamente superior para definir en forma unívoca el tipo de cable adecuado.

En caso de no encontrarse un cable normalizado se deberá recurrir a un diseño especial.



## LOS MÁS UTILIZADOS

En general, los coaxiales más utilizados para el cableado en la industria de la seguridad electrónica y comunicaciones son los siguientes:

- **RG 59 U PP** (pesado), con cobertura de malla al 90%, 75 Ohms.
- **RG 59 U SP** (semi pesado), con cobertura de malla a 67%
- **RG 59 DM** (doble malla), con cobertura de malla 67% +90%, 75 Ohms
- **RG 59 U + Bipolar** de 2 x 0.50 mm. En cobertura de malla de 90% con el bipolar integrado al coaxil para conducir energía en 12 o 24 voltios, 75 Ohms
- **RG 58 FOAM**, con conductor de cobre macizo y dieléctrico de polietileno expandido por el método de inyección gaseosa, 50 Ohms
- **RG 213 FOAM**, con conductor central de cobre macizo y dieléctrico de polietileno expandido por inyección gaseosa.

Los coaxiales para televisión por cable más usual y cctv, en tanto, son los siguientes:

- **RG 59** 40%; 67%; 67% Trishield; 90%; 90% Trishield, con o sin mensajero.
- **RG 6:** 67%; 67% Trishield; 90%; 90% Trishield, con o sin mensajero.
- **RG 11:** 67%, 67% Trishield; 90%; 90% Trishield, con o sin mensajero. [8]

## CONECTORES:

Son aquellos elementos que nos hacen posible la unión entre determinado tipo de cable que transporta una señal y un equipo o accesorio que la envía o recibe. Nos facilitan la tarea de conectar y desconectar, permitiéndonos cambiar equipo o cableado rápidamente.



**CONECTORES PARA CABLE COAXIAL:** Tenemos el tipo "N", "BNC", "DNC", "SMA" y "TNC".



Figura 11. Conectores para cable Coaxial.  
Fuente: [10]

Para todos los casos anteriores, existen los conectores MACHOS:



Figura 12. Conectores Machos.  
Fuente: [10]

Y los conectores HEMBRAS:



Figura 13. Conectores Hembra.  
Fuente: [10]

### 2.2.1.8 VIDEOVIGILANCIA IP

Para garantizar la seguridad local o remota por medio de video captado por cámaras, el sistema de Video vigilancia por IP resulta una tecnología apropiada para dicho fin, reemplazado a las cámaras de vigilancia analógicas y teniendo una gran aceptación por parte de las empresas. Se utiliza para la protección de intrusión, control de accesos, supervisión de comercios, trabajadores y procesos, además de controlar personal y familiares en áreas domésticas.

#### 2.2.1.8.1 VENTAJAS DE LA VIDEOVIGILANCIA IP

- **Accesibilidad remota**

Se pueden configurar las cámaras de red y los codificadores y acceder a ellos de forma remota, lo que permite a diferentes usuarios autorizados visualizar vídeo en vivo y grabado en cualquier momento y desde prácticamente cualquier ubicación en red del mundo. Esto resulta ventajoso si los usuarios quisieran que otra empresa, como por ejemplo una empresa de seguridad, tuviera también acceso al vídeo. En un sistema CCTV analógico tradicional, los usuarios necesitarían encontrarse en una ubicación de supervisión in situ para ver y gestionar vídeo, y el acceso al vídeo desde fuera del centro no sería posible sin un equipo como un codificador de vídeo o un grabador de vídeo digital (DVR) de red. Un DVR es el sustituto digital de la grabadora de cintas de vídeo.

- **Alta calidad de imagen**

En un sistema de vigilancia IP digital completo, las imágenes de una cámara de red se digitalizan una vez y se mantienen en formato digital sin conversiones innecesarias y sin degradación de las imágenes debido a la distancia que recorren por una red. Además, las imágenes digitales

se pueden almacenar y recuperar más fácilmente que en los casos en los que se utilizan cintas de vídeo analógicas.

- **Gestión de eventos y video inteligente**

A menudo existe demasiado material de vídeo grabado y una falta de tiempo suficiente para analizarlo adecuadamente. Las cámaras de red y los codificadores de vídeo avanzados con inteligencia o análisis integrado pueden ocuparse de este problema al reducir la cantidad de grabaciones sin interés y permitir respuestas programadas. Este tipo de funcionalidad no está disponible en un sistema analógico.

- **Integración sencilla y preparada para el futuro**

Los productos de vídeo en red basados en estándares abiertos se pueden integrar fácilmente con sistemas de información basados en ordenadores y Ethernet, sistemas de audio o de seguridad y otros dispositivos digitales, además del software de gestión de vídeo y de la aplicación. Por ejemplo, el vídeo de una cámara de red se puede integrar en un sistema de punto de venta o en un sistema de gestión de edificios.

- **Escalabilidad y flexibilidad**

Un sistema de vídeo en red puede crecer a la vez que las necesidades del usuario. Los sistemas basados en IP ofrecen a muchas cámaras de red y codificadores de vídeo, así como a otros tipos de aplicaciones, una manera de compartir la misma red inalámbrica o con cable para la comunicación de datos; de este modo, se puede añadir al sistema cualquier cantidad de productos de vídeo en red sin que ello suponga cambios significativos o costosos para la infraestructura de red. Esto no sucede con un sistema analógico. En un sistema de vídeo analógico, se debe extender un cable coaxial directamente desde cada cámara a un puesto de visualización o grabación. Asimismo, se deben



usar cables de audio independientes si se requiere audio. Los productos de vídeo en red también se pueden implementar y utilizar en red desde prácticamente cualquier lugar, y el sistema puede ser tan abierto o cerrado como se necesite.

- **Rentabilidad de la inversión**

Un sistema de vigilancia IP tiene normalmente un coste total de propiedad inferior al de un sistema CCTV analógico tradicional. Una infraestructura de red IP a menudo ya está implementada y se utiliza para otras aplicaciones dentro de una organización, por lo que una aplicación de vídeo en red puede aprovechar la infraestructura existente. Las redes basadas en IP y las opciones inalámbricas constituyen además alternativas mucho menos caras que el cableado coaxial y de fibra tradicionales utilizados por un sistema CCTV analógico. Por otro lado, las transmisiones de vídeo digitales se pueden encaminar por todo el mundo mediante una gran variedad de infraestructuras interoperativas. Los costes de gestión y equipos también son menores ya que las aplicaciones back-end y el almacenamiento se ejecutan en servidores basados en sistemas abiertos, de estándar industrial, no en hardware propietario como un DVR en el caso de un sistema CCTV analógico.

Además, la tecnología PoE (Alimentación a través de Ethernet), que no se puede aplicar a un sistema de vídeo analógico, se puede utilizar en un sistema de vídeo en red. PoE permite a los dispositivos en red recibir alimentación de un conmutador o midspan compatible con PoE a través del mismo cable Ethernet que transporta los datos (vídeo). Ofrece un ahorro sustancial en los costes de instalación y puede aumentar la fiabilidad del sistema. Para más información, visite Power over Ethernet.

[11]



Figura 14. Un sistema que utiliza la Alimentación a través de Ethernet.  
Fuente: [11]

## 2.2.1.8.2 COMPONENTES DE UN SISTEMA DE VIDEOVIGILANCIA IP

### 2.2.1.8.2.1 CAMARA IP

Las cámaras IP captan imágenes, y tienen las mismas funcionalidades que las analógicas, únicamente disponen además de un pequeño servidor web que permite su conexión directa a Internet o a una red de datos para la visualización de la misma.

La cámara IP, también conocida como cámara de red o cámara de Internet, es un dispositivo que tiene una CPU y se conecta directamente a un punto de red (Ethernet o inalámbrico). La cámara IP no necesita ningún hardware adicional ya que es capaz de procesar imágenes y sonido internamente y servirlos a través de Internet. [12]



### ➤ **Funcionamiento**

El funcionamiento de las cámaras IP se puede considerar como una mezcla entre las cámaras de CCTV y las webcam. Están diseñadas para poder conectarse a través de cables de larga distancia sin perder calidad de imagen, y, en algunos casos, incluyen audio. Podemos conectar varias cámaras IP a una misma PC, y, utilizando software para monitoreo, es posible visualizar varias cámaras al mismo tiempo.

El funcionamiento interno es sencillo y se puede comparar, en cierto modo al de las cámaras de fotos, ya que procesa imágenes; en la cámara de fotos, estas imágenes son almacenadas en su memoria, mientras que en las cámaras de seguridad son enviadas al receptor, que es un monitor externo y alejado de donde se encuentran las cámaras IP. En su interior, poseen una lente, que puede ser un lente genérico fijo de poco megapíxeles o incluso VGA (0,3 MP), y, según su calidad, podremos visualizar la imagen con mayor o menor nitidez. Las cámaras IP de seguridad profesional poseen lentes intercambiables de gran precisión que se pueden ajustar según la distancia a la que se encuentren, incluso con visión nocturna. Esta lente está montada a través de conectores o soldada a una placa lógica, que posee conexión Ethernet, y el Jack para la alimentación eléctrica. La mayoría de las cámaras incluyen un pequeño micrófono, y algunas pueden tener salidas de audio. En esta salida de audio, irán conectados unos parlantes que reproducirán lo que nosotros digamos desde el micrófono de nuestra PC, y, a través del micrófono que está en la misma cámara, podemos interactuar con las personas que estemos observando. Además de la conexión Ethernet, incluyen conexión wireless; aunque visualmente no podamos distinguir su antena, es muy probable que cuenten con ella. Todos estos datos son procesados en forma digital por la placa lógica de la cámara y enviados a través de la conexión Ethernet o Wi-Fi.

### ➤ **Hardware**

A nivel hardware, la lente permite el paso de la luz hacia el sensor. Los sensores CMOS y CCD (Charged-coupled Device, que en español significa dispositivos de carga acoplada) son circuitos eléctricos compuestos por varios capacitores acoplados, llamados células fotoeléctricas. La resolución máxima a la que se puede obtener una imagen coincide con la cantidad de células que posee el sensor, o sea que la resolución máxima de una fotografía o video no solo está determinada por la lente, sino directamente por el sensor. En la actualidad, encontramos modelos con un tipo de sensor u otro; si bien el funcionamiento es similar, el sensor CMOS permite tomar fotografías por ráfagas, lo que hace ideal para la grabación de video de alta definición. Este sensor recibe la luz proveniente de la lente y, por efecto fotoeléctrico, genera una corriente por cada célula, que será procesada para generar la imagen.

### ➤ **Software**

Algunos fabricantes incluyen con sus cámaras software específico para poder visualizarlas. La ventaja que tiene la utilización del software reside no solo en que contaremos con opciones de grabación, sino que, si decidimos agregar más cámaras del mismo fabricante, podremos visualizar, en forma simultánea, todas las cámaras que tengamos instaladas, construyendo un CCTV. Esto proporciona la escalabilidad del sistema. Las cámaras IP no requieren drivers para la visualización desde la PC, tablet o smartphone y, comparadas con el viejo sistema de CCTV, poseen la ventaja, hasta cierto punto, de ser una solución más económica, de fácil manejo y reemplazo; comparadas con el nuevo sistema CCTV, es una alternativa económica. Su elección dependerá de nuestras necesidades. [13]



### ➤ Tipos de cámaras IP

Los fabricantes de cámaras IP nos proveen de varios modelos que pueden ajustarse a nuestras necesidades; por esa razón, es posible encontrar cámaras de muy alto valor, y otras convencionales; su elección dependerá de dónde las ubicaremos. Por ejemplo, una institución bancaria requerirá un complejo sistema de seguridad con cámaras ultrasensibles; en cambio, en nuestro hogar no necesitaremos una cámara con grandes prestaciones.

#### **Cámara IP estándar**

Este tipo de cámara tiene conexión Ethernet, y opcionalmente con wireless. Debido a la poca diferencia económica, ya es común que incluyan ambas conexiones de red. Poseen un lente fijo de baja resolución, lo que no la hace apta para visualizar lugares abiertos o con mucha intensidad de luz solar; en cambio podemos utilizarla en espacios reducidos, como pequeñas oficinas. Posee dos ajustes a presión para establecer la mejor posición de acuerdo a su ubicación física.

#### **Cámara IP con visibilidad nocturna**

Este tipo de cámaras traen un conjunto de led fotosensible alrededor de la lente, que se activa en forma gradual según la menor intensidad de luz que haya en el ambiente. Pueden utilizarse en ambientes exteriores si se toman ciertas precauciones para evitar daños por lluvias, etc. La desventaja que poseen las cámaras genéricas con visión nocturna reside en que, en ambientes totalmente oscuros, los leds de la lente que se iluminan la hacen fácilmente detectable a varios metros de distancia. Se pueden configurar para que, al captar movimiento en una zona que hayamos configurado como sensible, tomen fotografías y las reenvíen por correo electrónico.



## Cámara IP PTZ

Su nombre proviene de Pan Tilt Zoom. También se las suele conocer con el nombre de Cámara Domo. Además de contener las ventajas de las dos cámaras anteriores, estas incluyen un mecanismo que puede rotar su posición y, así, conseguir un mayor grado visual. Poseen un mecanismo que permite rotar horizontalmente (panning), otro verticalmente (tilt), y hacer zoom a una determinada área. Algunas cámaras incluyen la función de autoseguimiento, que es similar a la detección por movimiento, solo que, en este caso, la cámara rotará en forma automática siguiendo la fuente en movimiento. Todos sus controles para el movimiento pueden realizarse desde el mismo navegador en el que visualizamos nuestra cámara IP PTZ.

Este tipo de cámara no posee ajustes a presión para colocarla, y, como viene todo en conjunto debido a su mecanismo de rotación, si decidiéramos colocarla en una pared o un techo, tendríamos que configurar su visualización para que nos permitiera rotar la imagen que vemos. En la parte posterior, posee cuatro conectores que podremos utilizar para conectar un relé que activará luces, y un sensor de movimiento adicional, para complementar las funcionalidades de la cámara. [13]



Figura 15. Tipos de cámaras IP.  
Fuente: [Elaboración propia]

### 2.2.1.8.2.2 NETWORK VIDEO RECORDER (NVR)

El NVR utiliza cámaras IP para todo su conjunto; estas se conectarán por cable Ethernet o wireless al NVR, que, además de incluir las funciones del DVR, tiene conexión a Ethernet directa para el router, con lo cual podremos visualizar todas las cámaras desde cualquier puesto de la red o desde Internet. [13]



Figura 16. Sistema NVR.  
Fuente: [13]

### 2.2.1.8.2.3 SWITCH

El switch reemplazó la combinación de hubs y puentes. Puede tener varios puertos, lo que permite ampliar la red fácilmente, y su funcionamiento es similar al de un puente. Podría definirse al switch como un puente multipuerto. Para su funcionamiento, se basa en las direcciones MAC, generando una tabla con aquellas que están conectadas a cada puerto.

Es posible conectar dos o más switches entre sí, y cada uno aprenderá del otro sus respectivas tablas de MAC (tablas de conmutación). Al igual que sucede con el puente, para su funcionamiento el switch compara, de las tramas recibidas, la dirección MAC de destino con su tabla de conmutación, y reenvía las tramas al puerto correspondiente. Existen switches de capa 3 (red) que operan con direcciones IP y tienen algunas de las funciones de un router, como la posibilidad

de crear redes virtuales (VLAN) y establecer el límite de ancho de banda a puertos específicos. [15]



Figura 17. Switch de 24 puertos CISCO.  
Fuente: [14]

#### 2.2.1.8.2.4 ROUTER

Este dispositivo nos permite conectarnos a una WAN (Wide Area Network), es decir, a internet.

Trabaja en la capa 3 del modelo OSI (red) y envía paquetes de datos basándose en direcciones IP. El router puede tomar decisiones sobre cuál es la mejor ruta para el envío de paquetes, y admite que se conecten a él diferentes tecnologías, como Ethernet y fibra óptica, ya que toda su conmutación se realiza por medio del protocolo IP.

Al trabajar en la capa 3, tiene su propia IP (que se puede configurar) y, además, es posible configurarlo para que entregue automáticamente direcciones IP a los dispositivos que se van conectando (DHCP) de manera directa o indirecta (por ejemplo, a través de un switch). Su funcionamiento es sencillo: analiza los paquetes entrantes, elige la mejor ruta para reenviarlos y los conmuta por el

puerto correspondiente. El modelo de router y la complejidad de configuración dependerán de lo que necesitemos. Podemos encontrar routers que admiten un solo proveedor ISP, y otros que pueden admitir simultáneamente dos o más proveedores, conexiones VPN, etc. [15]



Figura 18.Router CISCO 2801.  
Fuente: [14]

#### 2.2.1.8.2.5 PATCH PANEL

Los llamados Patch Panel son utilizados en algún punto de una red informática donde todos los cables de red terminan. Se puede definir como paneles donde se ubican los puertos de una red, normalmente localizados en un bastidor o rack de telecomunicaciones. Todas las líneas de entrada y salida de los equipos (ordenadores, servidores, impresoras... etc.) tendrán su conexión a uno de estos paneles.

En una red LAN, el Patch Panel conecta entre sí a los ordenadores de una red, y a su vez, a líneas salientes que habilitan la LAN para conectarse a Internet o a otra red WAN. Las conexiones se realizan con “*patch cords*” o cables de parcheo, que son los que entrelazan en el panel los diferentes equipos.

Los Patch Panel permiten hacer cambios de forma rápida y sencilla conectando y desconectando los cables de parcheo. Esta manipulación de los

cables se hará habitualmente en la parte frontal, mientras que la parte de atrás del panel tendrá los cables más permanentes y que van directamente a los equipos centrales (Switches, Routers, concentradores... etc.).

Los hay de diferentes modelos y pueden ser usados, no solo con datos y teléfonos, sino con aplicaciones de video y audio. El tipo de cable puede ser también variado, desde cable de pares a coaxial y fibra, dependiendo de los elementos que queramos interconectar. [17]

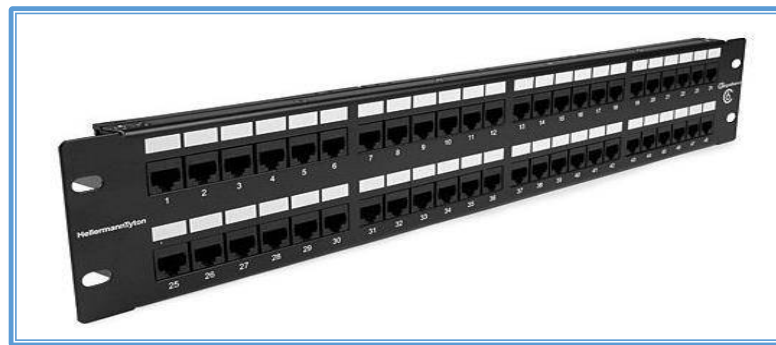


Figura 19. Patch Panel.  
Fuente: [18]

### 2.2.1.9 SISTEMA DE CONTROL DE ACCESO

**Es el control sobre “quien tiene acceso, a dónde y cuándo”**

El sistema de Control de Acceso permite administrar con seguridad las áreas restringidas, sin importar la cantidad de personas que tengan acceso.

El sistema de Control de Acceso da "Acceso" sólo a personas autorizadas y en horarios autorizados.

El Control de Acceso funciona como una llave para controlar la entrada y salida, por medio de dispositivos electrónicos, tales como: lectores biométricos de huellas digitales, lectura del iris, lectura de mano, teclados, y lectores de tarjetas.

Actualmente los Sistemas de Control de Acceso Biométricos emplean la verificación facial, la de retina o la de huella dactilar, que también pueden ser

combinados con tarjetas de proximidad o claves de acceso, con el fin de garantizar el acceso a través de puertas que deben ser protegidas al máximo nivel.

De esta forma se impide que las cerraduras tradicionales sean violadas y que personas no autorizadas ingresen a zonas protegidas, además que se controla la pérdida o duplicados de llaves

Son administrados por un Software de Control que identifica plenamente la persona que entró o salió y a la vez almacena automáticamente cada evento.  
[16]



Figura 20. Sistema de seguridad con Control de Acceso.  
Fuente: [16]

#### 2.2.1.9.1 BENEFICIOS DEL CONTROL DE ACCESO

- Controlar y monitorear el acceso del personal.
- Registros estadísticos actualizados del movimiento del personal.
- Programación de usuarios, turnos y claves.
- Genera reportes de asistencia del personal.
- Bajo costo de operación y ágil recopilación de información.

- Conexión por RED, crece fácilmente en usuarios y en puertas controladas.
- Los lectores biométricos no requieren insumos y son personales.
- Con lectores biométricos se evita el riesgo de pérdida o duplicados de llaves o tarjetas.

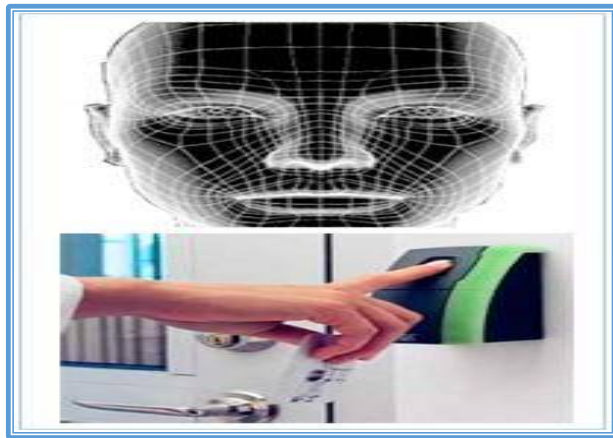


Figura 21.Reconocimiento facial y lector dactilar.  
Fuente: [16]

#### **2.2.1.9.2 PRINCIPALES DISPOSITIVOS PARA CONTROL DE ACCESO Y CONTROL DE ASISTENCIA.**

- Lectores Biométricos: de huella dactilar, de mano, facial e iris.
- Tarjetas de proximidad.
- Tarjetas inteligentes.
- Chapas magnéticas.
- Teclados para digitar claves.
- Tarjetas de código de barras.





Figura 22. Dispositivos para Control de Acceso.  
Fuente: [16]

### 2.2.1.10 SISTEMA DE CABLEADO ESTRUCTURADO

#### 2.2.1.10.1 SISTEMA DE CABLEADO ESTRUCTURADO DE LAS LAN

El cableado estructurado es un enfoque sistemático del cableado. Es un método para crear un sistema de cableado organizado que pueda ser fácilmente comprendido por los instaladores, administradores de red y cualquier otro técnico que trabaje con cables.

Hay tres reglas que ayudan a garantizar la efectividad y eficiencia en los proyectos de diseño del cableado estructurado.

La primera regla es buscar una solución completa de conectividad. Una solución óptima para lograr la conectividad de redes abarca todos los sistemas que han sido diseñados para conectar, tender, administrar e identificar los cables en los sistemas de cableado estructurado. La implementación basada en estándares está diseñada para admitir tecnologías actuales y futuras. El cumplimiento de los estándares servirá para garantizar el rendimiento y confiabilidad del proyecto a largo plazo.

La segunda regla es planificar teniendo en cuenta el crecimiento futuro. La cantidad de cables instalados debe satisfacer necesidades futuras. Se deben





tener en cuenta las soluciones de Categoría 5e, Categoría 6 y de fibra óptica para garantizar que se satisfagan futuras necesidades. La instalación de la capa física debe poder funcionar durante diez años o más.

La regla final es conservar la libertad de elección de proveedores. Aunque un sistema cerrado y propietario puede resultar más económico en un principio, con el tiempo puede resultar ser mucho más costoso. Con un sistema provisto por un único proveedor y que no cumpla con los estándares, es probable que más tarde sea más difícil realizar traslados, ampliaciones o modificaciones.

### **2.2.1.10.2 SUBSISTEMAS DE CABLEADO ESTRUCTURADO**

Hay siete subsistemas relacionados con el sistema de cableado estructurado, como se ve en la Figura 16. Cada subsistema realiza funciones determinadas para proveer servicios de datos y voz en toda la planta de cables:

- Punto de demarcación (demarc) dentro de las instalaciones de entrada (EF) en la sala de equipamiento.
- Sala de equipamiento (ER)
- Sala de telecomunicaciones (TR)
- Cableado backbone, también conocido como cableado vertical
- Cableado de distribución, también conocido como cableado horizontal.
- Área de trabajo (WA)
- Administración

El demarc es donde los cables del proveedor externo de servicios se conectan a los cables del cliente en su edificio. El cableado backbone está compuesto por cables de alimentación que van desde el demarc hasta la salas de equipamiento

y luego a la salas de telecomunicaciones en todo el edificio. El cableado horizontal distribuye los cables desde las salas de telecomunicaciones hasta las áreas de trabajo. Las salas de telecomunicaciones es donde se producen las conexiones que proporcionan una transición entre el cableado backbone y el horizontal.

Estos subsistemas convierten al cableado estructurado en una arquitectura distribuida con capacidades de administración que están limitadas al equipo activo, como por ejemplo los PC, switches, hubs, etc. El diseño de una infraestructura de cableado estructurado que enrute, proteja, identifique y termine los medios de cobre o fibra de manera apropiada, es esencial para el funcionamiento de la red y sus futuras actualizaciones. [19]

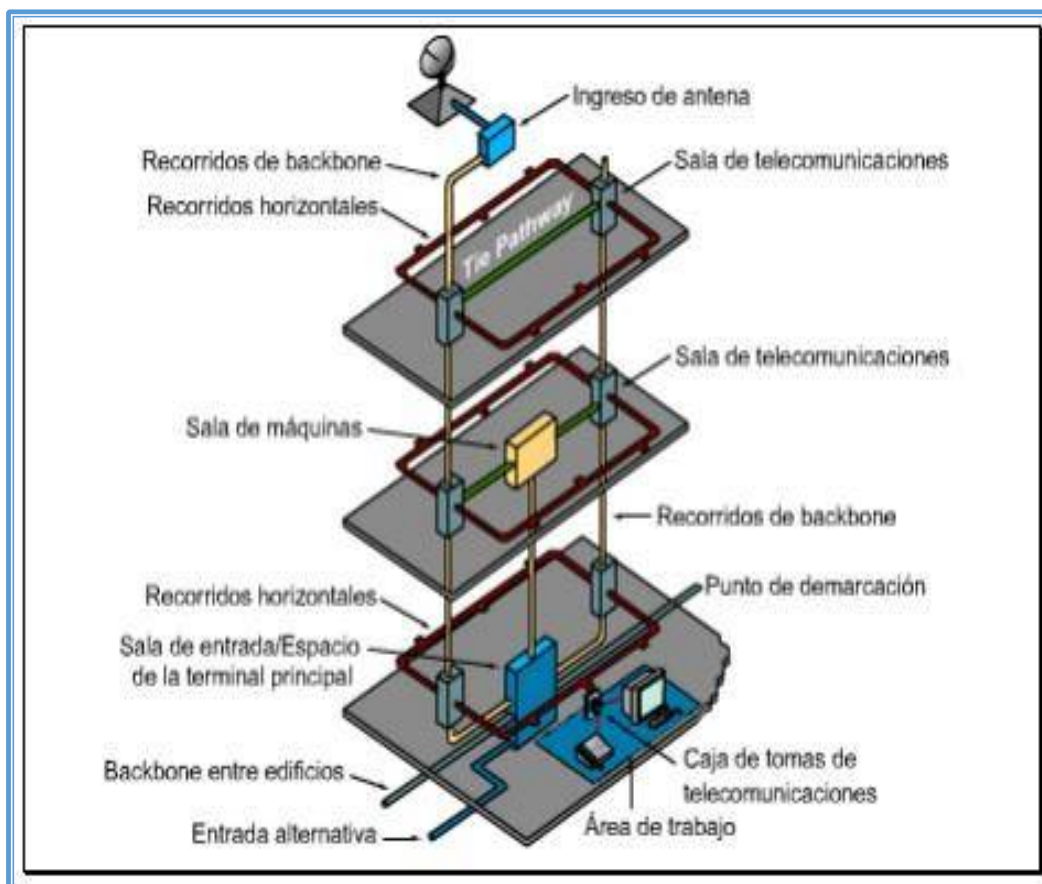


Figura 23.Subsistemas de Cableado Estructurado.  
Fuente: [19]



## 3 CAPITULO 3

### PROPUESTA DE DISEÑO

En este capítulo se detalla la solución propuesta, considerando los parámetros que se utilizaron para el diseño del sistema de videovigilancia IP y control de acceso. También se manifiesta los objetivos que se buscan con el planteamiento de este diseño, en la zona del mercado central de la ciudad de Chiclayo.

#### 3.1 HIPOTESIS DE LA SOLUCIÓN PROPUESTA.

Como bien se sabe, en la actualidad la seguridad es un factor primordial para los diferentes lugares donde nos encontremos. Con la hipótesis planteada lo que se busca es tener un sistema de video vigilancia, que permita monitorear las diferentes zonas del mercado central de Chiclayo, de manera que las personas que laboran en este lugar, así como las diferentes consumidores recurrentes al mercado, tengan la confianza de poder realiza sus actividades con el menor riesgo posible. La solución propuesta para cumplir con este objetivo consiste en utilizar una red IP, con cámaras de video que utilicen la tecnología PoE. Todas las cámaras concentraran su tiempo de grabación en un servidor NVR. Se dispondrá de un Switch POE el cual permitirá concentrar las cámaras en nuestro servidor NVR y del cual por medio de un Router contar con un monitoreo remoto. En este dispositivo se almacenará todas las imágenes captadas por las cámaras que se encuentran interconectadas en el interior del mercado central de Chiclayo.

La visualización de las imágenes captadas por las cámaras, se podrán observar en un Monitor, el cual estará conectado directamente al servidor NVR. La zona de monitoreo será las instalaciones de la administración del mercado central de Chiclayo, allí se encontraran los equipos que harán posible que las videocámaras IP, estén en red y sean desplegadas por las instalaciones del



mercado. Para una mejor distribución se utilizará un rack de piso. Y para asegurar que nuestro sistema siga en funcionamiento ante un eventual corte del suministro de energía eléctrica, se conectará todo nuestro sistema de video vigilancia a un UPS.

Teniendo en cuenta que las instalaciones de la administración, será donde se realice el monitoreo de las videocámaras IP, así también será el lugar donde se encuentren el núcleo de la red IP, resulta necesario integrar un sistema de control de acceso a dicha instalaciones, esto será posible mediante la instalación de una unidad lectora de huella digital en la puerta, garantizando el ingreso, solo a personal autorizado.

### **3.2 OBJETIVOS DE LA SOLUCIÓN PROPUESTA.**

El principal objetivo de este proyecto es diseñar un sistema integrado de video vigilancia IP y Control de Acceso como base para mejorar la seguridad en las instalaciones del Mercado Central de Chiclayo. Para cumplir con este objetivo se diseñara una red IP, con cámaras de video interconectadas en la que se incorpora la tecnología PoE (Power Over Ethernet), a manera de hacer una red eficiente y permitiendo suministrar alimentación eléctrica a través del cable utilizado para la conexión de nuestra red de cámaras IP, de esta manera se abarata la creación de un suministro eléctrico altamente robusto para el sistema. La eficiencia de esta red se medirá cuando se detalle la elección de los equipos utilizados, para el diseño del sistema de video vigilancia. Adicionalmente el control de acceso será implementado, con un equipo que detecte la huella dactilar del personal que ingrese al área de Administración, teniendo un control del horario de ingreso y salida. Este equipo será una unidad de control de acceso, colocada en la puerta de ingreso a Administración.

Otro de los objetivos que se desea cumplir, es diseñar la red lógica fundada sobre una plataforma IP con servidores para la grabación (NVR), de manera que las imágenes obtenidas por las cámaras de video de alta definición (HD), no solo



sean visualizadas en tiempo real sino también se almacenen para una mejor y detallada visualización posterior, de los hechos ocurridos en las instalaciones del mercado central de Chiclayo.

Para lograr diseñar un sistema de video vigilancia y control de acceso de manera eficiente, se requiere estudiar las diferentes tecnologías aplicadas a este tema.

Por otro lado se ha requerido examinar la estructura de las instalaciones del mercado, los puntos de alimentación eléctrica disponibles, ductería y la manera óptima de interconectar los diferentes tipos de cámaras IP a emplear, así como la disposición del control de acceso. Todo ello nos permita darnos una amplia visión de las posibilidades y alternativas de diseño.

Por último se va a plantear una disposición óptima de los equipos de seguridad en las instalaciones del Mercado Central de Chiclayo, de manera que las cámaras cumplan de la manera más eficiente la función de vigilar y brindar seguridad en el interior del mercado central de Chiclayo.

### **3.3 ZONA DE DISEÑO.**

La zona, escenario del diseño a plantear, es el mercado central de Chiclayo. Cuenta con un área total de  $4672.52 \text{ m}^2$ .

Es este mercado muy visitado por gran cantidad de personas, esto tiene que ver con el hecho de encontrarse en una zona céntrica de la ciudad. Dada la magnitud de sus instalaciones, se distribuye en distintas áreas, como son, el área designada a administración, servicios higiénicos, distribución de puestos, área ocupada por comerciantes varios (carnicería, pescado, comidas, verduras, etc).

### **3.4 CONSIDERACIONES PARA EL DISEÑO.**

Resulta necesario tener en cuenta algunas pautas para la realización de un buen diseño. Es así que será posible contar con un eficiente sistema de Videovigilancia IP y la integración adecuada de una unidad de control de acceso.

#### **3.4.1 SISTEMA DE VIDEOVIGILANCIA IP.**

Constituyen el primer escalón del sistema y por tanto, su selección repercute en el nivel de calidad máxima, que pueda lograrse en las imágenes que se registren.

Para seleccionar el tipo de cámara conveniente para el proyecto, es necesario tener en cuenta los siguientes factores:

- El tipo de sensor de imagen.
- El rendimiento de la cámara en casos de iluminación baja.
- La resolución de la imagen.
- Las necesidades de tamaño de archivo y ancho de banda.
- El tratamiento adicional como el balance de blancos y aumento de la definición.

#### **3.4.2 CÁMARA DE RED.**

Existen dos tipos a considerar, como son las cámaras para exteriores e interiores. Basado en el ambiente donde se dispondrán las cámaras, estas deben contar con su respectiva carcasa de protección.

Otro parámetro importante que se debe considerar es la cobertura de las cámaras. Este concepto refiere a cuál es el alcance de visión de cada cámara IP. Así mismo, teniendo en cuenta la cobertura, paralelamente es posible realizar un despliegue adecuado del sistema de videovigilancia, cubriendo todas las zonas y evitando problemas como son la existencia de puntos ciegos, que podría



multiplicarse por todas las cámaras que se encuentren instaladas, exponiendo zonas libres de vigilancia.

La característica más importante que se debe tener en cuenta, es la tasa de FPS (fotogramas por segundo), la que influirá en el ancho de banda que cada cámara ocupe y en la capacidad de almacenamiento. Es importante que en el diseño se delibere cual es la tasa correcta que debe establecerse ya que habrá cámaras y aplicaciones que no necesiten tan buena calidad de imagen.

A continuación se presenta algunas características principales que debe tener cada cámara:

- Lentes: Para la aplicaciones externas
- Sensor de imagen: CCD o CMOS
- Resolución: 640x480, 320x240
- Tasa de cuadro: 30, 25 o 20 cuadros por segundo
- Formatos de video: MJPEG y/o MPEG4
- Audio: G.711 o formato AAC-LC
- Software compatible
- Seguridad: nombre y contraseña de usuario

### **3.4.3 USO DE ANCHO DE BANDA.**

Los requisitos de ancho de banda es un aspecto importante en el diseño de sistemas de videovigilancia. Y depende de factores como:

- El tamaño de la imagen
- La compresión
- La frecuencia de imagen (fotogramas por segundo)





- La complejidad de la imagen

La cantidad de ancho de banda dependerá de cuanta información pasará por la red.

También se tendrá en cuenta el número de cámaras necesarias en el diseño y de cuantos cuadros por segundo se estén empleando, ya que esta medida es proporcional al ancho de banda.

Por otro lado para tener una visualización remota, resulta necesario valerse de un proveedor de internet que cubra la necesidad al subir las imágenes en tiempo real a la web. De esta manera es indispensable que el ancho de banda de subida proporcionado por el proveedor sea el adecuado.

#### **3.4.4 SEGURIDAD.**

Para una red de cámaras IP es necesario contar con medidas de seguridad que hagan posible el despliegue y buen desempeño del sistema, así como también contar con una codificación al momento de la configuración de las cámaras, evitando infiltraciones no deseadas. Es así que se debe tener en cuenta las siguientes consideraciones.

- Teniendo en cuenta el cable que se empleara en la conexión, se debe considerar las especificaciones técnicas, tales como resistencia, atenuación, distancias máximas de trabajo, blindajes, etc. De esta manera evitar deficiencias en la red.
- El canal por donde se desplegara el tendido de cable, este asegurado y con los lubricantes adecuados para conservación y sea posible deslizar el cable en su interior (Tubo de acero Galvanizado).
- Evitar las vueltas y curvas de manera excesiva, mientras más recto se conduzca el cable, menor será la atenuación.
- Configuración de las direcciones IP y puertos de las cámaras.



- Trabajar con cámaras IP que usen sistemas de seguridad (SSL/TLS), lo que nos permite codificar la información captada por las cámaras IP que simultáneamente será enviada a la web, para un acceso remoto. Es necesario también contar con protocolos adecuados para evitar la congestión de datos (RTP y RTSP).

### 3.4.5 PROTECCIÓN FÍSICA DE LAS CÁMARAS.

#### 3.4.5.1 DISEÑO DE LA CÁMARA/CARCASA

Las carcasas y los componentes fabricados en metal proporcionan mejor protección contra el vandalismo que las de plástico. Otro factor es la forma de la carcasa de la cámara. Una carcasa o una cámara fija convencional que sobresalga de una pared o techo es más vulnerable a ataques (patadas o golpes) que las carcasas con un diseño más discreto para domos fijas o domos PTZ. La cubierta suave y redondeada de una domo fija o domo PTZ dificulta más el hecho de, por ejemplo, bloquear la visión de la cámara colgando una pieza de ropa sobre ella. Cuanto más disimulada quede una carcasa o cámara en el entorno, o más se parezca a otra cosa distinta de una cámara, por ejemplo, a una luz exterior, mejor protegida estará contra el vandalismo. [20]



Figura 24. Tipos de carcasa.  
Fuente: [Elaboración Propia]



### 3.4.5.2 CUBIERTA TRANSPARENTE

La "ventana" o cubierta transparente de una carcasa suele estar fabricada en vidrio de alta calidad o de plástico policarbonato resistente. Puesto que las ventanas actúan como lentes ópticas, deben estar fabricadas en material de alta calidad para minimizar su efecto en la calidad de la imagen. La claridad se verá afectada si hay imperfecciones integradas en el material transparente. Las ventanas de las carcasas para domos y cámaras PTZ son las que requieren mayores exigencias. Las ventanas no sólo deben tener una forma perfecta de burbuja, sino que también deben tener mucha claridad, ya que podría aumentar las imperfecciones como partículas de suciedad, especialmente en cámaras con altos factores de zoom. Además, si el grosor de la ventana es desigual, en la imagen resultante una línea recta puede aparecer curvada. Una burbuja de alta calidad debería tener muy poco impacto en la calidad de la imagen, independientemente del nivel de zoom de la cámara y la posición del objetivo. El grosor de una burbuja puede aumentarse para que soporte golpes fuertes; sin embargo, tanto más gruesa sea, mayores son las posibilidades de que tenga imperfecciones. También es posible que un mayor grosor cree reflejos no deseados y refracción de la luz. Por ello, las cubiertas más gruesas deberían cumplir mayores requisitos con el fin de minimizar el efecto sobre la calidad de la imagen.

### 3.4.5.3 MONTAJE

También es importante el modo en el que están montadas las cámaras y las carcasas. Una cámara de red fija convencional y una cámara domo PTZ montadas en la superficie del techo son más vulnerables a ataques que una domo fija o domo PTZ montadas a ras del techo o pared, donde sólo se ve la parte transparente de la cámara. [20]



Figura 25. Carcasas para cámaras de red fijas montadas a ras del techo.  
Fuente: [Axis Communications]

#### 3.4.5.4 TIPOS DE MONTAJE

Las cámaras necesitan colocarse en todo tipo de ubicaciones y esto requiere una gran cantidad de variantes en el tipo de montaje.

##### ➤ Montaje en techos

Este tipo de montajes son los más utilizados en instalaciones de interior. La carcasa en sí misma puede ser:

- Un montaje en superficie: montada directamente sobre la superficie del techo y, por lo tanto, completamente visible.
- Un montaje empotrado: empotrada dentro del techo y con sólo parte de la cámara y carcasa (normalmente la burbuja) visibles.
- Un montaje colgante: carcasa que cuelga del techo como un colgante.



Figura 26. Montaje en superficie (izquierda), un montaje empotrado (centro) y un montaje colgante (derecha).  
Fuente: [Axis Communications]

### ➤ Montaje en pared

Los montajes en pared a menudo se utilizan para montar cámaras dentro o fuera de un edificio. La carcasa está conectada a una alarma, que está montada en la pared. Los montajes avanzados tienen un prensaestopas del cable interior para proteger el cable. Para instalar una carcasa en una esquina de un edificio se puede utilizar un montaje en pared normal, junto con un adaptador de esquina adicional. Otros montajes especiales son el montaje de kit colgante, que permite montar una cámara de red fija de un modo similar a una carcasa para domos PTZ.

### ➤ Montaje en poste

A menudo se utiliza el montaje en poste con una cámara PTZ en lugares como un aparcamiento. Este tipo de montaje normalmente tiene en cuenta el impacto del viento. Las dimensiones del poste y el propio montaje deben estar diseñados para minimizar las vibraciones. Los cables suelen estar dentro del poste y las tomas deben estar bien selladas. Las cámaras domo PTZ más avanzadas tienen un mecanismo de estabilización de imagen electrónico integrado para limitar las vibraciones y los efectos del viento.

### Montaje en parapeto

Los montajes en parapeto se utilizan para carcasas montadas en azoteas o para elevar la cámara y conseguir así mejor ángulo de visión. [20]



Figura 27.Montaje en parapeto.  
Fuente: [Axis Communications]

### 3.4.5.5 COLOCACIÓN DE CÁMARAS.

La colocación de la cámara también es un factor importante a la hora de disuadir el vandalismo. Si se coloca fuera de alcance en paredes altas o en el techo, se pueden evitar la mayoría de ataques espontáneos. La desventaja es el ángulo de visión que, hasta cierto punto, puede compensarse con un objetivo distinto.

### 3.4.5.6 VIDEO INTELIGENTE.

La función de alarma anti manipulación, ayuda a proteger las cámaras contra el vandalismo. Puede detectar si se ha modificado la dirección de la cámara, si se ha tapado o manipulado y puede enviar alarmas a los operadores. Esta función es especialmente útil en instalaciones con cientos de cámaras situadas en un entorno exigente donde es difícil controlar su correcto funcionamiento. También es útil en situaciones en las que no se visualizan las imágenes en directo y se puede avisar a los operadores cuando se manipulen las cámaras.



### **3.4.6 COMPRESIÓN.**

La compresión de video consiste en utilizar técnicas, que permitan reducir y eliminar datos redundantes del video, para que el archivo de video digital pueda enviarse a través de la red y almacenar en discos informáticos.

Con técnicas de compresión eficaces se puede reducir considerablemente el tamaño del fichero sin que ello afecte la calidad de la imagen.

La elección de una técnica adecuada de compresión depende de la tasa de grabación de imágenes, calidad de imágenes y consumo de ancho de banda,

Como ya se ha detallado anteriormente los formatos de compresión de video, es momento de comparar solo 3 formatos, los cuales se tendrán en cuenta para la realización de este proyecto.

#### **3.4.6.1 H264**

Es un estándar muy utilizado, esto debido a que sin comprometer la calidad de la imagen, un codificador H.264 puede reducir el tamaño de un archivo de video digital en más de un 80% si se compara con el formato Motion JPEG, y hasta un 50% más en comparación con el estándar MPEG-4. Esto significa que se requiere menos ancho de banda y espacio de almacenamiento para los archivos de video. Es así que se puede lograr mayor calidad de imagen de video para una frecuencia de bits determinada.

#### **3.4.6.2 MJPEG**

Una de las ventajas de Motion JPEG es que cada imagen de una secuencia de video puede conservar la misma calidad garantizada que se determina mediante el nivel de compresión elegido para la cámara de red o codificador de video. Cuanto más alto es el nivel de compresión, menor es el tamaño del archivo y la calidad de imagen

### 3.4.6.3 MPEG4

Una de las grandes ventajas que ofrece este formato es una muy buena calidad, muy parecida al del formato DVD, a cambio de un factor de compresión mucho más elevado que otros formatos, dando como resultado archivos o ficheros más comprimidos que otros e ideales para poder transmitir los datos a través de Internet. [21]

### 3.4.7 ALMACENAMIENTO.

Es muy importante a la hora de diseñar, debido que en un sistema de vigilancia requiere poder almacenar grandes cantidades de información. Dicha información de video puede ser almacenada en un servidor o en un disco duro. Para este diseño se tomará en cuenta la utilización de un NVR, para almacenar información.

El tipo de compresión de vídeo utilizado es uno de los factores que afectan a los requisitos de almacenamiento. El formato de compresión H.264 es de lejos la técnica de compresión de vídeo más eficiente que existe actualmente. Sin asegurar calidad de imagen, un codificador H.264 puede reducir el tamaño de un archivo de vídeo digital en más de un 80% comparado con el formato Motion JPEG y en más de un 50% con el estándar MPEG-4 (Parte 2). Esto significa que se necesita mucho menos ancho de banda de red y espacio de almacenamiento para un archivo de vídeo H.264. En las siguientes tablas, se proporcionan los cálculos de almacenamiento de muestra de los tres formatos de compresión. A causa de diversas variables que afectan a los niveles de frecuencia de bits media, los cálculos no son tan claros para los formatos H.264 y MPEG-4. Con relación a Motion JPEG, existe una fórmula clara porque cada imagen es un fichero individual. Los requisitos de almacenamiento para las grabaciones en Motion JPEG varían en función de la frecuencia de imagen, la resolución y el nivel de compresión.

### 3.4.7.1 CÁLCULO EN H.264

Velocidad binaria aprox. /8 (bits en un byte) x 3.600s = KB por hora/1.000=MB por hora.

MB por hora x horas de funcionamiento diarias/1.000 = GB por día.

GB por día x periodo de almacenamiento solicitado + Necesidades de almacenamiento.

Cámara	Resolución	Velocidad binaria aprox. (kbps)	Imágenes por segundo	MB/hora	Horas de funcionamiento	GB/día
No. 1	CIF	110	5	49.5	8	0.4
No. 2	CIF	250	15	112.5	8	0.9
No. 3	4CIF	600	15	270	12	3.2
Capacidad total para las 3 cámaras y 30 días de almacenamiento = 135 GB						

Tabla 3.Capacidad de almacenamiento: Formato H.264  
Fuente: [Axis Communications]

### 3.4.7.2 CÁLCULO EN MPEG-4

Velocidad binaria aprox. /8 (bits en un byte) x 3.600s = KB por hora/1.000 = MB por hora.

MB por hora x horas de funcionamiento diarias/1.000 = GB por día.

GB por día x periodo de almacenamiento solicitado = Necesidades de almacenamiento.



Nota: La fórmula no tiene en cuenta la cantidad de movimiento, factor importante que puede influir en el tamaño del almacenamiento requerido.

Cámara	Resolución	Velocidad binaria aprox. (kbps)	Imágenes por segundo	MB/hora	Horas de funcionamiento	GB/día
No. 1	CIF	170	5	76.5	8	0.6
No. 2	CIF	400	15	180	8	1.4
No. 3	4CIF	880	15	396	12	5
Capacidad total para las 3 cámaras y 30 días de almacenamiento = 204 GB						

Tabla 4.Capacidad de almacenamiento: Formato MPEG-4  
Fuente: [Axis Communications]

### 3.4.7.3 CÁLCULO EN MOTION JPEG

Tamaño de imagen x imágenes por segundo x 3.600s = kilobyte (KB) por hora/1.000 = megabyte (MB).

MB por hora x horas de funcionamiento diarias/1.000 = gigabyte (GB) por día.

GB por día x periodo de almacenamiento solicitado = Necesidades de almacenamiento. [22]

Cámara	Resolución	Velocidad binaria aprox. (kbps)	Imágenes por segundo	MB/hora	Horas de funcionamiento	GB/día
No. 1	CIF	13	5	234	8	1.9
No. 2	CIF	13	15	702	8	5.6
No. 3	4CIF	40	15	2160	12	26
Capacidad total para las 3 cámaras y 30 días de almacenamiento = 1.002 GB						

Tabla 5.Capacidad de almacenamiento: Formato JPEG  
Fuente: [Axis Communications]

### 3.4.8 SISTEMA DE CONTROL DE ACCESO

Los sistemas de control de acceso son la tecnología con más demanda en el mercado actual, hemos migrado de sistemas mecánicos y con personal especializado, a tener procesos de control de entrada y salida completamente automatizados con diferentes tipos de tecnologías y dispositivos. Es importante realizar un estudio adecuado, segmentando las zonas, los grupos de acceso, los horarios permitidos, el nivel de acceso de cada usuario, medir la cantidad de personas o carros que transitan por cada zona y establecer claramente los objetivos de cada control de acceso. Es importante el estudio y diseño previo a cualquier instalación y puesta en marcha de un proyecto de seguridad y control de acceso. Una adecuada integración de los dispositivos electrónicos con los dispositivos electromecánicos permitirá incluso reducir drásticamente los costos



de personal y totales del proyecto, haciendo incluso que un sistema de control de accesos se pueda pagar literalmente solo en un tiempo muy corto.

#### **3.4.8.1 BENEFICIOS DE UN SISTEMA DE CONTROL DE ACCESOS:**

- Control de Entradas y Salidas
- Mayor Seguridad y Control del Público
- Ahorro en Costos de Personal
- Capacidad de Diferir Pagos del Costos del Proyecto
- Rápido Retorno de la Inversión
- Disminución en Tiempo de Registro
- Mejoramiento en la Productividad del Personal
- Permitir/Restringir la Apertura de Puertas
- Valorización Monetaria de la Edificación
- Valor Agregado en Modernización

#### **3.4.8.2 CONTROL DE PERSONAL**

Es indispensable tener un control del personal que ingresa a determinadas áreas dentro de un establecimiento comercial, empresa, universidad, etc. De esta manera se busca restringir el ingreso a personas no autorizadas. Esto es posible implementando una unidad de control, la que permite registrar a una cantidad de personas en su base de datos, las cuales tendrán acceso a determinadas áreas restringidas. Esta unidad de control de acceso, permite también llevar un control de horarios, ingresos/salidas y asistencia del personal autorizado. Resulta de gran importancia integrar esta tecnología dentro de un sistema de seguridad, el cual se buscare sea eficiente. [23]

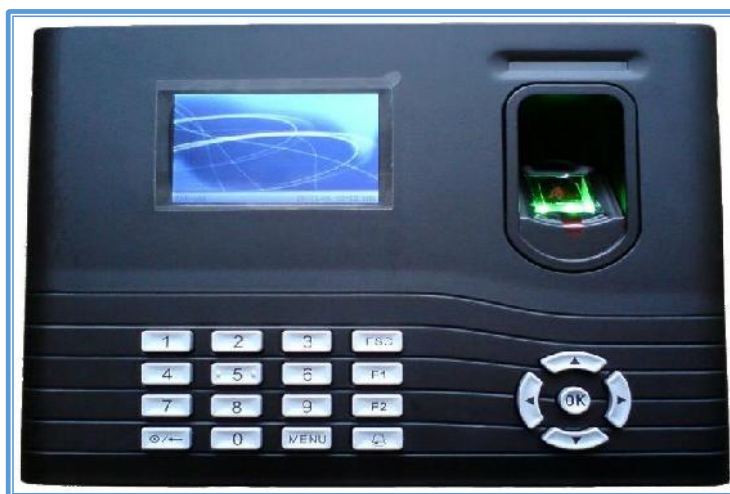


Figura 28.Unidad de Control de Acceso.  
Fuente: [Revista HikVISION]

### 3.5 PRESENTACION DE DISEÑO.

La complejidad de un sistema de Videovigilancia IP y un control de acceso, varía según la aplicación y lugar donde será implementado posteriormente. Resulta de gran importancia para el diseño y/o implementación de un sistema integrado de Videovigilancia IP y control de acceso, determinar las dimensiones de la zona de trabajo, que para en este proyecto son la instalaciones del “Mercado Central de Chiclayo”. El mercado cuenta un área total de  $4672.52 m^2$ , conformada por administración ( $14.35m^2$ ), SS.HH ( $68.00m^2$ ), Puestos ( $2707.61m^2$ ), Tiendas ( $51.64m^2$ ) y Pasadizos ( $1830.92m^2$ ). Existen 4 pasadizos que sobresalen de la zona central de mercado y permiten el acceso/salida, de sus instalaciones. La edificación se ha dividido en 4 sectores independientemente.

Se desarrollará el diseño del sistema integrado de videovigilancia IP y control de acceso, tomando en cuenta los parámetros antes vistos. De acuerdo a esto se distribuirán los elementos del sistema para lograr cubrir todas las zonas, así también ubicar la unidad de control de acceso, además de usar los elementos necesarios. Es de consideración importante la cantidad de elementos en la red;



la utilización de elementos mayor a los necesarios, podría conllevar a una sobrecarga de la red por el alto consumo de ancho de banda. Teniendo en cuenta estas consideraciones, conducirán a un sistema eficiente y sin sobrecarga de red. Por último y no menos importante, es el uso de la unidad de control de acceso. Su ubicación será determinada por la zona donde se realizara el monitoreo del sistema de videovigilancia IP. El lugar elegido para este fin es el área de Administración.

Una vez conocida el área de la zona de trabajo, posteriormente se realizara la distribución de las cámaras, de esta manera se conocerá el número que se empleara. Cabe recordar que en un sistema de videovigilancia basado en red IP, resulta flexible en la ampliación del sistema, lo que permite sea fácil y económico, además, cada elemento del sistema puede adaptarse según las necesidades. En la sección anterior se desarrolló las consideraciones que se debe tener para el diseño, al igual que los parámetros de los elementos que lo conforman. En esta sección, basados en las consideraciones y parámetros, se procederá a elegir todos los elementos.

Ayudados por el software “IP Video System Design Tool 8” en su versión de prueba, se lograra medir los parámetros para la correcta elección de los elementos del sistema. Los parámetros que se calcularán son: la capacidad del disco para el servidor (necesaria para almacenar toda la información), cálculo de los lentes y sensor de la cámara, y la estimación del ancho de banda obtenido según el número de cámaras que se propongan. En estos cálculos influye el tipo de formato de compresión utilizado, el cual se establecerá según convenga en el diseño.



### **3.5.1 ENTORNO DEL SISTEMA.**

#### **3.5.1.1 ELECCIÓN DEL FORMATO DE COMPRESIÓN**

Para el diseño y habiendo analizado los distintos formatos de compresión se ha convenido emplear el estándar H.264. Permite reducir más de un 80% en tamaño de un archivo de video digital si se compara con el formato Motion JPEG, y hasta un 50% más en comparación con el estándar MPEG-4. Esto significa que se requiere menos ancho de banda y espacio de almacenamiento para los archivos de vídeo. O, visto de otra manera, se puede lograr mayor calidad de imagen de vídeo para una frecuencia de bits determinada. Esto es posible, ya que las cámaras IP que se han tenido en cuenta tienen como característica de compresión este formato.

#### **3.5.1.2 PARÁMETROS DE LAS CÁMARAS.**

El diseño del sistema de videovigilancia, se basa en el uso de cámaras IP, las cuales son capaces de emitir imágenes directamente a la red, sin la necesidad de un ordenador para ser procesadas.

Las cámaras consideradas para el diseño cuentan con una dirección IP predispuestas, funciones de servidor independiente, servidor FTP; todo lo necesario para la visualización local o remota de las imágenes a través de la red está incluida en la cámara. Protocolos como HTTP, DDNS, FTP, TCP/IP, etc., son parte de las características de las cámaras IP elegidas para el diseño y las responsables de las funciones de estos equipos.

Por otra parte, las cámaras IP poseen una lente que enfoca la imagen en el sensor de imágenes (CCD o). Antes de llegar al sensor, la imagen pasa a través del filtro óptico, que elimina cualquier luz infrarroja, para que los colores mostrados sean los correctos. El sensor de imagen convierte la imagen, compuesta por información lumínica, en señales eléctricas. Estas señales eléctricas digitales están ya en un formato que puede comprimirse y enviarse a

través de la red. A continuación se presenta una imagen con una estructura interna de una cámara IP.

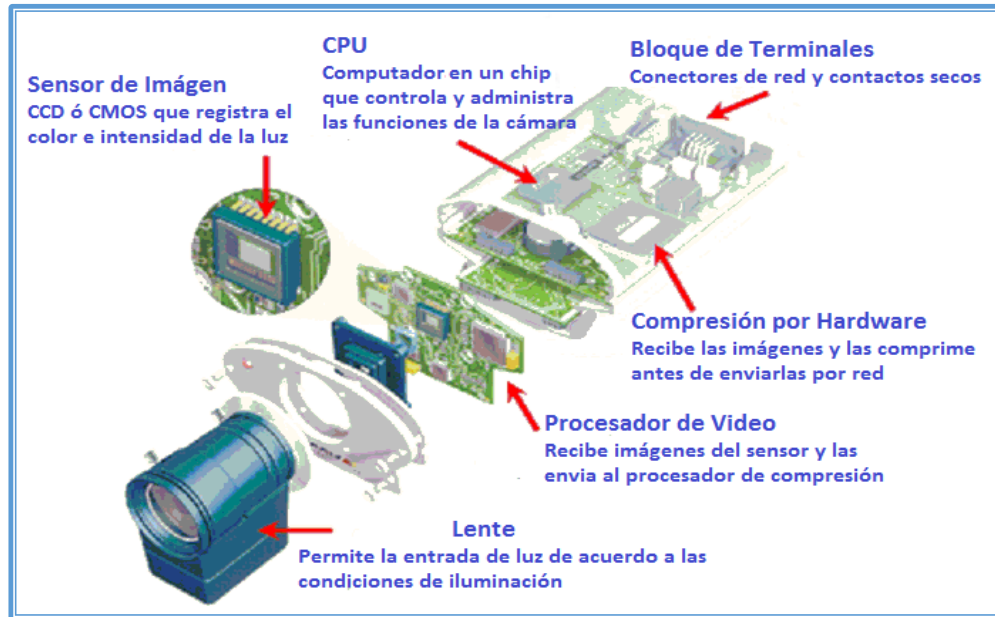


Figura 29.Arquitectura de una cámara IP.  
Fuente: [24]

### 3.5.1.2.1 SENSOR DE IMAGEN.

Las cámaras IP capturan las imágenes con los chips sensores de imagen y estos se dividen entre los CCD (Charge Coupled Device o Dispositivo de Cargas Acopladas), que fueron los primeros en aparecer en el mercado, y los más recientes CMOS (Complementary Metal Oxide Semiconductor – Semiconductor de Óxido de Metal Complementario). La captura de las imágenes se hace a través de sensores CCD y CMOS. Ambos tipos de sensores, están fabricados con materiales semiconductores de Metal-Óxido (MOS) y estructurados en forma de matriz. Acumulan una carga eléctrica en cada celda de la matriz (o pixel) en proporción a la intensidad de luz que incide sobre ella localmente.

No obstante, existen ventajas y desventajas en cada uno de ellos:





### A. Ventajas de cámaras IP con sensores CCD.

**Rango Dinámico:** (RD) Es el cociente entre el nivel de saturación de los píxeles y el umbral por debajo del cual no captan señal. En este aspecto CCD supera a CMOS en un factor de dos, dado que en la actualidad el RD de un sensor CCD es típicamente del doble que el de un CMOS

**Ruido:** Los sensores CCD aventajan a los de tecnología CMOS en este apartado, ya que debido a su construcción todo el procesamiento de señal se da fuera del CCD, con lo que se podrá aprovechar la mejor tecnología disponible en convertidores A/D, pudiendo elegir los más rápidos o mejores procesadores. Por su parte, los CMOS al realizar la gran mayoría de las funciones dentro del sensor (amplificación, conversión A/D, etc.) destinan menos espacio para los fotodiodos encargados de recoger la luz, por lo que se produce más ruidos en la lectura.

**Respuesta Uniforme:** Idealmente se espera que un píxel sometido al mismo nivel de excitación de luz que sus vecinos no presente cambios apreciables respecto de ellos. En este aspecto la individualidad de cada píxel de un sensor CMOS los hace más sensibles a sufrir fallos, siendo mayor la uniformidad en CCD.

### B. Ventajas de cámaras IP con sensores CMOS

**Precio:** Las cámaras IP CMOS son mucho más económicas que las CCD debido a que tienen menos circuitería por lo que son más baratas de fabricar.

**Consumo Eléctrico:** la tecnología CMOS por su fabricación, consume mucha menos electricidad que los CCD. Normalmente las cámaras IP CMOS de Zavio tienen transformadores de 220V a 5V 1.2A y las cámaras IP CCD de 220V a 12V 1.25A.

**Velocidad:** Si nos concentramos en la velocidad con la que se captura la imagen, veremos que los CMOS son bastante superiores a los CCD, debido a que muchas





funciones, como la propia conversión analógico-digital son realizadas en el propio sensor.

**Blooming:** Esta palabra define el fenómeno por el cual un píxel que ha alcanzado la saturación empieza a saturar a sus vecinos, creando efectos y patrones no deseados. Esto se da principalmente en sensores CCD, que necesitan de algunos trucos de construcción para evitarlos. En cambio, gracias a su construcción los sensores CMOS no sufren de este defecto. Los sensores CMOS son mejores a la hora de capturar imágenes como brillos que refleja un anillo, o el reflejo de la luz del sol sobre un lago.

En conclusión, los sensores CCD son más sensibles que los CMOS por lo que son mucho mejores en situaciones de poca luz, y los CCD tienden a darnos una imagen más limpia que los CMOS que nos pueden dar más ruidos (pequeños defectos en la imagen) pero hay que recordar que los CMOS son más económicos y consumen menos electricidad. Sin embargo para nuestro diseño se opta por cámaras IP con tecnología CMOS. Es importante tener en cuenta la estructura del mercado, el cual permite un ingreso de luz exterior moderado y a ello se suma la iluminación en su interior. Por otra parte tenemos que tener en cuenta que en la actualidad las limitaciones de los CMOS están prácticamente subsanadas o compensadas (cámaras con iluminación infraroja IR). La tecnología CCD ha llegado a su límite y es ahora cuando se está desarrollando la CMOS. Así mismo hacemos uso de las ventajas mencionadas, que nos proporciona la tecnología CMOS. [25]

### 3.5.1.2.2 TAMAÑO DEL SENSOR.

Ya considerado el tipo de sensor (CMOS), un parámetro adicional de importancia, es el tamaño del sensor, que varía de acuerdo a la distancia del objeto que se quiere detectar y su ancho. Entre los más comerciales se tiene los de  $2/3"$ ,  $1/2"$ ,  $1/3"$  y  $1/4"$ .

Esta característica es muy importante y tiene que ser considerada en un sistema de vigilancia para poder captar sin problemas la imagen. Si, por ejemplo, un lente está dispuesto para un sensor más pequeño que el que está colocado dentro de la cámara, la imagen mostrará esquinas de color negro. Pero si un lente está dispuesto para un sensor mayor que el que está colocado dentro de la cámara, el ángulo de visión será menor que el ángulo por defecto de dicho objetivo, dando como resultado la pérdida de una parte de la información. Esta característica se demuestra en la siguiente imagen.

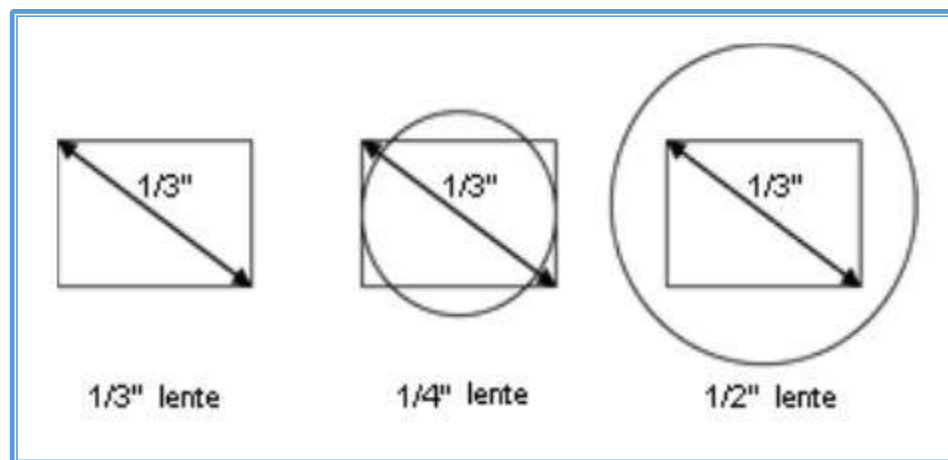


Figura 30. Relación de tamaños entre el lente y sensor.  
Fuente: [Axis Communications]

Como se puede observar, existe un sensor que se acomoda a un lente específico, es por eso que es importante tener en cuenta la relación que los dos componentes tienen entre ellos. En tal sentido, la elección del tamaño del sensor depende de la elección del lente.

### 3.5.1.2.3 SELECCIÓN DEL TIPO DE LENTE.

El lente es el encargado de capturar la imagen, que luego será procesada por los demás componentes de la cámara IP.

El lente varía de tamaño y características según la imagen específica que se quiera detectar, y, además, está relacionado con el tamaño del sensor.

Para el lente existen dos montajes estándar (montaje C y CS) que se diferencian en la distancia de ambas lentes al sensor cuando se acoplan en la cámara:

- Montura CS. La distancia entre el sensor y la lente es 12.5mm.
- Montura C. La distancia entre el sensor y la lente es 17.5mm. Se puede utilizar un espaciador de 5mm (anillo adaptador C/CS) para convertir una lente C a montaje CS.

#### A. Tipos de lentes

El tipo de lente se escoge de acuerdo a la distancia focal y está relacionado con el tamaño y tipo de sensor que se utilice.

- **LENTE FIJO:**

Es un objetivo con una distancia focal fija.

#### Ventaja de tener un lente fijo:

- Más ligeros.

El interior del lente es menos complicado, lo que significa que tendrás un objetivo más liviano con el que trabajar.

- Calidad de imagen.

Por lo general es más pequeño y más ligero que un zoom. Al ofrecer mayor apertura máxima, brinda una mejor capacidad de captar la luz en comparación

con un zoom, el cual está diseñado para compensar sus características, con las variables de distancias focales.

➤ Más baratos.

Otro de los beneficios de los lentes fijos es que son menos costosos en comparación con los zoom, debido a una construcción más sencilla.

#### **Desventaja de tener un lente fijo:**

La única desventaja es que los objetivos de focal fija no son tan versátiles como un zoom.



Figura 31. Lente Fijo.  
Fuente: [Lentes Objetivo fijo NIKKOR]

- **LENTE VARIFOCAL:**

Esta lente permite el ajuste manual de la longitud focal (campo de visualización). Cuando la longitud focal se cambia, el objetivo tiene que volver a enfocarse. Los tipos más comunes están en el rango de 3,5 - 8mm.



Figura 32. Lente Varifocal.  
Fuente: [Lentes Objetivo CCTV-KOWA]

## B. Requisitos de longitud focal.

Otro parámetro con respecto a la cámara es la longitud focal, que viene a ser la distancia entre el centro óptico de la lente o plano nodal posterior y el foco (o punto focal) cuando enfocamos al infinito. La distancia focal se mide en milímetros, y suele variar entre 2.25 mm y 16 mm en cámaras IP, aunque por supuesto hay lentes con medidas en el mercado mucho mayores y menores.

En el mercado existen cámaras con lente fija que no permite realizar acercamiento a distancias fuera de su rango de visión (Con distancia focal única), pero resulta adecuada para una distancias limitada o corta y las cámaras varifocales que llevan una lente como el nombre indica, que se puede variar manual o electrónicamente.

Una lente de menos milímetros abre más su ángulo de visión que una lente de mayor milímetro. Ejemplo, cuando queremos hacer un zoom a algo, utilizaríamos lentes con una distancia focal con mayor número de milímetros, y cuando queremos ver una imagen que abarque el mayor espacio, una de menos milímetros. [26]

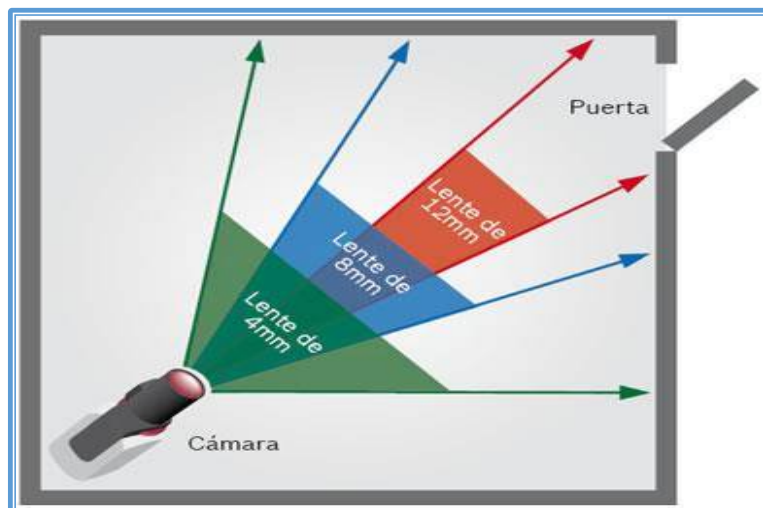


Figura 33.Apertura del lente.  
Fuente: [27]

Lente	1/2"	1/3"	1/4"
Tamaño del Sensor (ancho)	6.4mm	4.8mm	3.2mm

Tabla 6.Relación entre lente y el tamaño del sensor.  
Fuente: [Axis Communications]

### C. Tipo de Iris.

Es el iris el responsable de ajustar la cantidad óptima de luz que pasa a través del lente. De esta manera se asegura contar con una buena calidad de imagen. Generalmente, las cámaras IP controlan la cantidad de luz que pasa al mecanismo de imagen a través del iris o ajustando el tiempo de exposición. Existen dos tipos de control de iris: manual y automático.

- Iris manual: Cuando se cuenta con un lente de iris manual, este se debe ajustar adecuadamente al momento de la instalación de la cámara, teniendo en cuenta las condiciones de luz del ambiente. No resulta conveniente el uso en ambientes donde las condiciones de luz son variables, o se busca ajustar el iris a un valor medio. No es recomendable para aplicaciones de vigilancia exterior.
- Iris automático: Este tipo de control es el que cuenta las cámaras para el diseño. Existen dos tipos de lente con iris automático: Iris DC e iris de vídeo. Ambos se ajustan automáticamente a las condiciones de luz. Ambos emplean una señal analógica para control la apertura del iris. La diferencia radica en la ubicación de los circuitos para convertir la señal analógica en señales de control del motor. Iris DC (circuito dentro de la cámara e Iris de Video (circuito dentro del lente).

En este caso, las cámaras para el diseño, cuentan con un lente con iris automático DC. El iris se encargara de ajustar los niveles de luz que alcanzan la

cámara y a la vez protege al sensor de imagen ante un exceso. Según el diámetro del iris, será posible una reducción de luz, proporcionando una distancia mayor de visión (diámetro pequeño) y poder ofrecer buenas imágenes en situaciones de luz escasa (diámetro grande).

El iris está definido por el número F:

Número F = longitud focal / diámetro del iris

Cuanto mayor sea el número F, menor será la luz admitida en el sensor. Cuanto menor sea el número F, mayor luz será admitida en el sensor y, por lo tanto, se logrará una calidad de imagen superior en condiciones de escasa luz.



Figura 34. Apertura Relativa.  
Fuente: [28]

#### 3.5.1.2.4 CÁLCULOS DEL DISEÑO.

Para el diseño a resultado conveniente valerse de tres tipos de cámara y una unidad de acceso, las que en conjunto permiten establecer un diseño óptimo y eficaz.





En el cálculo de los parámetros requeridos en el diseño del sistema de video IP, una herramienta adecuada es el software **IP Video System Design Tool 8**, con el cual se pudo trabajar de forma rápida, fácil y precisa.

Considerando las distancias en el diseño, el ancho de la escena que captura la cámara, se ajustara a la distancia de visión requerida para el diseño. Hay que tener en cuenta que dos tipos de cámaras estarán ubicadas en los pasadizos de un máximo de 3 metros de ancho. Lo que se busca es lograr la distancia de visión requerida para el diseño. Teniendo una distancia fija para cada tipo de cámara, no resulta una limitante en la proyección de la visión ya que esta va más allá. Se precisa tener la mejor calidad posible en las imágenes captadas por las cámaras, por lo que en el diseño se le asigna una distancia adecuada; la visión se sigue proyectando pasada esta distancia fija, no con la misma calidad pero hace posible se identifique y se haga un reconocimiento de los sucesos captados por las cámaras. Cabe mencionar que la distancia de visión (mayor o menor distancia al punto fijo asignado) depende del tipo de lente, y este al variar, también lo hace el ancho de la escena capturada por la cámara.

En administración habrá un tercer tipo de cámara, aquí el parámetro principal será el ancho de la escena más que la distancia de visión.

Por otra parte se debe considerar parámetros como son la altura en la que se colocaran las cámaras, la altura del campo de visión a una altura específica, el ángulo de inclinación, la zona muerta, anchura de la zona muerta, relación de aspectos, etc. Parámetros que serán posibles manejar con el software.

Para las cámaras ubicadas en los pasadizos de las instalaciones del mercado (Cámara para exteriores):

- **Cámara HKDS2CD2732 F-I.**

Estas cámaras estarán ubicadas en los pasadizos. Este tipo de cámara cuenta con un lente varifocal, que permite tener un alcance de visión mayor con relación al otro tipo de cámara, que también se ubicara en los pasadizos, pero



será menor la distancia que tendrán que llegar a captar. La posibilidad de acercamiento y el alcance de visión permiten que a distancias de 30 metros proporcione una óptima calidad de imagen.

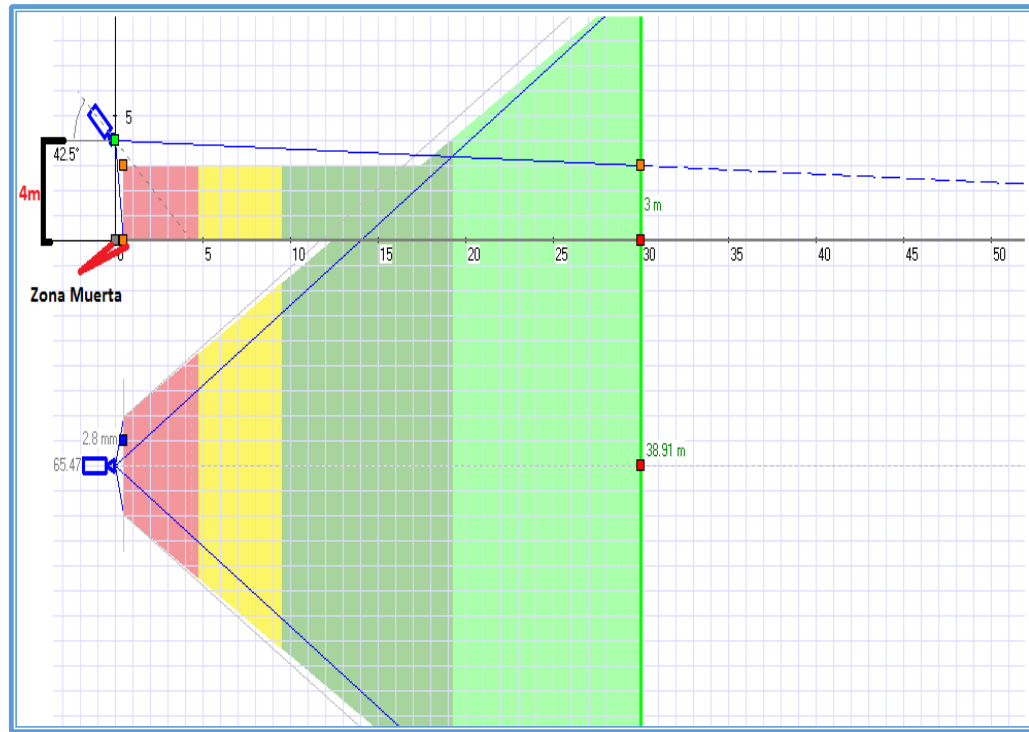


Figura 35. Dibujo de instalación de Cámaras (Relación de aspecto 3:4).  
Fuente: [IP Video System Design Tool]

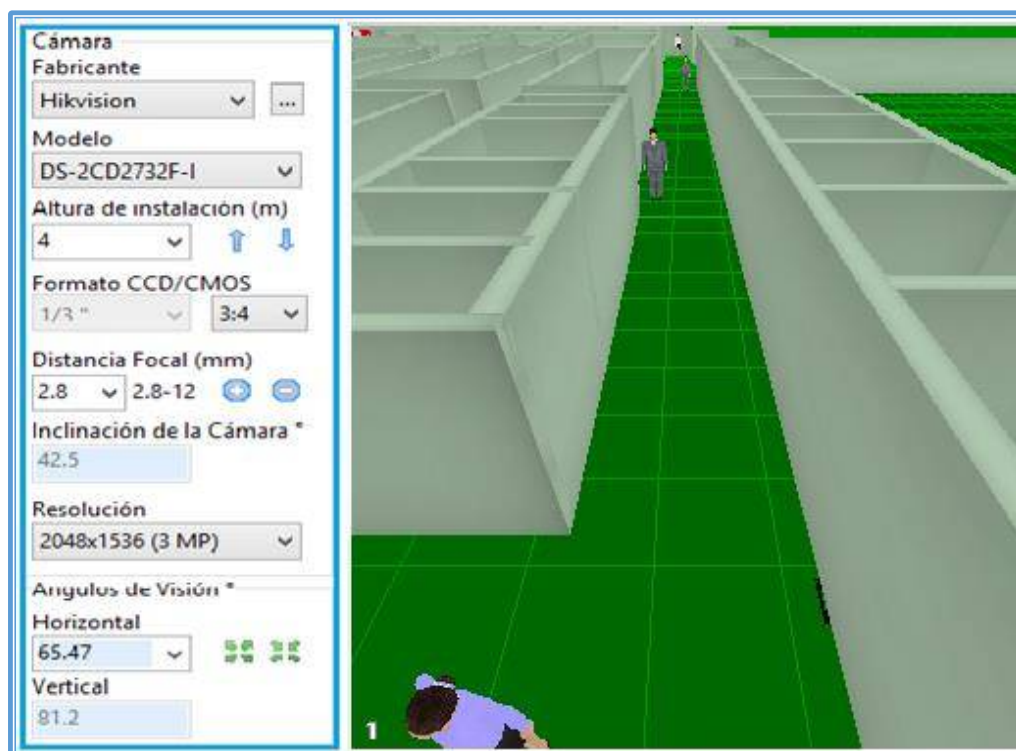


Figura 36. Vista 3D – Relación de aspectos 3:4.  
Fuente: [IP Video System Design Tool]



Figura 37. Relación de aspectos 4:3.  
Fuente: [IP Video System Design Tool]

En este caso con una relación de aspecto de 3:4 se obtiene una zona muerta (0.48m) menor que la obtenida con la relación 4:3 y una imagen más enfocada en los pasadizos.

El ancho de la escena es de 38.91 m. Dada la disposición a una altura de 4 metros el ancho de escena no solo se verá limitada en los pasadizos.

El lente varifocal con el que cuenta esta cámara, permite llegar a tener una distancia focal de 12mm, así poder hacer un acercamiento al punto fijo asignado como distancia y a la vez una proyección de la zona de visión pasado este punto. Por otra parte el ancho de escena disminuye, comprobando lo ya antes mencionado en una sección anterior.



Figura 38. Visión con una distancia focal de 12mm.  
Fuente: [IP Video System Design Tool]

- **Cámara HKDS2CD2132 -I.**

Al igual que el caso anterior, esta cámara también se ubicará en los pasadizos. Para esta cámara se ha considerado cubrir, una distancia máxima de 23 metros. A diferencia de la anterior no se requiere que la visión de proyectora pasado esta distancia fija, por lo que esta cámara cuenta con un lente fijo de 4mm de distancia focal.

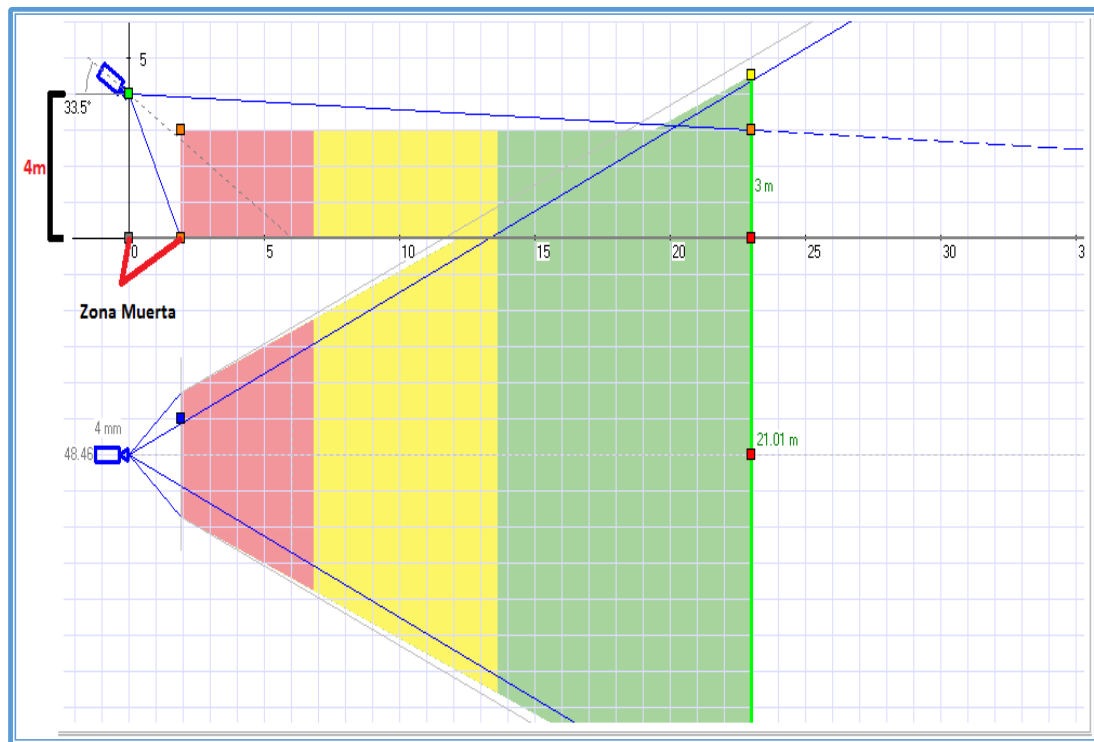


Figura 39. Dibujo de instalación de Cámaras (Relación de aspecto 3:4).  
Fuente: [IP Video System Design Tool]

Cabe señalar que las imágenes captadas por estas cámaras se complementarán con la visión desde otros ángulos, con las distintas cámaras distribuidas. De esta manera si no hubiera cierta claridad en un evento captado por esta cámara, se compensará con las imágenes de otra cámara que tenga visión de la misma zona.

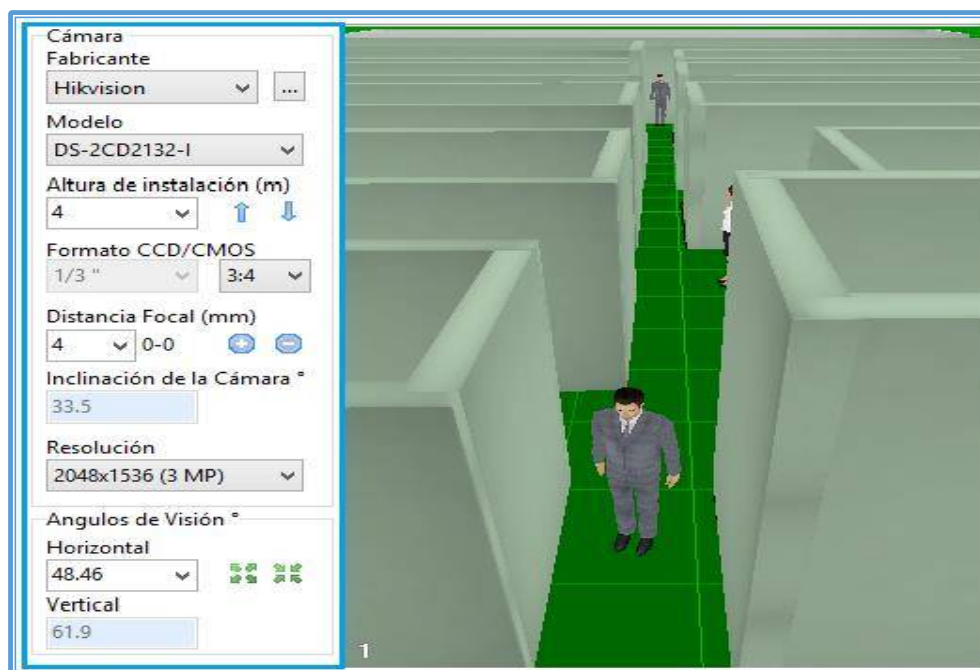


Figura 40. Vista 3D – Relación de aspecto 3:4 (Cámara 1).  
Fuente: [IP Video System Design Tool]

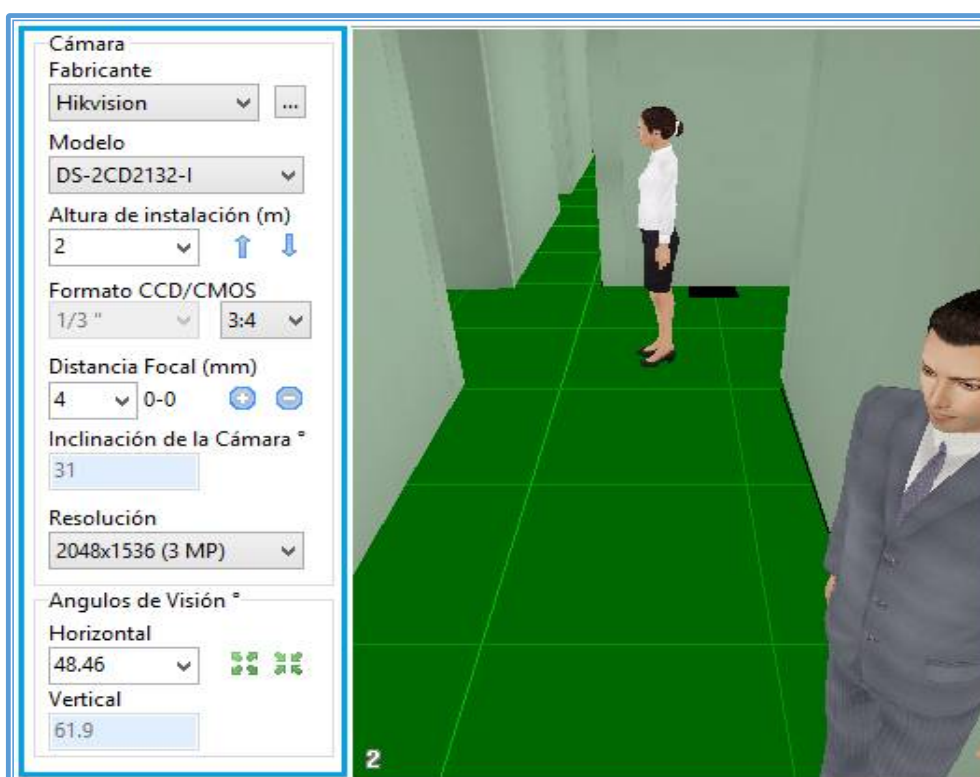


Figura 41. Vista 3D – Relación de aspecto 3:4 (Cámara 2).  
Fuente: [IP Video System Design Tool]



Tomando las imágenes de 2 cámaras, dispuestas para un pasadizo se logra tener una visión completa de este. Las zonas muertas varían levemente (1.92 y 1.07m) entre la cámara 1 y 2. Por otro lado se observa que para la cámara 1 existe un bloqueo de visión, por lo que esa zona es cubierta por la cámara 2. Ambas están en una relación de aspecto de 3:4 y su con respecto al ancho de escena, los valores son de 21.1 m para la cámara 1 y 20.8 m para la cámara 2. En las alturas, hay una leve variación en la disposición de la cámara 2, pues esta se colorara a una altura de 2 metros; la visión será óptima para cubrir la zona por la que se dispuso contar con la cámara 2.

En el NVR una visión conjunta, seria de esta manera:

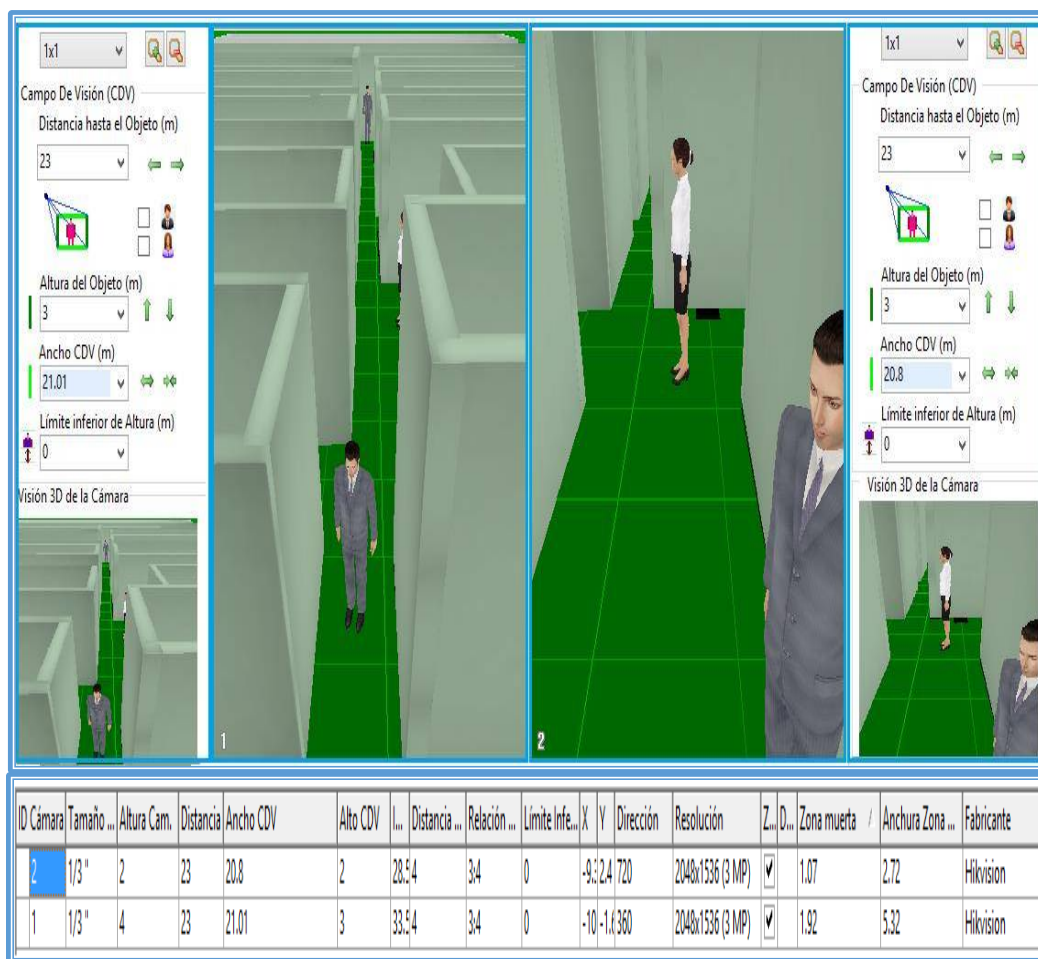


Figura 42. Vista NVR- Relación de aspecto 3:4.

Fuente: [IP Video System Design Tool]

Para la cámara dispuesta en administración:

- **Cámara HKDS2CD2132 -I.**

En el diseño se dispuso contar con este tipo de cámara para el área de administración. Es aquí donde se realizara el monitoreo de las cámaras; y por otra parte se ubicaran los equipos que forman parte del sistema de vigilancia IP.

Esta cámara cuenta con un lente varifocal de 2.7 – 9 mm .Se ha considerado una distancia fija de 6 metros. Se ha previsto con este tipo de cámara, un adecuado ancho de escena para cubrir ampliamente la zona de administración.

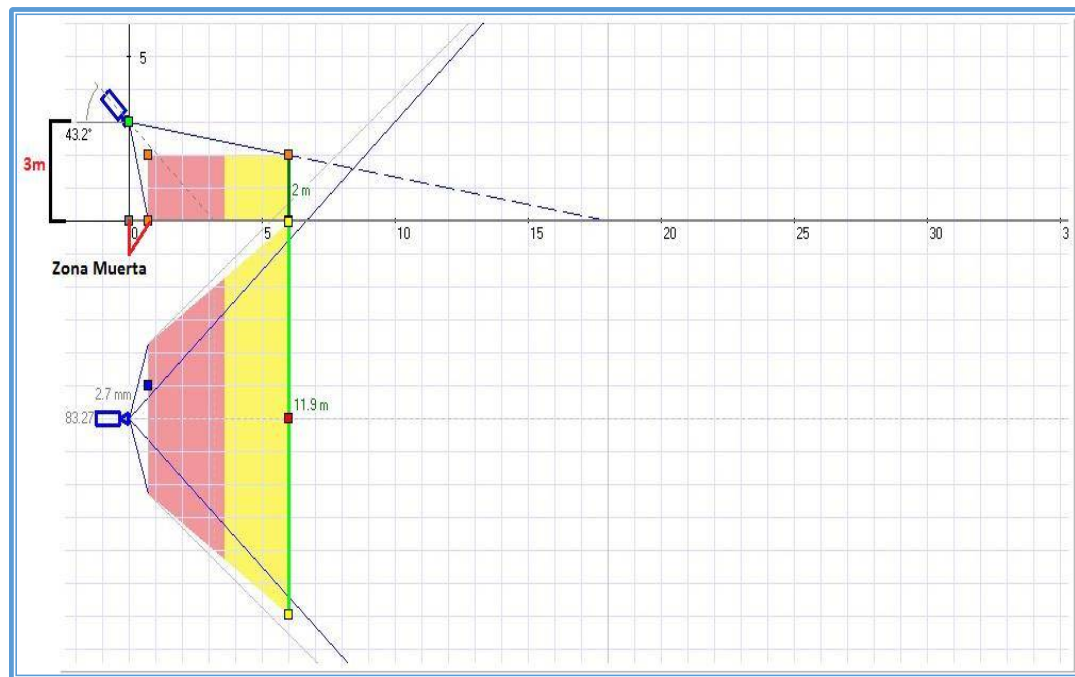


Figura 43.Dibujo de instalación de Cámaras (Relación de aspecto 4:3).  
Fuente: [IP Video System Design Tool]

En este caso la relación de aspecto es de 4:3, siendo la adecuada para visualizar las escenas q se registraran en administración.

La zona muerta en la disposición de esta cámara es mínima (0.7 m), lo que permite tener una visión total de los suceda en administración.

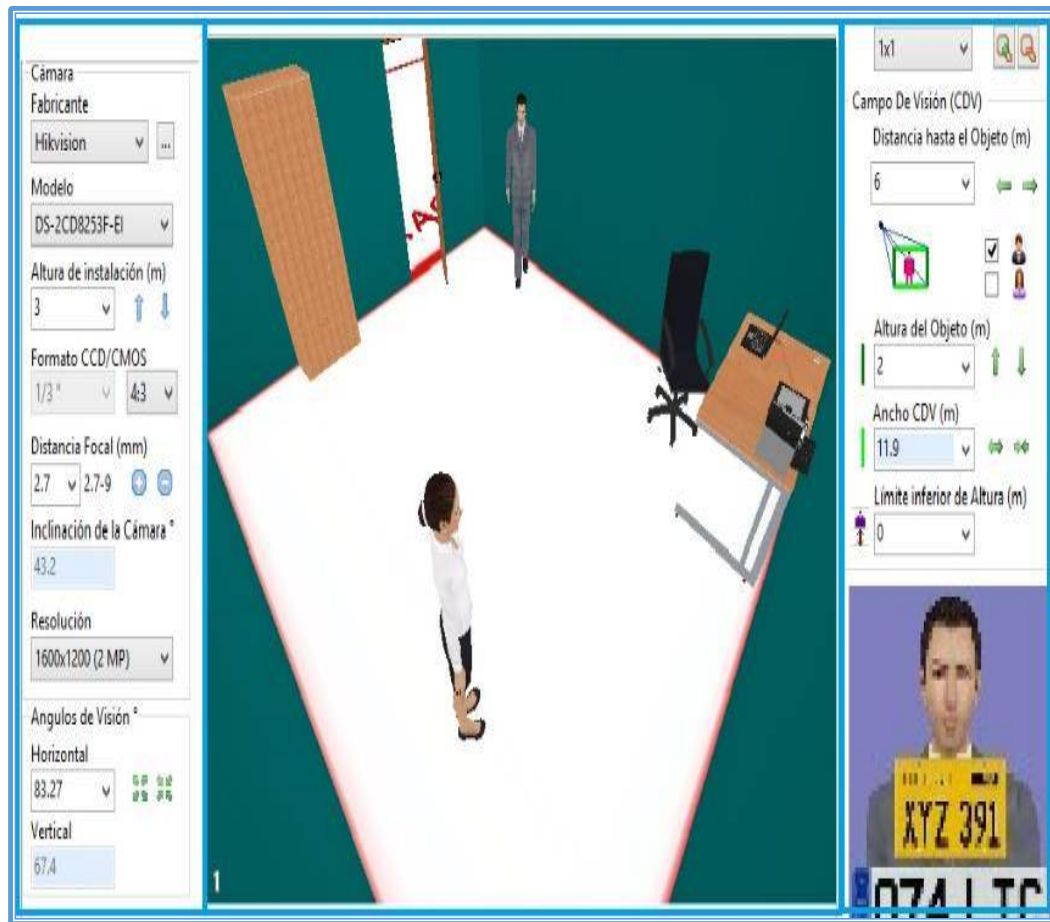


Figura 44. Vista 3D- Relación de aspecto 4:3.  
Fuente: [IP Video System Design Tool]

Con un ancho de escena de 11.9m a una distancia focal de 2.7mm es posible tener una adecuada visión en el área de administración; el ancho de escena disminuirá al realizar un acercamiento, aumentando la distancia focal (máx. 9mm). Hay que recordar que esta cámara siendo varifocal, es posible realizar un acercamiento para obtener imágenes más precisas al momento de realizar una identificación o recuento de los sucesos.



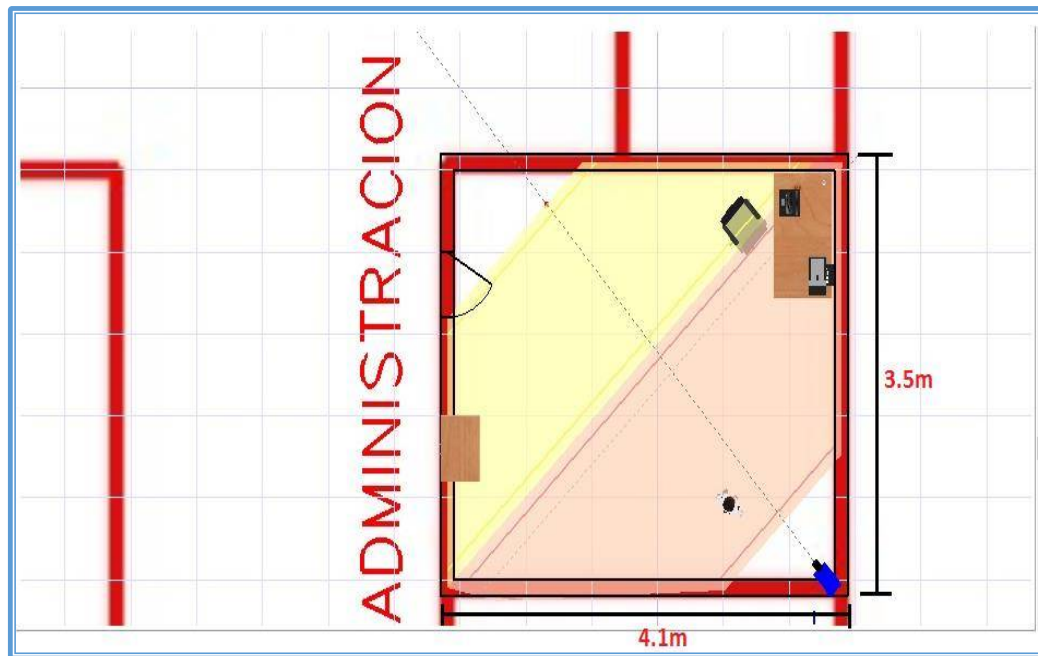


Figura 45. Vista en el plano del Área de administración.  
Fuente: [AutoCad]

### 3.5.1.3 CAPACIDAD DE ALMACENAMIENTO.

Los principales parámetros para hallar la capacidad de almacenamiento son el número de cámaras, el número de horas que estarán activas las cámaras, cuantos días a la semana y la frecuencia de imágenes que utilicen las cámaras.

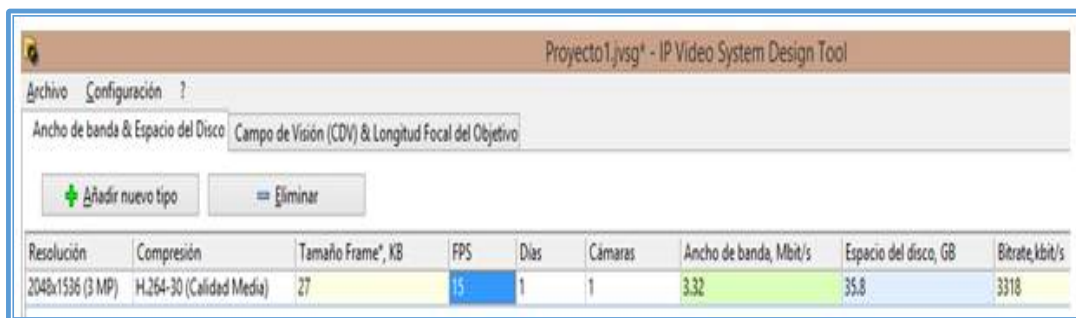
También es necesario tener en cuenta el formato de compresión de video que en este caso se ha considerado sea H.264.

Para hacer estos cálculos utilizaremos el software “**IP Video System Design Tool**”, el cual nos brinda valores exactos y nos ahorra tiempo en el cálculo de estos valores.

Este cálculo lo realizaremos con los 3 tipos de cámaras IP que hemos considerado para el diseño.

- **Cámara HKDS2CD2732 F-I.**

Los parámetros que necesitamos ingresar al software son la resolución que es 2048 x 1536, el formato de compresión H264 y los fps que son igual a 15. Consideremos para una sola cámara y para un día entero de grabación.



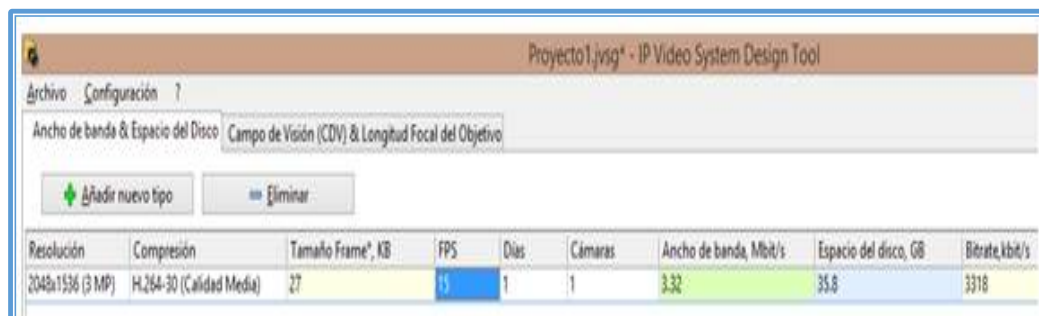
Resolución	Compresión	Tamaño Frame*, KB	FPS	Días	Cámaras	Ancho de banda, Mbit/s	Espacio del disco, GB	Bitrate, kbit/s
2048x1536 (3 MP)	H.264-30 (Calidad Media)	27	15	1	1	3.32	35.8	3318

Figura 46.Almacenamiento-Cámara HKDS2CD2732 F – I.  
Fuente: [IP Video System Design Tool]

Entonces obtenemos los valores de 35.8 GB que es la capacidad de almacenamiento a una tasa de bits de 3318 kbits/s.

- **Cámara HKDS2CD2132 -I.**

Los parámetros que ingresaremos al software son la resolución 2048 x 1536, el formato de compresión H264 y los fps que son igual a 15. Consideremos para una sola cámara y para un día entero de grabación.



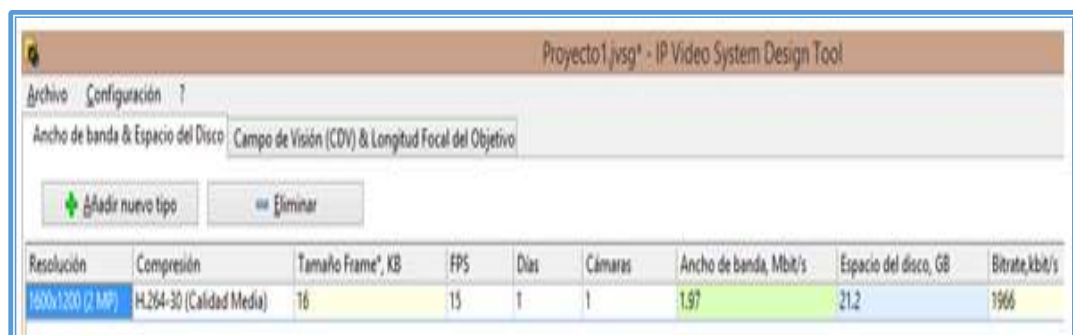
Resolución	Compresión	Tamaño Frame*, KB	FPS	Días	Cámaras	Ancho de banda, Mbit/s	Espacio del disco, GB	Bitrate, kbit/s
2048x1536 (3 MP)	H.264-30 (Calidad Media)	27	15	1	1	3.32	35.8	3318

Figura 47.Almacenamiento-Cámara HKDS2CD2132 - I.  
Fuente: [IP Video System Design Tool]

Obtenemos los valores de 35.8 GB que es la capacidad de almacenamiento a una tasa de bits de 3318 kbits/s.

- **Cámara HKDS2CD2132 -I.**

Por último ingresaremos al software los parámetros como la resolución 2048 x 1536, el formato de compresión H.264 y los fps que son igual a 15. Igual que en los casos anteriores consideremos una sola cámara y para un día entero de grabación.



Resolución	Compresión	Tamaño Frame*, KB	FPS	Días	Cámaras	Ancho de banda, Mbit/s	Espacio del disco, GB	Bitrate, kbit/s
1080x1280 (2 MP)	H.264-30 (Calidad Media)	16	15	1	1	1.97	21.2	1966

Figura 48. Almacenamiento-Cámara HKDS2CD8253F – EI.  
Fuente: [IP Video System Design Tool]

La capacidad de almacenamiento para este caso es de 21.2 GB a una tasa de bits de 1966 kbits/s.

### 3.5.1.4 DISTRIBUCIÓN DE LAS CÁMARAS IP Y UNIDAD DE CONTROL DE ACCESO.

El “Mercado central de Chiclayo” cuenta con una estructura metálica. Vigas y columnas de acero, son las sostiene el techo. Dicha estructura puede ser aprovechada para la instalación de las cámaras, de esta manera valerse de las estructuras del mercado. Cabe señalar que cada cámara dispondrá de su correspondiente soporte y accesorio, que se acondicionara al medio, permitiendo su instalación. También la disposición de los puestos y el que alguno de estos, cuente con un almacén en la parte superior (encima del puesto), permite

aprovechar estos medios para la instalación de las cámaras. Lo mencionado hace posible se facilite la instalación de las cámaras.

### 3.5.1.4.1 MEDIDAS

El “Mercado central de Chiclayo” cuenta con un área de  $4672.52 \text{ m}^2$ , en las que se disponen áreas para: administración, SS.HH, puestos, tiendas y pasadizos. Existen 4 pasadizos que sobresalen de la zona central del mercado y permiten el acceso/salida, de sus instalaciones. La edificación se ha dividido en 4 sectores independientemente, para un mejor manejo y visualización en la distribución de las cámaras IP, así como en la ubicación de la unidad de control de acceso.

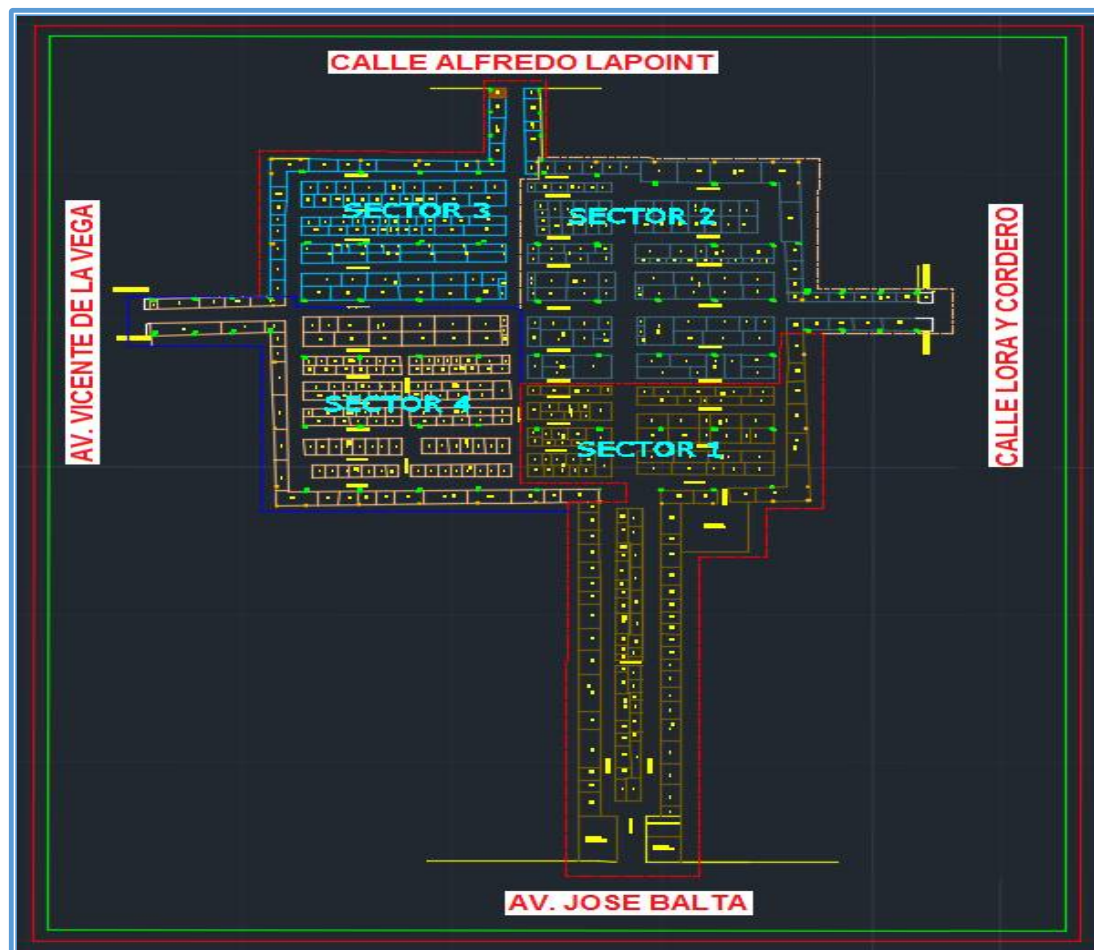


Figura 49. Plano sectorizado en AutoCAD del “Mercado Central de Chiclayo”.  
Fuente: [AutoCad]

A continuación se muestra, las gráficas de los 4 sectores en los que fue dividido el plano original del “Mercado central de Chiclayo”. Se podrá visualizar medidas, que sirven de referencia para saber si las distancias de visión y cobertura asignadas a cada cámara IP, dispuestas en los pasadizos, son las adecuadas.

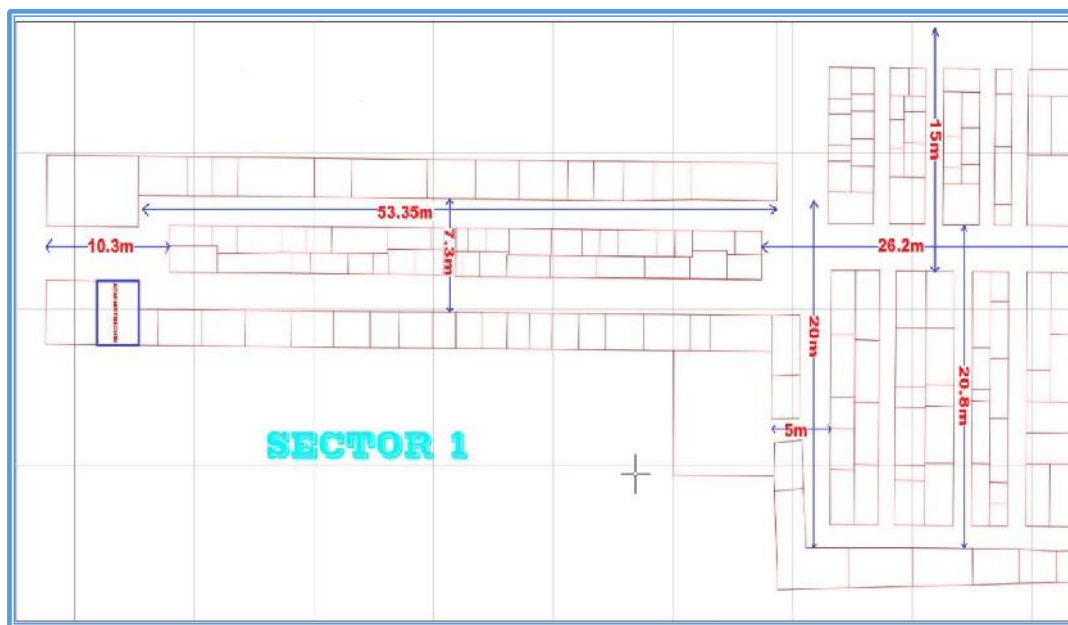


Figura 50. Primer Sector: Medidas de referencia para la colocación de las cámaras IP.

Fuente: [AutoCad]

En este primer sector, se señala las medidas tomadas con respecto a la colocación de las cámaras IP en los pasadizos. Como es sabido, a cada cámara se le asignará una distancia fija para cubrir, por lo tanto estas medidas sirven de referencia para un análisis particular de las cámaras IP distribuidas en cada sector; en conjunto no solo se tendrá cubierto cada sector, sino también se complementará la visión de las imágenes captadas, evitando haya zonas muertas y reforzando eventos con imágenes desde otro sector o ángulo.

En el primer sector se encuentra encerrado de color azul, el área de administración. Es en el área de administración donde se instalará la unidad de



control de acceso, teniendo en cuenta que ahí se realizara el monitoreo y estarán ubicados los equipos que conforman el sistema de videovigilancia IP.

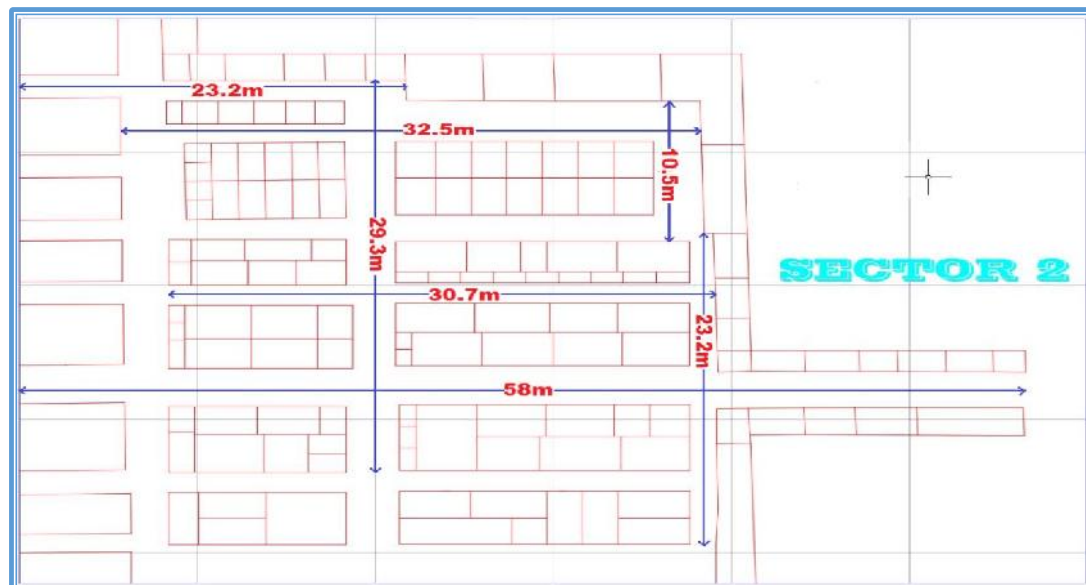


Figura 51. Segundo Sector: Medidas de referencia para la colocación de las cámaras IP.

Fuente: [AutoCad]

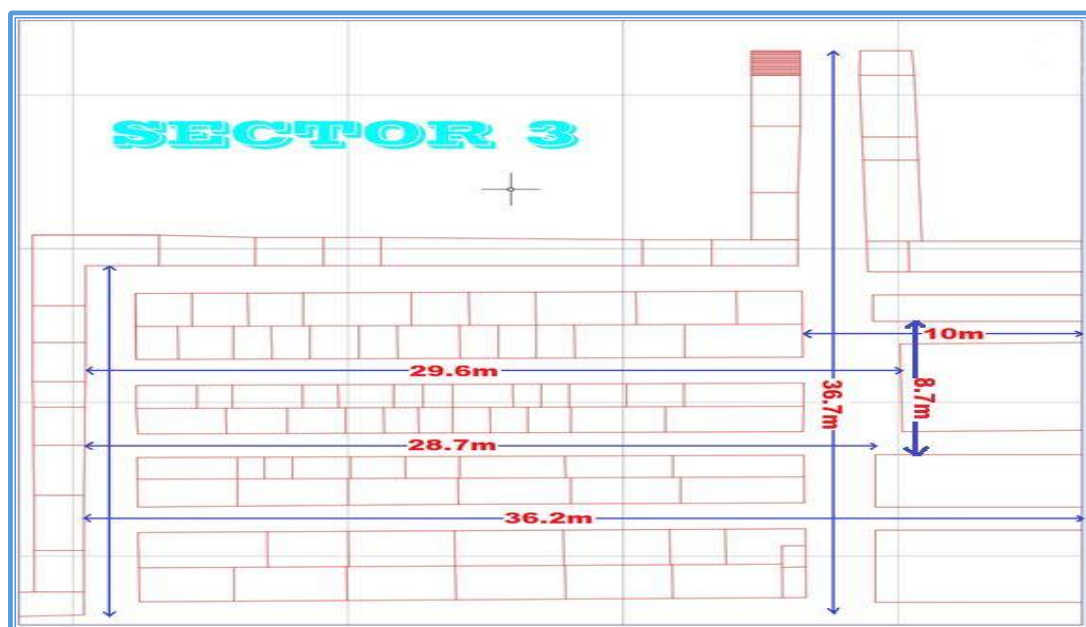


Figura 52. Tercer Sector: Medidas de referencia para la colocación de las cámaras IP.

Fuente: [AutoCad]

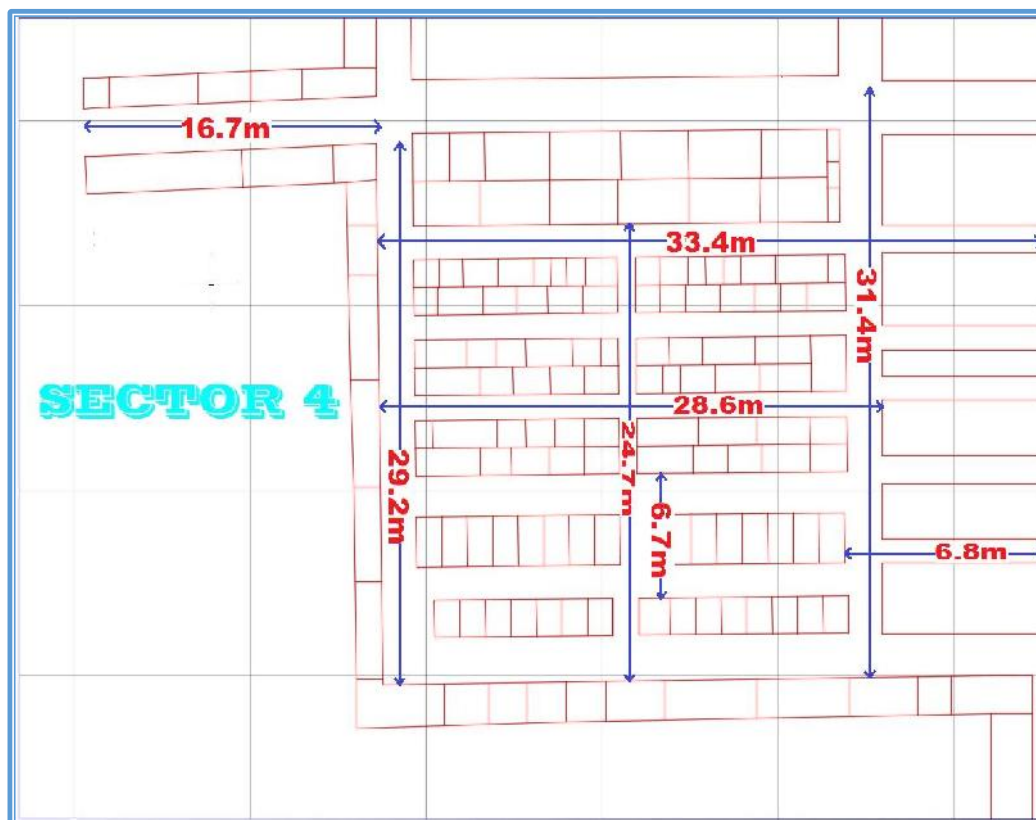


Figura 53. Cuarto Sector: Medidas de referencia para la colocación de las cámaras IP.

Fuente: [AutoCad]

En el sector 3 y 4, existen zonas aisladas de visión, a un costado de los pasadizos. Resulta necesario instalar cámara IP, exclusivas para cubrir estas zonas, ya que a pesar de tener distancias no muy grandes (8.7m en el sector 3 y 6.7m en el sector 4), son zonas que las cámaras IP colocadas en los pasadizos, no son capaces de cubrir.

### 3.5.1.4.2 DISTRIBUCIÓN

Se realizó una distribución adecuada de la cámara IP teniendo en consideración sus características y la estructura de las instalaciones del mercado. Es así que dadas las medidas de referencia antes tomadas, es posible asignar una ubicación adecuada de los equipos y también precisar la cantidad necesaria, para cubrir en conjunto todos los sectores antes graficados.

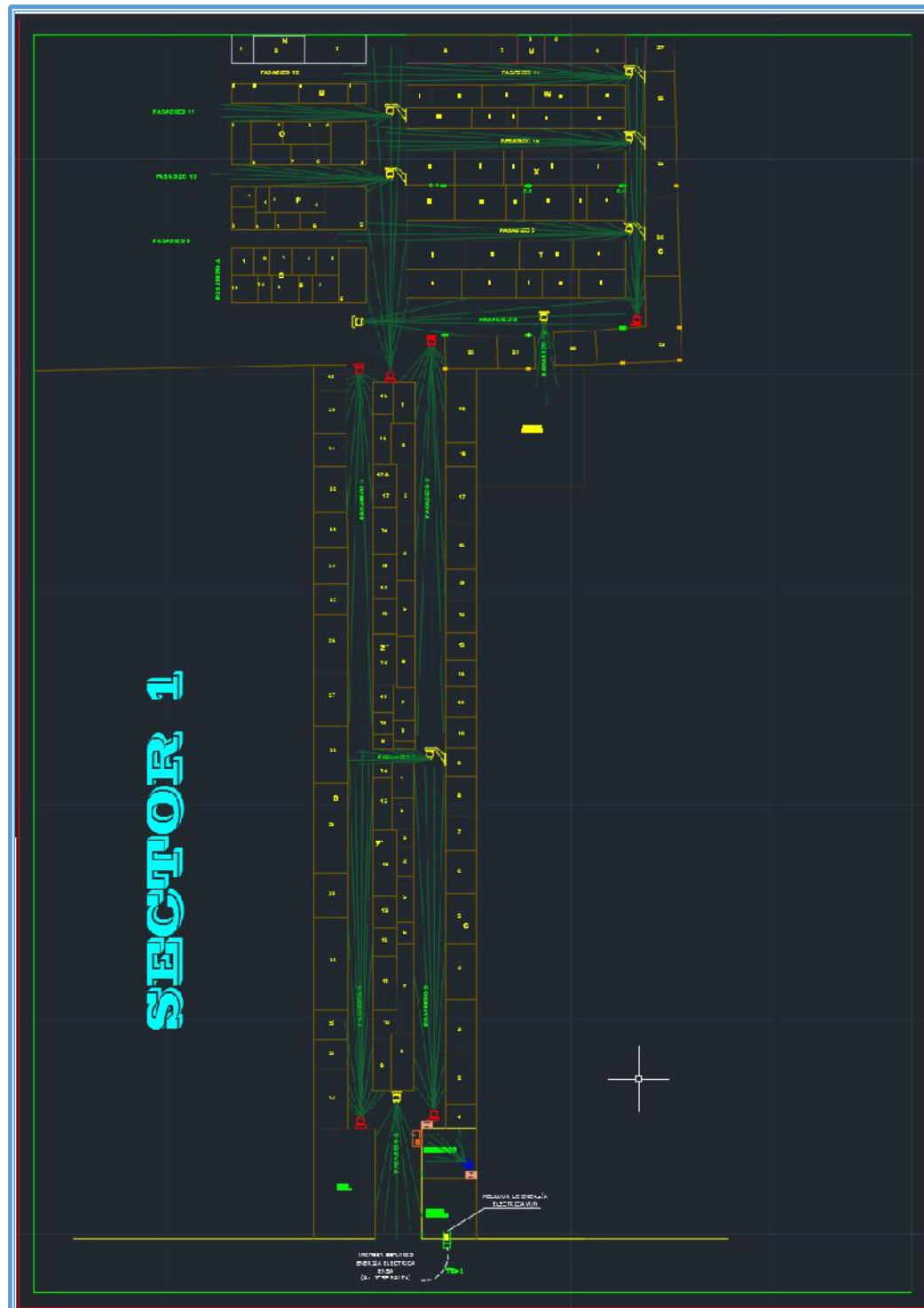
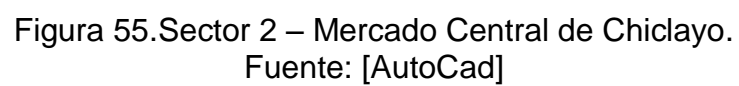


Figura 54.Sector 1 – Mercado Central de Chiclayo.  
Fuente: [AutoCad]





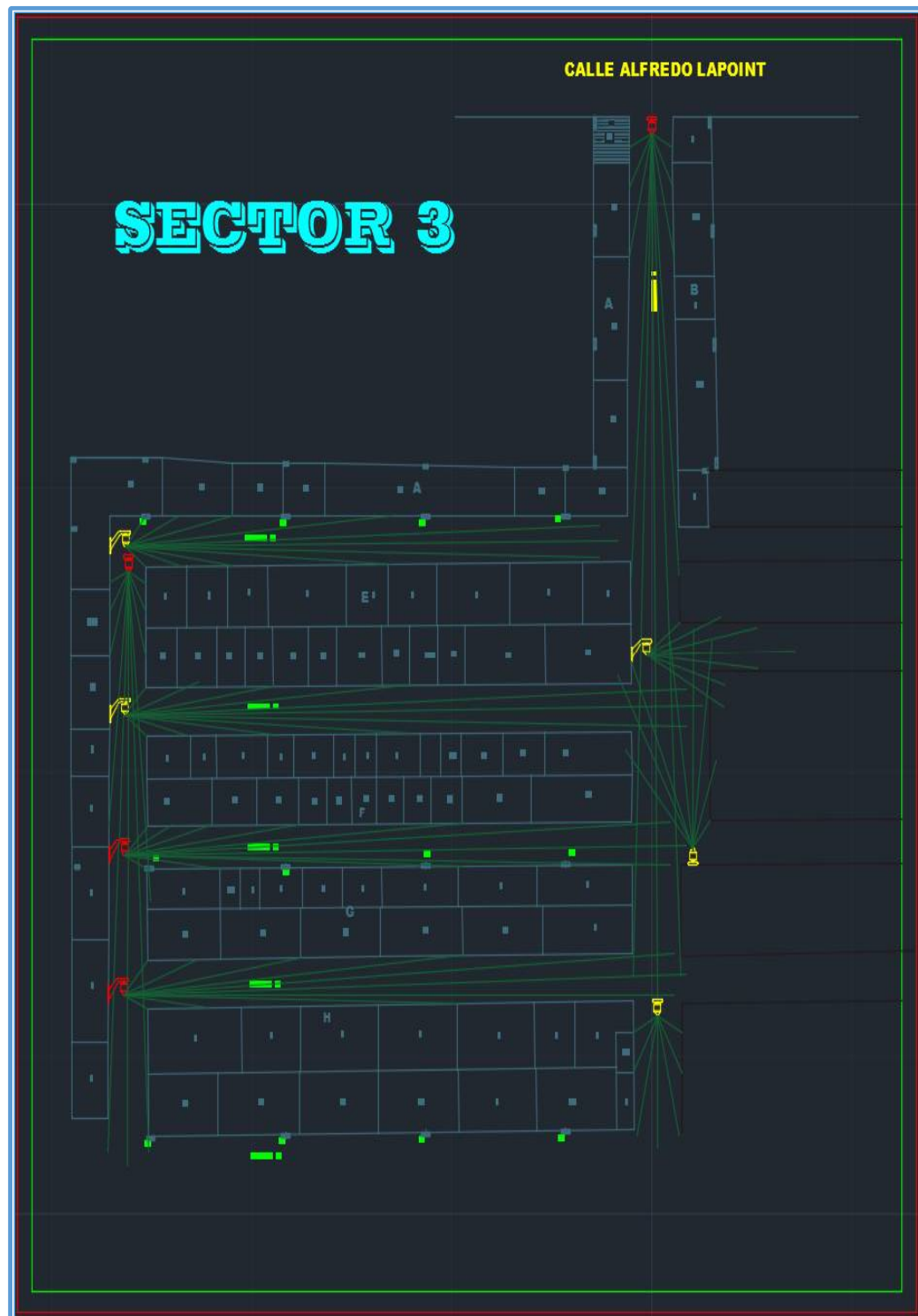


Figura 56.Sector 3 – Mercado Central de Chiclayo.  
Fuente: [AutoCad]



Figura 57. Sector 4 – Mercado Central de Chiclayo.  
Fuente: [AutoCad]

En la distribución se tuvo en cuenta tres tipos de cámaras IP, de acuerdo a las consideraciones de diseño. Dichas cámaras se describirán con detalle posteriormente.

En el sector 1, está ubicada el área de administración, en la que será restringirá el ingreso a personal no autorizado por medio de la unidad de control de acceso, dispuesta en la puerta.

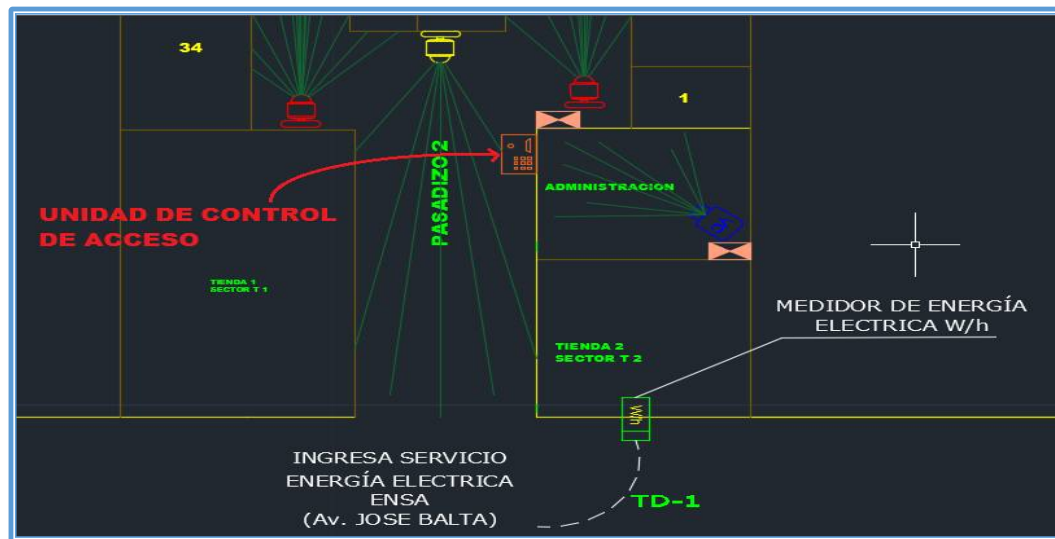


Figura 58. Unidad de control de acceso ubicada en el Sector 1 Administración.

Fuente: [AutoCad]

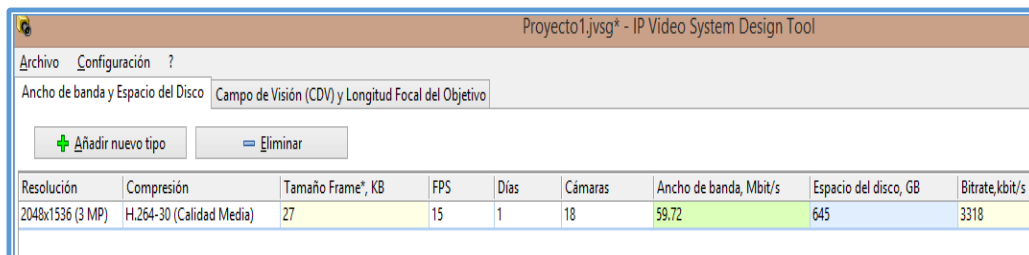
### 3.5.1.5 CÁLCULO DEL ANCHO DE BANDA.

La manera de calcular el ancho de banda, es conociendo el número de cámaras que se van a utilizar para la totalidad del diseño. Como ya sabemos se han tomado en cuenta 3 tipos de cámaras, considerando las condiciones y la distancia que queremos vigilar en los ambientes del mercado central de Chiclayo.

Con la ayuda del software IP Video System Design Tool, es posible calcular de una manera menos complicada el ancho de banda, de acuerdo al número de cámaras que se vaya a utilizar.

- **Cámara HKDS2CD2732 F - I.**

Se utilizarán 18 de este tipo de cámaras, teniendo en cuenta que son para ambientes exteriores. Entonces el ancho de banda se calcula de la siguiente manera:



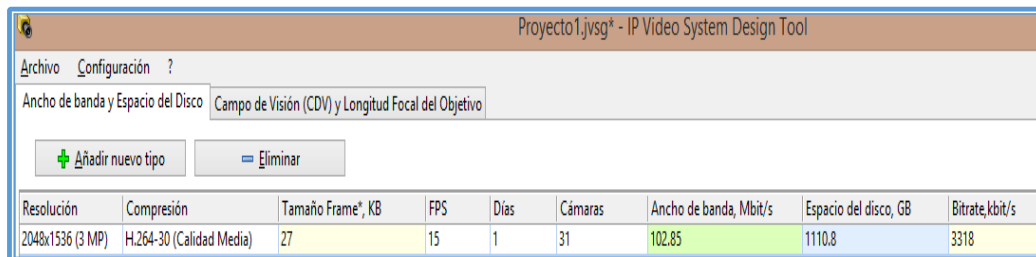
Resolución	Compresión	Tamaño Frame*, KB	FPS	Días	Cámaras	Ancho de banda, Mbit/s	Espacio del disco, GB	Bitrate, kbit/s
2048x1536 (3 MP)	H.264-30 (Calidad Media)	27	15	1	18	59.72	645	3318

Figura 59. Ancho de Banda - HKDS2CD2732 F – I.

Fuente: [IP Video System Design Tool]

- **Cámara HKDS2CD2132 - I.**

En este tipo de cámaras también se usarán un total de 31. Por lo tanto el ancho de banda se calcula así:



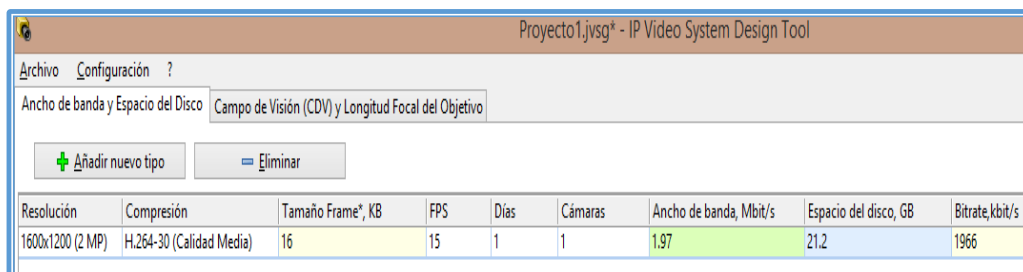
Resolución	Compresión	Tamaño Frame*, KB	FPS	Días	Cámaras	Ancho de banda, Mbit/s	Espacio del disco, GB	Bitrate, kbit/s
2048x1536 (3 MP)	H.264-30 (Calidad Media)	27	15	1	31	102.85	1110.8	3318

Figura 60. Ancho de Banda - HKDS2CD2132 - I.

Fuente: [IP Video System Design Tool]

- **Cámara HKDS2CD8253F - EI.**

Considerando este tipo de cámara, tan solo utilizaremos 1 en total. Entonces se hace el cálculo de la siguiente manera:



Resolución	Compresión	Tamaño Frame*, KB	FPS	Días	Cámaras	Ancho de banda, Mbit/s	Espacio del disco, GB	Bitrate, kbit/s
1600x1200 (2 MP)	H.264-30 (Calidad Media)	16	15	1	1	1.97	21.2	1966

Figura 61. Ancho de Banda - HKDS2CD8253F – EI

Fuente: [IP Video System Design Tool]



Entonces tomando como resultado la suma de la totalidad de las cámaras, el ancho de banda por un día de vigilancia de todas las cámaras que se van a utilizar será 164.54 Mbit/s y sumando la capacidad de almacenamiento, entonces nos resulta 1777 GB, a pesar que el tamaño de almacenamiento es alto, se puede conseguir un servidor de video que nos asegure el almacenamiento de esta información de videovigilancia. Con respecto al ancho de banda, no se considerará el funcionamiento en simultáneo de todas las cámaras, esto debido a que el ancho de banda máximo posible asignado por la compañías que brindan este servicio, es entre 16 a 18 Mbps. Por ello al momento de visualizar las cámaras, tan solo se seleccionarán como máximo 6 cámaras en simultáneo, para ser monitoreadas.

### **3.5.2 ENTORNO DE LA RED.**

En la siguiente gráfica resume el funcionamiento de nuestro sistema de videovigilancia. Las imágenes son captadas por las cámaras IP, esta información viaja desde las cámaras hacia dos patch panel, estos a su vez se interconectan a un switch. Un NVR se conecta al switch, este equipo es el encargado de almacenar la información que es grabada durante el día por las cámaras IP.

Para poder lograr la administración de todas las cámaras IP, se conecta una computadora con un monitor que mediante el software proporcionado por el fabricante de las cámaras, se logrará visualizar el contenido capturado por las cámaras IP en su totalidad.

Por último se tiene un marcador de huella digital, que se conecta al switch, el cual permitirá controlar el acceso al mercado central de Chiclayo, como por ejemplo la entrada y salida del personal que labora en este lugar.

Para que nuestro sistema no tenga inconvenientes con problemas de la ausencia de fluido eléctrico, se necesita conectar a un sistema de alimentación ininterrumpida (UPS), De esta manera se asegura el funcionamiento



ininterrumpido de nuestro sistema, aun cuando se presenten ausencias de energía eléctrica en los ambientes del mercado central de Chiclayo.

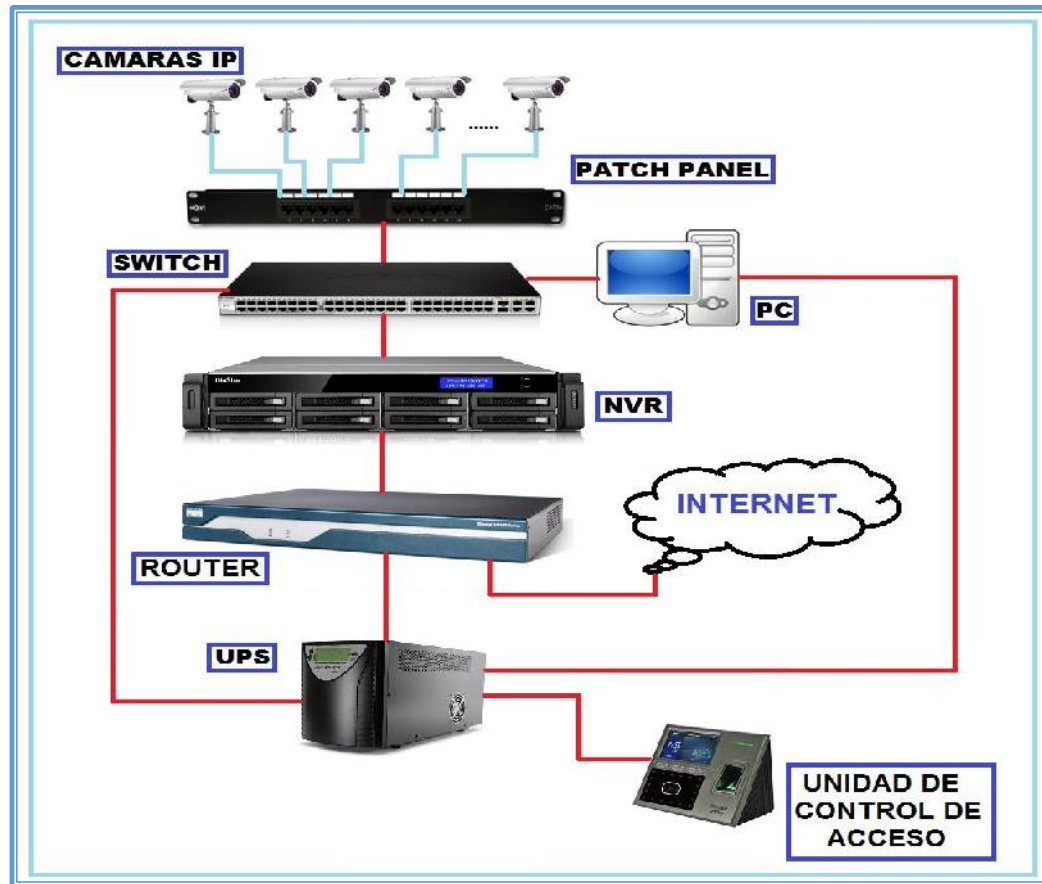


Figura 62.Red del Sistema integrado de Videovigilancia IP y Control de Acceso.

Fuente: [Elaboración Propia]

### 3.5.2.1 CABLEADO

La infraestructura de la red, que conectara las cámaras con el servidor NVR viene dada por cable UTP CAT6 y cable coaxial RG-6, teniendo en consideración la distancia a las que se encuentren ubicadas estas, del servidor.

A continuación se describirá las características de los cables a emplear, así como los conectores y balun (adaptador) adecuados para estos, pudiendo sea posible la transmisión de imágenes de las cámaras.

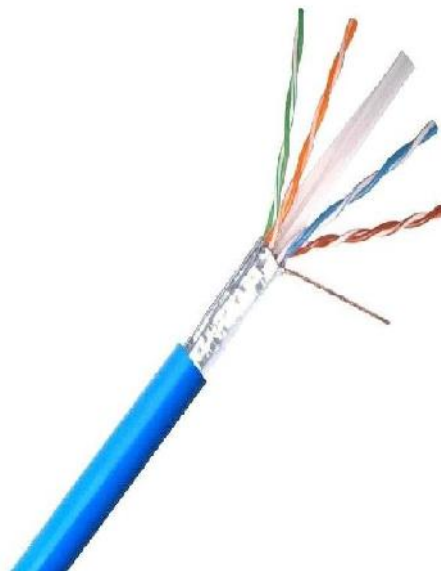
### 3.5.2.1.1 CABLE UTP

Cable de categoría 6, o Cat. 6 (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retrocompatible con los estándares de categoría 5/5e y categoría 3.

Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1Gbps.

Soporta una distancia máxima de 100 metros.

Pin	T568A Par	T568B Par	Cable	T568A Color	T568B Color
1	3	2	tip	Blanco/linea verde	Blanco/linea naranja
2	3	2	ring	Verde	Naranja
3	2	3	tip	Blanco/linea naranja	Blanco/linea verde
4	1	1	ring	Azul	Azul
5	1	1	tip	Blanco/linea azul	Blanco/linea azul
6	2	3	ring	Naranja	Verde
7	4	4	tip	Blanco/linea marrón	Blanco/linea marrón
8	4	4	ring	Marrón	Marrón



UTP CAT-6

Figura 63.Cable UTP Cat. 6.

Fuente: [29]



### 3.5.2.1.2 CONECTOR RJ-45

RJ (Registered Jack) -45, interfaz física usada en los extremos del cable UTP Cat 6, estos se colocaran de manera adecuada de acuerdo a sus 8 pines respecto a los 4 pares del cable UTP.

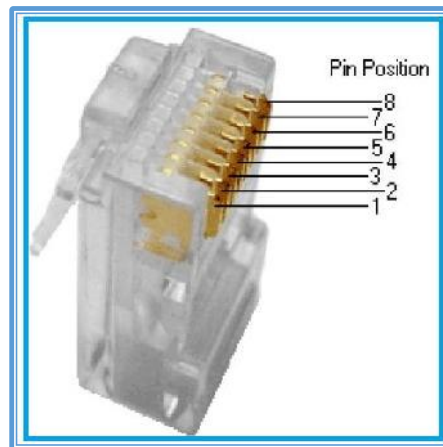


Figura 64. Conector RJ-45.  
Fuente: [29]

### 3.5.2.1.3 CABLE COAXIAL RG-6

Los cables de la serie RG6 son capaces de procesar señales de la más alta resolución y son ideales para aplicaciones exigentes y distancias de cable más largas, incluidas las exigentes aplicaciones SDI/HD-SDI digitales y aplicaciones analógicas de alta definición. Cuando el cableado recorre largas distancias, se pueden producir pérdidas del brillo o nitidez de la imagen o errores de datos en sistemas digitales. Las señales que se transmiten a frecuencias altas son especialmente vulnerables a la pérdida de señal. El cable RG6 es perfecto para largos recorridos porque transporta tanto gráficos de una terminal de alta resolución como vídeo de baja resolución, con una pérdida de señal mínima, garantizando la mejor transmisión de señales de vídeo.

Soporta una distancia máxima de aprox 300 metros. [30]

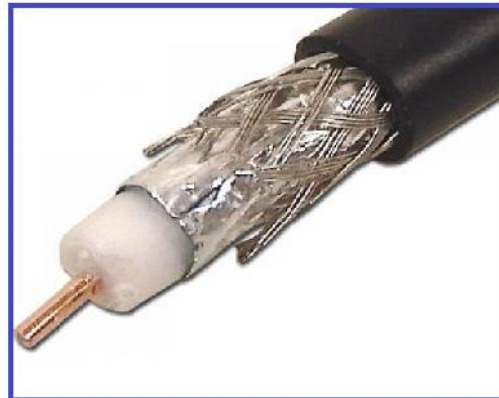


Figura 65. Cable coaxial RG6.  
Fuente: [Telnetron]

#### 3.5.2.1.4 CONECTOR BNC

El conector BNC (Bayonet Neill-Concelman) es un tipo de conector, de rápida conexión/desconexión, utilizado para cable coaxial.

Este conector será el empleado para el cable RG-6, el cual se utilizara para las cámara ubicadas a distancias mayores a 100m, donde es imposible utilizar el UTP, debido a la atenuación producida.



Figura 66. Conector BNC macho.  
Fuente: [31]

### 3.5.2.1.5 PoE ETHERNET EXTENDER SET OVER COAXIAL CABLE (EoC).

Al realizar la distribución de las cámaras IP en el proyecto, nos encontramos con una limitante que es la distancia, la que nos impide realizar nuestro cableado de manera uniforme con cable UTP (cat.6). Dada esta situación, nos lleva a emplear cable coaxial RG-6 como alternativa, permitiendo conectar las cámaras IP encontradas a distancias mayores a 100 metro.

Para la conexión de las cámaras por medio del cable coaxial RG-6, es necesario usar un adaptador para el RJ-45/ BNC, para la conexión del switch POE. En este caso se pensó en un Tx/Rx Mini Power, el que permitira adaptar nuestra conexión del switch hacia un Tx, extenderlo por medio del cable RG-6 y finalmente recibido en un Rx, el cual proporcionara a la cámara IP plena conexión con el switch. Contando el Switch con la tecnología POE, esta también proporcionara de alimentación con el extensor IP, por medio de cable coaxial a cada cámara IP.



Figura 67.Elementos extensores PoE.  
Fuente: [32]

A continuación se muestra la conexión a realizarse con coaxial RG-6 desde el switch empleando los Mini-Power Tx/Rx, hasta la cámara IP.

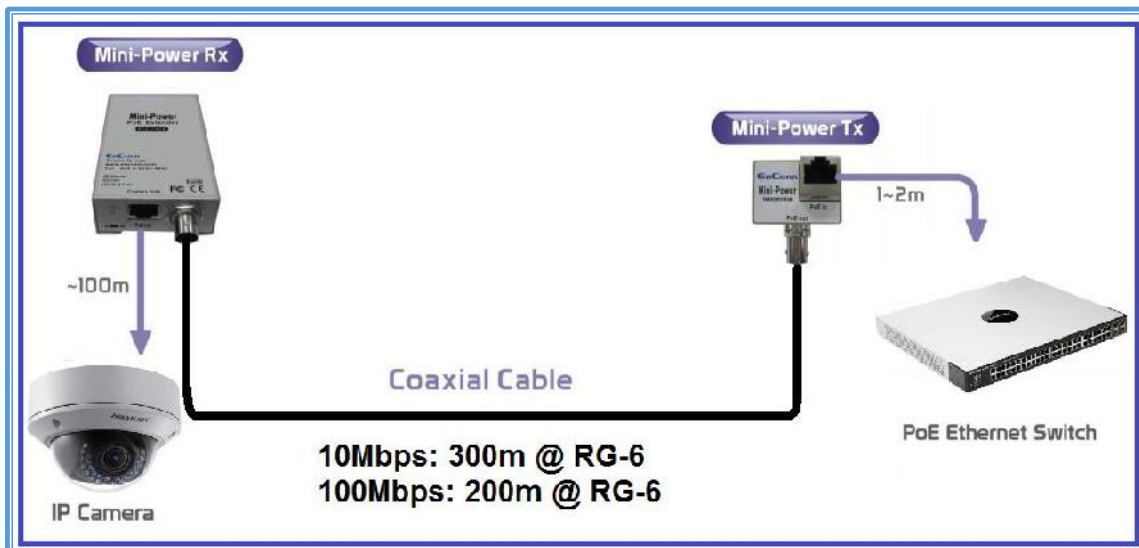


Figura 68. Conexión de los elementos extensores con el RG6.  
Fuente: [Elaboración Propia]

### 3.5.2.2 ELEMENTOS DEL SISTEMA

Para el diseño se han elegido los equipos adecuados, de manera que puedan ser lo más eficientes posible para lograr un buen desempeño de nuestro sistema de videovigilancia.

#### 3.5.2.2.1 CÁMARAS IP.

Se ha optado por elegir tres tipos de cámaras, de la marca HIKVISION, esto basado en sus características, las cuales cumplen los requisitos del diseño como el tipo de compresión de video H.264 y MJPEG, tipo de sensor en este caso CMOS, y la alimentación PoE. Sus especificaciones y características más resaltantes, se detallan a continuación



❖ **HK-DS2CD2132-I**

DOMO IR IP. CMOS 1/3"Progressive Scan.Full HD 3Mp. D-WDR. 3D DNR.  
PoE. Slot SD. IP66

- Domo fijo exterior 3Mp, video full HD 1080p.
- Resolución: 15fps (2048\*1536), 30fps (2048\*1536).
- Iluminación: Color: 0.07 lux@F1.2/0 lux con IR On.
- Lente (M12)2.8mm@F2.0, Ángulo de visión: 92°.
- Disparador electrónico: 1/30s a 1/100 000s.
- Función día/noche verdadero con ICR, BLC.
- Reducción de ruido digital 3D DNR, digital WDR.
- Compresión de video: H264/MJPEG.
- Dual stream de video. Nivel de protección IP66.
- Respaldo local: slot micro SD/SDHC/SDXC, hasta 64GB.
- Interface de RED: 1 puerto RJ45 10M/100M.
- Anti vandálico: IEC60068-275Eh, 50J; EN50102, hasta 1K10.
- Alimentación: 12 VDC+-10%, PoE (802.3af)
- Consumo: Max.5.5W.Rango IR hasta 20m.
- Temperatura: 30°C-60°C. Peso: 1Kg.
- Dimensiones: 140\*99.9mm.



Figura 69. Cámara IP HIKVISION.  
Fuente: [Catálogo HIKVISION 2014]

#### ❖ HK-DS2CD8253F-EI

- Cámara tipo tubo IR, verdadero Día/Noche.
- Resolución: 2 Megapíxel (1600\*1200).Tiempo real HD720p.
- Chip CMOS 1/3" Escaneo progresivo.
- Lente A/I 2.7-9mm@F1.2, ángulo de visión 101°-30.4°.
- Iluminación 0.5 lux@F1.2, AGC on, 0.1lux@F1.2,AGC on.
- Alcance de visión nocturna: 20-30m.
- Velocidad de transmisión 60Hz:15fps (1600\*1200), 15fps (1600\*912), 25fps (1280\*960), 30fps (1280\*720).
- Interface WEB (IE).
- Compresión H. 264/ MPEG 4/ MJPEG.
- Soporta dual stream.
- Power over ethernet (PoE) 802.3af.
- Protocolo TCP/IP, HTTP, RTP, DDNS.

- Compatible: ONVIF, PSIA, CGI.
- Alimentación 12VDC+-10%, PoE (802.3af).
- Consumo máximo 9.5W.
- Temperatura de operación: 10°C A 60°C.
- Nivel de protección: IP66.
- Dimensiones 98\*88.58\*328.79mm.
- Incluye lente, soporte y fuente.



Figura 70. Cámara IP HIKVISION.  
Fuente: [Catálogo HIKVISION 2014]

#### ❖ HK-DS2CD2732F-I

Domo "IR" IP-CMOS 1/3" Progressive Scan – Full HD 3Mp – D-WDR – 3D DNR – PoE – Slot SD – IP66

- Cámara exterior 3Mp, video full HD 1080 p.
- Resolución: 15 fps (2048\*1536), 30 fps (1920\*1080).
- Iluminación: Color: 0.07 lux@F1.2/0 lux con IR On.
- Lente (M14) varifocal 2.8mm-12 mm@F1.4, Ángulo de visión: 98°-30.5°.
- Disparador electrónico: 1/25s a 1/100 000s.



- Función día/noche verdadero con ICR, BLC.
- Reducción de ruido digital 3D DNR, digital WDR.
- Compresión de video: H264/MJPEG.
- Dual stream de video. Nivel de protección IP66.
- Respaldo local: slot micro SD/SDHC/SDXC, hasta 64GB.
- Interface de RED: 1 puerto RJ45 10M/100M.
- Anti vandálico: IEC60068-275Eh, 50J; EN50102, hasta 1K10.
- Alimentación: 12 VDC+-10%, PoE (802.3af)
- Consumo: Max.5.5W.Rango IR hasta 20m.
- Temperatura: 30°C-60°C. Peso: 1Kg.
- Dimensiones: 140\*99.9mm.



Figura 71.Cámara IP HIKVISION.  
Fuente: [Catálogo HIKVISION 2014]

### 3.5.2.2.2 GRABADORA DE VIDEO (NVR).

Para seleccionar este equipo, es necesario y como característica principal que cumpla con la capacidad de almacenamiento calculada que es 1777 GB, según su capacidad se puede almacenar 24 TB, también se puede conectar hasta 32

cámaras IP, cuenta con salida VGA, para la visualización local en HD. La grabación que se puede obtener de este equipo es de alta calidad, en comparación con otros equipos.

Se detalla sus características más importantes:

❖ **QN-VS-8132U-RP PRO.**

- Servidor de video para 32 cámaras IP.
- 8 bahías para discos duros. Capacidad total de 24TB.
- Procesador Dual-Core Intel. Core i3-2120,3.3GHz, RAM 2GB DDR3.Dual Puertos Gigabit LAN.
- Salida VGA para visualización local HD.
- Grabación megapíxel de alta calidad. Soporta Raid.
- Fuente de alimentación redundante. Chasis 2U.
- Nivel de consumo máximo en la red: 360 Mbps.
- Dimensiones: 88(H)\*439(W)\*520(D) mm.
- Peso: 20.76Kg.
- Consumo 130Watts.



Figura 72. NVR QNAP.  
Fuente: [Catálogo HIKVISION 2014]



### 3.5.2.2.3 UNIDAD DE ACCESO POR HUELLA DIGITAL.

Debido que en nuestro diseño, solo necesitamos controlar el registro de entrada y salida del personal, es que se eligió este equipo que tiene una capacidad de registrar hasta 3000 huellas digitales, y soportar hasta 100000 registros.

Cuenta con batería de respaldo, para que se pueda trasladar de un lugar a otro sin necesidad de estar conectado siempre a fluido eléctrico. El tipo de comunicación que se usa es el puerto USB, para poder conectarlo a una computadora y así poder descargar y visualizar los registros que contiene almacenado este lector digital.

Se detallan algunas de sus principales características:

#### ❖ ZK-IN01A/ID.

- Control de acceso y asistencia biométrico: Huella digital + Lector RF +Clave.
- Pantalla color TFT 3", soporta 3000 huellas.
- Soporta 100000 registros
- Plataforma de hardware ZEM510.
- Comunicación RS232/485, TCP-IP, USB-Cliente, USB-Host.
- Soporta batería de respaldo.
- Funciones estándar: Código de trabajo, mensajes cortos (SMS), cambio de horario de verano (DLST), consulta de registros de asistencia en pantalla.
- Soporta multilinguaje.
- Salida de relevador NO/NC.

- Comunicación Wiegand Entrada/Salida.
- Alimentación 12VDC. Consumo de corriente 3 A.
- Dimensiones 210\*157\*50 mm.



Figura 73. Unidad de Control de Acceso ZKSoftware.  
Fuente: [Catálogo HIKVISION 2014]

#### 3.5.2.2.4 COMPUTADORA

##### ❖ ADVANCE VISSION VS 5059

Se elige una computadora para conectarla a nuestro sistema de Videovigilancia IP, así poder configurar y administrar a través del software que nos permita acceder a las cámaras IP. Las especificaciones de esta computadora son las siguientes:

- Procesador Intel Core i3-3240 3.40GHz
- Disco duro 4GB DDR3, 500GB SATA.
- Tarjeta de video NVIDIA GeForce GT610 1GB DDR3 64-bit
- Puerto de red LAN GbE.
- Accesorios teclado y mouse.

- Sistema Operativo Windows 8 SL 64-bit en español.
- Voltaje de alimentación 110/220 VAC.
- Potencia de la fuente 275 Watts.



Figura 74. Computadora Core i3 ADVANCE  
Fuente: [33]

### 3.5.2.2.5 MONITOR PARA VISUALIZACIÓN DE LAS CÁMARAS.

#### ❖ SAMSUNG LS27D590CS 27 PULGADAS.

Es importante el elegir un monitor de gran tamaño, debido a que esto genera una mejor visualización de los sucesos que graben las cámaras IP instaladas en nuestro sistema de videovigilancia.

Presentamos las características de este equipo a continuación:



## Pantalla

- Tamaño de pantalla 27 pulgadas.
- Relación de aspecto 16: 9.
- Tipo de panel VA (curvo).
- Tipo BLU LED.
- Brillo (típico) 350 cd/m2.
- Relación de contraste 3000: 1.
- Relación de contraste dinámico Mega DCR.
- Resolución 1920 x 1080.
- Tiempo de respuesta 4 (GTG) ms.
- Ángulo de visión (H / V) 178° / 178°.
- Soporte de color 16.7 M.
- Características generales.
- Funciones integradas.
- Modo de juego, Magic Upscale, Ahorro ecológico, Temporizador de apagado, Tamaño de imagen, Samsung MagicBright, Flicker Free.
- Software adicional para PC.
- Cuadro de configuración fácil.
- Compatibilidad con sistemas operativos.
- Windows, Mac.
- Certificación de Windows.
- Windows 8.1.



### **Diseño**

- Color Negro de alto brillo.
- Tipo de soporte Forma curva en T.
- Inclinación  $-2^{\circ}$  a  $+20^{\circ}$ .
- Montaje para pared 100 x 100.

### **Eco**

- Calificación energética / medioambiental Energy Star 6.0.
- Energía.
- Fuente de alimentación CA 100 - 240 V (50 / 60 Hz).
- Consumo de energía 24 (condiciones de prueba actuales de Energy Star).
- Consumo de energía (DPMS) 0.3 W.
- Consumo de energía (en espera) 0.3 W.
- Tipo Adaptador externo.

### **Dimensiones**

- Dimensiones del equipo con soporte (ancho x alto x prof.).
- 62.35 x 46.3 x 18.2 cm.
- Dimensiones del equipo sin soporte (ancho x alto x prof.).
- 62.35 x 36.6 x 5.95 cm.
- Dimensiones del paquete (ancho x alto x prof.).
- 69.5 x 13.5 x 43.5 cm.
- Peso.
- Peso del equipo con soporte 5.6 kg.



- Peso del equipo sin soporte 5 kg.
- Peso del paquete 7.4 kg.

### Accesorios

- Cables Cable HDMI, Cable de audio.



Figura 75. Monitor SANSUNG.  
Fuente: [SANSUNG PERU]

### 3.5.2.2.5.1 UPS (SISTEMA DE ALIMENTACION ININTERRUMPIDA)

Es necesario elegir un UPS, que pueda adecuarse a la potencia total consumida por nuestro sistema de videovigilancia, para ello primero tenemos que calcular la potencia de cada uno de los equipos a utilizar en nuestro diseño.

EQUIPO	CONSUMO EN WATTS / H	CANTIDAD	TOTAL DE CONSUMO EN WATTS / H
Conmutador HP 1920-24G-PoE+	180 W/h	3	540 W/h
Router 5 port GIGA ETHERNET	6 W/h	1	6 W/h
Computadora Advance Vission VS5059	275 W/h	1	275 W/h
QN-VS-8132U-RP PRO. (NVR)	130 W/h	2	260 W/h
ZK-IN01A/ID (Lector de huellas)	36 W/h	1	36 W/h
Monitor de 27 pulgadas	0.3 W/h	2	0.6 W/h
		CONSUMO TOTAL EN WATTS / H	1117.6 W/h

Tabla 7. Consumo eléctrico de los elementos del Sistema.  
Fuente: [Elaboración Propia]



Según el cálculo del consumo de potencia de nuestro sistema de videovigilancia, es de 1117.6 Watts / H. Es necesario utilizar un UPS que tenga una potencia superior a la potencia calculada, esto es necesario para que al momento de empezar a funcionar, por alguna falla en el suministro eléctrico, la potencia que consuma el sistema de videovigilancia sea la adecuada, y que nuestro UPS brinde la seguridad que nuestro sistema siga en funcionamiento.

Se elige un UPS de la marca APC, que cuenta con 2700 Watts de potencia, lo suficiente para nuestro sistema. Su entrada de voltaje es de 230 Voltios, ideal para el suministro eléctrico en nuestro país. A continuación detallamos sus características más importantes.

#### ❖ **APC Smart-UPS 3000VA USB & Serial RM 2U 230V**

##### **Salida**

- Capacidad de Potencia de Salida 2700 Vatios / 3000 VA
- Máxima potencia configurable 2700 Vatios / 3000 VA
- Tensión de salida nominal 230V
- Frecuencia de salida (sincronizada a red eléctrica principal) 47 - 53 Hz para 50 Hz nominal, 57 - 63 Hz para 60 Hz nominal
- Tipo de forma de onda Onda senoidal
- Conexiones de salida

(8) IEC 320 C13



(1) IEC 320 C19



(2) IEC Jumpers

### Entrada

- Entrada de voltaje 230V.
- Frecuencia de entrada 50/60 Hz +/- 3 Hz (autosensible).
- Variación de tensión de entrada para operaciones principales 160 - 286V.
- Variación de tensión de entrada adaptable para operaciones principales 151 - 302V.

### Baterías y autonomía

- Tipo de batería: Batería sellada de plomo sin necesidad de mantención con electrolito suspendido: a prueba de filtración.
- Tiempo típico de recarga 3 hora(s).



Figura 76. Sistema de alimentación ininterrumpida.  
Fuente: [APC by Schneider Electric]

### 3.5.2.2.6 ROUTER

Este equipo nos sirve para tener acceso a nuestro sistema de videovigilancia IP, en cualquier lugar donde nos encontremos, mediante el acceso a Internet.

El RB450G es un router Gigabit Ethernet de cinco puertos. En comparación con el RB450, el RB450G no sólo añade capacidad de velocidad Gigabit, sino también 256Mb de RAM, una CPU más rápida y una ranura para tarjetas microSD para el almacenamiento de archivos.

El dispositivo es alimentado por una rápida CPU 680MHz Atheros AR7161, y también incluye un monitor de sensor de temperatura y voltaje.

RB450G incluye RouterOS - el sistema operativo, lo que a su vez, este sistema de gran alcance en un router, firewall o ancho de banda gerente altamente sofisticado.

Las características incluyen:

- CPU Atheros AR7161 de 680 MHz.
- 256 MB de memoria interna DDR SDRAM.
- A bordo de chip de memoria NAND de 64MB.
- Cinco puertos independientes de Ethernet 10/100 con chip de conmutación.
- Alimentación, actividad NAND, 5 LEDs Ethernet.
- MikroTik RouterOS licencia Level 5.
- Consumo de potencia: 6 watts.
- Temperatura de operación: -20 a 50 °C.
- Voltaje de alimentación: 8- 28 voltios.
- Botón de reset.

### Características:

- Pequeño y compacto.
- Caja de plástico blanca.
- Cinco puertos gigabit.
- Increíblemente rápida.
- Precio más bajo.



Figura 77. 5PORT GIGA ETHERNET.  
Fuente: [MIKROTIK PERU]

### 3.5.2.2.7 CONMUTADOR

#### ❖ HP 1920-24G-PoE+

Para la conexión y alimentación de nuestras cámaras IP, usaremos este tipo de switch, consideramos para el diseño 3 switch de 24 puertos, debido a que el número de cámaras es de 50.

### Características

La serie de conmutadores HP 1920, ideal para organizaciones pequeñas, ofrece una implementación plug-and-play fácil y lista para usar.



La serie ofrece una gama completa de opciones para una mayor flexibilidad. Consta de nueve modelos de montaje en bastidor con fuentes de alimentación internas, incluyendo cuatro sin consumo de energía en comparación con modelos Ethernet (PoE): puerto de 8 G, 16 G, 24 G y 48 G; cinco modelos PoE+: puerto de 8 G (2), 24 G (2) y 48 G.

Estos conmutadores de gestión inteligente utilizan una interfaz de gestión de Web intuitiva, basada en nuestra serie de conmutadores HP 1910 líder del sector, para simplificar la implementación y la gestión al tiempo que le ofrece una mayor granularidad de control de las funciones clave.

### **Especificaciones.**

- Puertos de entrada y salida: 24 RJ-45 10/100/1000 con conexión automática PoE + puertos (IEEE 802.3 tipo 10Base-T, IEEE 802.3u tipo 100BASE-TX, IEEE Tipo 802.3ab 1000BASE-T, IEEE 802.3af PoE, IEEE 802.3at) 4 puertos SFP 1000 Mbps. Admite un máximo de 24 autosensados puertos 10/100/1000 más 4 puertos 1000BASE-X.
- Procesador y memoria: MIPS @ 500 MHz, 32 MB de flash, 128 MB SDRAM; tamaño de búfer de paquetes 4,1 Mb.
- Temperatura de operación: 0 a 40 °C.
- Frecuencia eléctrica: 50/60 Hz.
- Voltaje AC: 100-240 VAC.
- Potencia PoE: 180 Watts.





Figura 78. Conmutador HP.  
Fuente: [HP Networking]

## 4 CAPITULO 4

### PRESUPUESTO

En esta sección detallamos cada uno de los elementos a utilizar en el diseño, la elección de estos elementos ya se ha detallado en los capítulos anteriores. Se ha elegido las marcas de cada equipo, de acuerdo a las necesidades de nuestro diseño.

En las siguientes tablas se detalla la cantidad de elementos, su precio respectivo para tomar en cuenta al momento del diseño.

EQUIPO	MODELO	MARCA	CANTIDAD
Cámara IP	HK-DS2CD2132-I	HIKVISION	31 und
Cámara IP	HK-DS2CD8253F-EI	HIKVISION	1 und
Cámara IP	HK-DS2CD2732F-I	HIKVISION	18 und
NVR	QN-VS-8132U-RP PRO	QNAP	2 und
Lector de Huellas	ZK-IN01A/ID	ZKSOFTWARE	1 und
UPS	APC Smart 3000VA	Schneider Electric	1 und
ROUTER	ROUTER 5 port GIGA ETHERNET	MIKROTIK	1 und
Switch	Conmutador HP 1920-24G- PoE+	NETWORKING	3 und
Computadora	Computadora ADVANCE VISSION Vs5059	ADVANCE	1 und
Monitor	Sansung de 27 pulgadas	SANSUNG	2 und

Cable UTP	Rollos de 100 metros	Lancom	3 rollos
Cable Coaxial	Rollos de 100 metros	Telnetron	3 rollos
Extensores PoE	Mini - Power	Enconn	150 und
Conectores	RJ45	Taiwanés	200 und
Conectores	BNC RG6 macho	Taiwanés	50 und
<b>DUCTERIA</b>			
Tubo	Acero Galvanizado 2"	CONDUIT	56 varillas x 6m
Tubo	Acero Galvanizado 1"	CONDUIT	5 varillas x 6m
Codo	Acero Galvanizado 2"	CONDUIT	7 und
T	Acero Galvanizado 2"	CONDUIT	7 und
Codo	Acero Galvanizado 1"	CONDUIT	3 und
T	Acero Galvanizado 1"	CONDUIT	2 und
<b>FERRETERÍA</b>			
Abrazaderas	Acero inoxidable	MetalPeru	80 und
Soporte para cámara domo	Metal	HIKVISION	49 und
Soporte para cámara interior	Metal	HIKVISION	1 und
Caja de paso 100x100mm	Metal	CONDUIT	41 und

Tabla 8. Modelo, cantidad de equipos y materiales a utilizar.  
Fuente: [Elaboración Propia]



EQUIPO	MODELO	PRECIO UNITARIO	CANTIDAD	PRECIO TOTAL
Cámara IP	HK-DS2C D2132-I	S/. 547.81	31 und	S/. 16,982.11
Cámara IP	HK-DS2C D8253F-EI	S/. 967.53	1 und	S/. 967.53
Cámara IP	HK-DS2C D2732F-I	S/. 331.25	18 und	S/. 5,962.50
NVR	QN-VS-8132U -RP PRO	S/. 4,373.75	2 und	S/. 8,747.50
Lector de Huellas	ZK-IN01A/ID	S/. 224.75	1 und	S/. 224.75
UPS	APC Smart 3000VA	S/. 3,645.60	1 und	S/. 3,645.60
ROUTER	ROUTER 5 port GIGA ETHERNET	S/. 104.16	1 und	S/. 104.16
Switch	Conmutador HP 1920-24G- PoE+	S/. 1,637.60	3 und	S/. 4,912.80
CPU	Cumputadora Advance Vission Vs 5059	S/. 1,716.43	1 und	S/. 1,716.43
Monitor	Sansung de 27 pulgadas	S/. 1,715.62	2 und	S/. 3,431.24
Cable UTP	Rollos de 100 metros	S/. 210	3 rollos	S/. 630.00
Cable Coaxial	Rollos de 100 metros	S/. 130	3 rollos	S/. 390.00
Extensores PoE	Mini - Power	S/. 100	30 und	S/. 3,000.00
Conectores	RJ45	S/.78.9(por 100 unidades)	200 und	S/. 157.80
Conectores	BNC RG6 macho	S/. 125 (por 50 unidades)	50 und	S/. 125.00

DUCTERIA				
Tubo	Acero Galvanizado 2"	S/. 66.50	56 varillas x 6m	S/. 3,724.00
Tubo	Acero Galvanizado 1"	S/. 34.00	5 varillas x 6m	S/. 170.00
Codo	Acero Galvanizado 2"	S/. 10.00	7 und	S/. 70.00
T	Acero Galvanizado 2"	S/. 22.00	7 und	S/. 154.00
Codo	Acero Galvanizado 1"	S/. 6.50	3 und	S/. 19.50
T	Acero Galvanizado 1"	S/. 12.50	2 und	S/. 25.00
FERRETERÍA				
Abrazaderas	Acero inoxidable	S/. 5.00	80 und	S/. 400.00
Soporte para camara domo	Metal	S/. 45.00	49 und	S/. 2,205.00
Soporte para camara interior	Metal	S/. 35.50	1 und	S/. 35.50
Caja de paso	Metal	S/. 16.25	41 und	S/. 666.25
<b>TOTAL</b>				<b>S/. 58,466.67</b>

Tabla 9. Precio de equipos y accesorios a utilizar (incluyen IGV).  
Fuente: [Elaboración Propia]

## 5 CAPITULO 5

# CONCLUSIONES Y RECOMENDACIONES.

### 5.1 CONCLUSIONES

1. Se logra diseñar un sistema de video vigilancia IP, para brindar seguridad y monitoreo a las instalaciones del mercado central de Chiclayo. El desarrollo del diseño, hizo necesario contar con cincuenta cámaras IP, distribuidas en los sectores del mercado, de esta manera se pudo cubrir todo el establecimiento, garantizando una buena cobertura, transmisión y recepción de la información.
2. Para el caso del almacenamiento de la información, nos ha resultado que el servidor de video (NVR) elegido, es el más óptimo, debido a su capacidad de almacenamiento de 24 TB, lo cual es de suma importancia al examinar posteriormente las imágenes captadas por el sistema de video vigilancia, ante cualquier eventualidad.
3. Se corrobora que con la ayuda del software de simulación IP Video System 8, se puede lograr un diseño más preciso, sin la necesidad de tener que realizar muchos cálculos y así obtener de manera inmediata los parámetros, tales como, el ancho de banda y la capacidad de almacenamiento del sistema de video vigilancia.
4. Se localizó el área donde se requiere se instale la unidad control de acceso. Disponiendo del área de administración, como centro de monitoreo y donde se ubicaran los elementos del sistema de Videovigilancia IP; es el ingreso al área de administración la que se restringirá con la unidad de control de personal a través de la huella digital.



5. Con los equipos propuestos en este tema de estudio, utilizando una red ampliamente difundida, se logra la implementación de un sistema moderno y factible de ser monitoreado a distancia. Es decir, se garantiza un medio de acceso seguro y los equipos pueden ser maniobrados y configurados desde cualquier parte del mundo, teniendo la autorización de la empresa.

## 5.2 RECOMENDACIONES.

1. Debido a que nuestro diseño está basado en una red IP, nos resulta factible para futuro el poder integrar al servicio de video vigilancia, otras aplicaciones como transmisión de datos, transmisión de voz sin alterar la infraestructura ya diseñada de manera previa, convergiendo en un data center.
2. Para una buena calidad de la imagen en la monitorización del sistema, resulta importante se cuente con equipos en óptimas condiciones. Frente a esto es necesario se realice un mantenimiento periódico del sistema.
3. Si se piensa adicionar más elementos al sistema, es preciso se realice las pruebas respectivas de tráfico de datos, así comprobar que el sistema cuenta con el adecuado ancho de banda, para el tráfico de imágenes captadas por las cámaras en conjunto. Estas pruebas evitara haya pérdida de imagen en ciertas cámaras o en el peor de los casos haya una congestión y como resultado el sistema quede inhabilitado.





## 6 CAPITULO 6

### FUENTES DE REFERENCIA

- [1] “Galeón: Material de Redes de Datos”, disponible por WWW en  
<http://www.redesdedatosinfo.galeon.com/enlaces2128619.html>
- [2] Bruce A. Hallberg, Traducción: Carlos Roberto Cordero Pedraza.  
“Fundamentos de Redes – Cuarta edición”. McGRAW-  
HILL/INTERAMERICANA EDITORES, S.A. DE C.V, México, 2007.
- [3] “Redes Cisco/ coordinado por Daniel Benchimol – Primera edición”. Manual  
USERS/GRANDI S.A., Argentina, 2010.
- [4] Vázquez, P. G., Baeza, J. P., & Herías, F. A. C. “Redes y transmisión de  
datos”. Publicación de la Universidad de Alicante. España, 2010.
- [5] Claudio Alejandro Peña Millahual. “Redes – Primera edición”. Manual  
USERS.Fox Andina S.A/DALAGA S.A., Argentina, 2012.
- [6] “Cable UTP”, disponible por WWW en  
<http://cableutpnubiaardila.blogspot.com/>
- [7] “Tipos de cables UTP”, disponible por WWW en  
[http://www.ehowenespanol.com/tipos-cables-utp-lista\\_85429/](http://www.ehowenespanol.com/tipos-cables-utp-lista_85429/)



**[8]** “Elementos de transmisión para seguridad electrónica”, disponible por WWW

en: [http://www.rnds.com.ar/articulos/038/rnds\\_116w.pdf](http://www.rnds.com.ar/articulos/038/rnds_116w.pdf)

**[9]** “Cables Coaxiales”, disponible por WWW en:

[http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes\\_1/cabc\\_oax.htm](http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/cabc_oax.htm)

**[10]** “Cables y Conectores”, disponible por WWW en:

<http://www.angelfire.com/wi/ociosonet/15.html>

**[11]** “Ventajas del sistema de Videovigilancia IP”, disponible por WWW en

[http://www.axis.com/es/products/video/about\\_networkvideo/digital\\_benefits.htm](http://www.axis.com/es/products/video/about_networkvideo/digital_benefits.htm)

**[12]** “Seguritecnia: Revista Decana Independiente de Seguridad”, disponible por

WWW en [http://www.borrmart.es/articulo\\_seguritecnia.php?id=1078](http://www.borrmart.es/articulo_seguritecnia.php?id=1078)

**[13]** “Técnico en redes y seguridad: CAMARAS IP / coordinado por Paula Budris

– Primera edición”. Manual USERS/Fox Andina S.A., Argentina, 2013.

**[14]** “Router – Switch”, disponible por WWW en

<http://www.router-switch.com/>

**[15]** “Técnico en redes y seguridad: DISPOSITIVOS DE RED / coordinado por

Paula Budris – Primera edición”. Manual USERS/Fox Andina S.A.,

Argentina, 2013.



**[16]** “Sistema de seguridad con control de acceso”, disponible por WWW en

<http://seguridadseat.com/control-acceso.html#.VNBDLGi-9UU>

**[17]** “Ordenadores y Portatiles”, disponible por WWW en

<http://www.ordenadores-y-portatiles.com/patch-panel.html>

**[18]** “Direct Industry”, disponible por WWW en

<http://www.directindustry.es/prod/hellermannntyton-usa/patch-paneles-categoria-6a-31061-653789.html>

**[19]** “Suplemento sobre cableado estructurado – v3.1 / Programa De La Academia De Networking De Cisco”. CCNA 1/ Cisco Systems, Inc, 2003.

**[20]** “Axis Communications – Protección y Montaje de cámaras IP”, disponible  
WWW en

<http://www.axis.com/global/es/learning/web-articles/technical-guide-to-network-video/vandal-protection>

**[21]** “Axis Communications – Formatos de Compresión”, disponible

WWW en

[http://classic.www.axis.com/es/products/video/about\\_networkvideo/compressionformats.htm](http://classic.www.axis.com/es/products/video/about_networkvideo/compressionformats.htm)



**[22]** “Axis Communications – Consideraciones sobre ancho de banda y

almacenamiento”, disponible WWW en

[http://classic.www.axis.com/es/products/video/about\\_networkvideo/bandwidth.htm](http://classic.www.axis.com/es/products/video/about_networkvideo/bandwidth.htm)

**[23]** “Sistema de Control de Acceso”, disponible WWW en

<http://www.dointech.com.co/control-de-acceso.html>

**[24]** “Que es una cámara IP - Componentes”, disponible WWW en

[http://videovigilanciaperu.blogspot.com/2009\\_11\\_01\\_archive.html](http://videovigilanciaperu.blogspot.com/2009_11_01_archive.html)

**[25]** “Sensores de Imagen”, disponible WWW en

<http://www.decamaras.com/CMS/content/view/347/40-Es-mejor-una-reflex-con-sensor-CCD-o-CMOS>

**[26]** “Ópticas para cámaras IP”, disponible WWW en

<http://qloudea.com/blog/distancia-focal-camara-ip/>

**[27]** “ADS soluciones confiables”, disponible WWW en

[http://www.ads-veracruz.com.mx/noticias\\_ver.php?id=23](http://www.ads-veracruz.com.mx/noticias_ver.php?id=23)

**[28]** “Fotografía Científica”, disponible WWW en

<http://foto.difo.uah.es>

**[29]** “Grafico - Cable UTP”, disponible WWW en

[http://es.wikipedia.org/wiki/Cable\\_de\\_categor%C3%ADa\\_6](http://es.wikipedia.org/wiki/Cable_de_categor%C3%ADa_6)



**[30]** “Cable Coaxial RG6”, disponible WWW en

<http://media.extron.com/>

**[31]** “Grafico - Conector BNC”, disponible WWW en

[http://es.wikipedia.org/wiki/Conector\\_BNC](http://es.wikipedia.org/wiki/Conector_BNC)

**[32]** “Extensores PoE”, disponible WWW en

<http://www.enconn.com/>

**[33]** “Computadora Core i3”, disponible WWW en

<http://www.pctecnoperu.com/lista.php?tipo=15&grupo=7>



## **7 CAPITULO 7**

### **ANEXOS**

#### **7.1 ANEXO A:**

**PLANO DEL SITEMA DE VIDEOVIGILANCIA IP Y CONTROL  
DE ACCESO.**

#### **7.2 ANEXO B:**

**PLANO DE SECTORIZACION**

#### **7.3 ANEXO C:**

**DATASHEET**