ESCUELA POLITÉCNICA DEL EJÉRCITO
SEDE – LATACUNGA

CARRERA DE TECNOLOGÍA EN ELECTRÓNICA

PROYECTO DE GRADO PARA LA OBTENCIÓN DEL TÍTULO DE:

"TECNÓLOGO EN ELECTRÓNICA"

"ESTUDIO Y DISEÑO DEL SISTEMA DE SEGURIDAD POR VIDEOVIGILANCIA IP PARA EL HOSPITAL DE BRIGADA NO. 11 GALAPAGOS"

CBOP. DE COM. AMAGUAÑA CH. ANGEL R.

CBOS. DE COM. CARDENAS O. FREDY F.

LATACUNGA – ECUADOR

2009

CERTIFICACIÓN

Certificamos, que el presente proyecto de grado fue desarrollado en su totalidad por los señores CBOP. DE COM. AMAGUAÑA CHAVARREA ANGEL ROBERTO Y CBOS. DE COM. CARDENAS ORELLANA FREDY FABIAN, previo a la obtención de su Título de Tecnólogo Electrónico.

Latacunga, Marzo del 2009

_____

Ing. César Naranjo

DIRECTOR

_____

Ing. Sixto Reinoso

CODIRECTOR

AGRADECIMIENTO

Agradecemos a Dios quien con sus bendiciones nos ha permitido concluir con éxito el objetivo trazado. A nuestras familias quienes se constituyen en el principal apoyo e inspiración en cada paso de nuestras vidas. A la Escuela Politécnica del Ejército, a sus docentes y directivos, en especial al Sr. Ing. César Naranjo y al Sr. Ing. Sixto Reinoso por la dedicación y paciencia al impartirnos sus conocimientos.

DEDICATORIA

El presente trabajo va dedicado a mis padres, Doña Victoria y Don Roberto quienes con amor y dedicación han guiado cada uno de mis pasos y me han inculcado los más altos valores. A mis hermanas Laura y Marcela y a mi sobrino David quienes día a día me sirven de apoyo e inspiración.

Angel Roberto

Este trabajo está dedicado a mi esposa Verónica Cabezas y a mis hijas Melany y Antonella que con su amor y compresión me dieron el aliciente para llegar al sitial en el que me encuentro hoy. A mis padres y hermanos que también supieron mantener en mí ese espíritu de lucha contra toda adversidad.

Fredy Fabián

INDICE

RESUMEN

En este proyecto se van a establecer las bases del funcionamiento de un sistema de seguridad por video vigilancia utilizando tecnología IP, como una alternativa a los servicios tradicionales de seguridad que al momento ofrecen las empresas especializadas en seguridad existentes en el mercado.

El proyecto se encuentra dividido en 4 capítulos en los que se exponen de forma ordenada los principios teóricos, diseño y análisis tanto técnico como económico del sistema propuesto.

En el **I Capítulo (Fundamento Teórico)**, luego de una breve introducción se expondrán los antecedentes y la justificación del proyecto. Seguidamente se describirán conceptos básicos de Comunicación inalámbrica, Digitalización de video, Redes IP y Videovigilancia.

El **II Capítulo (Análisis y Diseño del Sistema)**, comienza exponiendo el Planteamiento del problema con sus Objetivos (General y Específicos) y el estudio de Factibilidad (Técnica, Económica y Operacional). Seguidamente se empezará con el Análisis del Sistema, para luego continuar con el Diseño del Sistema en donde se destaca la Definición del escenario y las Consideraciones sobre las Cámaras. A continuación se realizará el diseño del Cableado Estructurado y por último en este capítulo se tratará lo correspondiente al Software a utilizarse.

El **III Capítulo (Resultados del Sistema),** se realizará el Análisis en base a Sistemas Existentes, así como el Análisis Técnico y Análisis Económico.

Finalmente en el **IV Capítulo (Conclusiones y Recomendaciones),** se destacan la conclusión de los principales objetivos trazados, se realizan recomendaciones para aprovechar al máximo el sistema y el correcto uso que se le debe dar al presente trabajo.

I. CAPITULO

FUNDAMENTO TEÓRICO

1.1 INTRODUCCIÓN

La seguridad es un factor de vital importancia para el desarrollo de las instituciones. La videovigilancia se encuentra entre las tecnologías más utilizadas por las instituciones ya sean públicas o privadas para proteger tanto a sus instalaciones como a su personal. La videovigilancia es una de las herramientas más útiles en la lucha contra la delincuencia, además de ayudar a detectar amenazas graves, las cámaras situadas en zonas estratégicas disuaden a los delincuentes para evitar agresiones, robos y vandalismo.

Un sistema de videovigilancia sirve para muchas acciones que se desarrollan en nuestro entorno, controlando las diferentes dependencias sin tener que movernos y además permite una visión global de todas nuestras instalaciones. Adicional a esto graba las imágenes presentes en las cámaras para poder ser analizadas posteriormente.

En los últimos años, la convergencia en redes IP[1] ha alcanzado el mundo de la videovigilancia, tradicionalmente estos sistemas han estado basados en la transmisión analógica del vídeo y su posterior grabación en el clásico formato analógico de cinta mediante equipos VCR, a los cuales se conectan las cámaras empleando una infraestructura dedicada de cable coaxial o fibra óptica.

La avanzada funcionalidad del vídeo IP lo convierte en un medio muy adecuado para las aplicaciones relacionadas con la videovigilancia y seguridad, razón por la cual ponemos en manifiesto el presente proyecto que tiene como tema; **Estudio y**

[1] **IP:** (Internet Protocol - Protocolo de Internet) Protocolo para la comunicación en una red a través de paquetes conmutados.

diseño del Sistema de Seguridad por Videovigilancia para el HOSPITAL DE BRIGADA No. 11 ¨GALAPAGOS¨, el mismo que coadyuvará al desarrollo institucional, proporcionando una herramienta que le permitirá desenvolverse en un ambiente de seguridad y confianza.

1.1.1 ANTECEDENTES

El HOSPITAL DE BRIGADA No. 11 ¨GALAPAGOS¨, es una Institución con un alto nivel de aceptación dentro de la región central que presta sus servicios al personal militar y por su gran desempeño y labor social también a extendido su ayuda a la ciudadanía en general de la provincia de Chimborazo atendiendo en todas sus áreas disponibles con total predisposición. Todos estos buenos resultados se deben al personal que conforma este prestigioso hospital que cumple sus funciones con responsabilidad. Para viabilizar de forma adecuada su atención se ha visto en la necesidad de mejorar su infraestructura, razón por la cual se está realizando la reubicación del mismo en las nuevas instalaciones que se encuentran dentro de la BRIGADA DE CABALLERIA BLINDADA No. 11 ¨GALAPAGOS¨.

Al existir muchos requerimientos por parte del HOSPITAL DE BRIGADA No. 11 ¨GALAPAGOS¨ y para el óptimo funcionamiento de dichas instalaciones, entre sus principales prioridades se a puesto de manifiesto la videovigilancia de manera que garanticen todo lo existente en el hospital.

Un sistema de videovigilancia permitirá establecer un mejor control del personal propio y ajeno que ingresa a las instalaciones, y las actividades que se desarrollan en los diferentes sectores de la dependencia, de tal forma que en lo posible no exista novedades de ningún índole**.**

1.1.2 JUSTIFICACIÓN

Luego de un exhaustivo análisis el HOSPITAL DE BRIGADA No.11 ¨GALAPAGOS¨ se ha visto en la necesidad de realizar un estudio de un sistema de vigilancia que preste las condiciones adecuadas para preservar todo lo existente en dicho lugar, para lo cual se ha considerado como un camino viable la utilización de la Videovigilancia IP que presta la condiciones adecuadas de diseño, instalación y operabilidad.

La Videovigilancia IP representa una alternativa a la mayoría de los problemas más comunes a la hora de instalar sistemas de video vigilancia como son:

- Distancia
- Falta de infraestructura de red
- Condiciones climatológicas
- Precio

La Videovigilancia IP ha crea una aplicación de seguridad que va más allá que cualquiera de las tecnologías disponibles y proporciona además las siguientes características:

- Fácil de desplegar
- Alto grado de funcionalidad
- Totalmente escalable

1.1.3 LA EVOLUCIÓN DE LOS SISTEMAS DE VIGILANCIA POR VIDEO

Los sistemas de vigilancia por video existen desde hace 25 años. Empezaron siendo sistemas analógicos al 100% y paulatinamente se fueron digitalizando. Los

sistemas de hoy en día han avanzado mucho desde la aparición de las primeras cámaras analógicas con tubo conectadas a VCR[2].

En la actualidad, estos sistemas utilizan cámaras y servidores de PC para la grabación de video en un sistema completamente digitalizado. Sin embargo, entre los sistemas completamente analógicos y los sistemas completamente digitales existen diversas soluciones que son parcialmente digitales.

Dichas soluciones incluyen un número de componentes digitales pero no constituyen sistemas completamente digitales.

Tabla 1.1 sistemas de vigilancia por video

Completamente análogo:	Sistemas de circuito cerrado de TV analógicos Usando VCR
En parte digital:	Sistemas de circuito cerrado de TV analógicos usando DVR Sistemas de circuito cerrado de TV analógicos Usando DVR de red
Completamente digital:	Sistemas de vídeo IP que utilizan servidores de vídeo Sistemas de video de red usando cámaras de Red

1.1.3.1 Sistemas de circuito cerrado de TV analógicos usando VCR

Un sistema de circuito cerrado de TV (CCTV) analógico que utilice un VCR (fig.1.1) representa un sistema completamente analógico formado por cámaras analógicas con salida coaxial, conectadas al VCR para grabar.

[2] **VCR:** (Video Cassette Recorder) Grabadora de casetes de video.

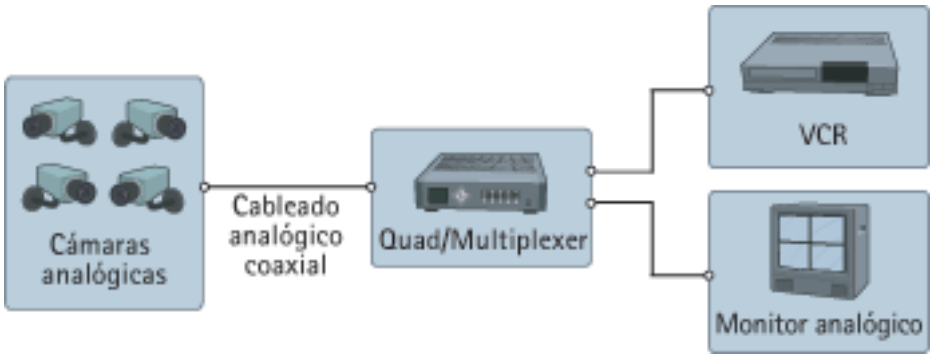


Fig.1.1 CCTV analógico con VCR

El VCR utiliza el mismo tipo de cintas que una grabadora doméstica. El video no se comprime y, si se graba a una velocidad de imagen completa, una cinta durara como máximo 8 horas. En sistemas mayores, se puede conectar un quad[3] o un multiplexor entre la cámara y el VCR. El quad/multiplexor permite grabar el vídeo procedente de varias cámaras en un solo grabador, pero con el inconveniente que tiene una menor velocidad de imagen. Para monitorear el video, es necesario un monitor analógico.

1.1.3.2 Sistemas de circuito cerrado de TV Analógicos usando DVR

Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR[4] (fig.1.2) es un sistema analógico con grabación digital. En un DVR, la cinta de video se sustituye por discos duros para la grabación de video, y es necesario que el video se digitalice y comprima para almacenar la máxima cantidad de imágenes posible de un día.

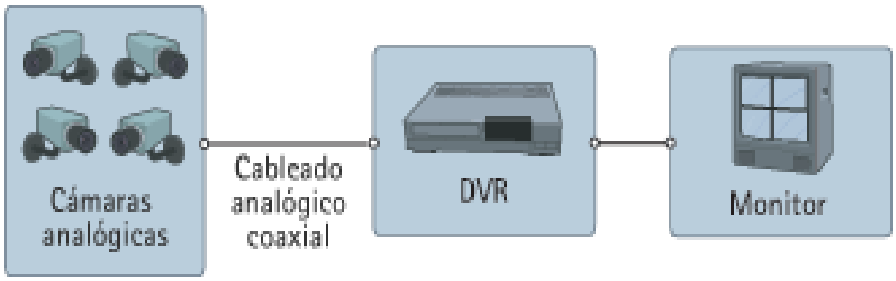


Fig.1.2 CCTV analógico con DVR

[3] **QUAD:** Dispositivos que permiten combinar hasta 4 cámaras y mostrarlas al mismo tiempo
[4] **DVR:** Digital Video Recorder – Grabador de Video Digital.

Con los primeros DVR, el espacio del disco duro era limitado, por tanto, la duración de la grabación era limitada, o debía usarse una velocidad de imagen inferior. El reciente desarrollo de los discos duros significa que el espacio deja de ser el principal problema. La mayoría de DVR dispone de varias entradas de video, normalmente 4, 9 ó 16, lo que significa que también incluyen la funcionalidad de los quads y multiplexores.

El sistema DVR añade las siguientes ventajas:

- No es necesario cambiar las cintas
- Calidad de imagen constante

1.1.3.3 Sistemas de circuito cerrado de TV analógicos usando DVR de red

Un sistema de circuito cerrado de TV (CCTV) analógico usando un DVR IP (fig.1.3) es un sistema parcialmente digital que incluye un DVR IP equipado con un puerto Ethernet para conectividad de red. Como el video se digitaliza y comprime en el DVR, se puede transmitir a través de una red informática para que se monitoree en un PC en una ubicación remota.

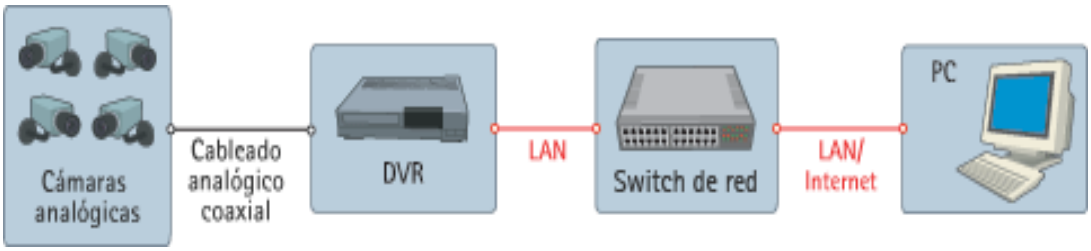


Fig.1.3 CCTV analógico con DVR IP

Algunos sistemas pueden monitorear tanto video grabado como en directo, mientras otros sólo pueden monitorear el video grabado. Además, algunos sistemas exigen un cliente Windows especial para monitorear el video, mientras que otros utilizan un navegador web estándar, lo que flexibiliza la monitorización remota.

El sistema DVR IP añade las siguientes ventajas:

- Monitorización remota de video a través de un PC
- Funcionamiento remoto del sistema

1.1.3.4 Sistemas de video IP que utilizan servidor de video

Un sistema de video IP que utiliza servidor de video (fig.1.4) incluye un servidor de video, un conmutador de red y un PC con software de gestión de video. La cámara analógica se conecta al servidor de video, el cual digitaliza y comprime el video. A continuación, el servidor de video se conecta a una red y transmite el video a través de un conmutador de red a un PC, donde se almacena en discos duros. Esto es un verdadero sistema de video IP.

Un sistema de video IP que utiliza servidor de video añade las ventajas siguientes:

- El sistema es escalable en ampliaciones de una cámara cada vez
- Es posible la grabación fuera de las instalaciones
- Preparado para el futuro, ya que este sistema puede ampliarse fácilmente incorporando cámaras IP

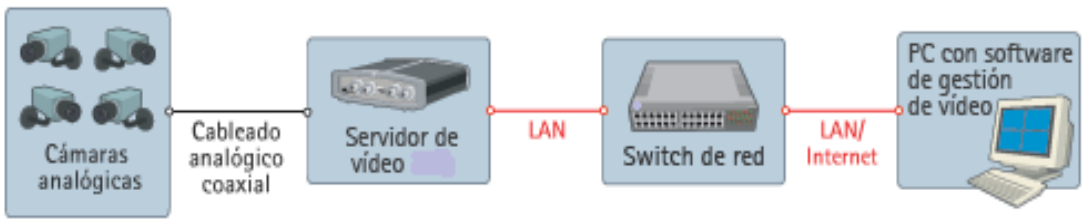


Fig.1.4 Sistema de video IP

Este diagrama muestra un sistema de video IP, donde la información del video se transmite de forma continua a través de una red IP. Utiliza un servidor de video como elemento clave para migrar el sistema analógico de seguridad a una solución de video IP.

1.1.3.5 Sistemas de video IP que utilizan cámaras IP

Una cámara IP combina una cámara y un ordenador en una unidad, lo que incluye la digitalización y la compresión del video así como un conector de red. El video se transmite a través de una red IP, mediante los conmutadores de red y se graba en un PC estándar con software de gestión de video. Esto representa un verdadero sistema de video IP donde no se utilizan componentes analógicos.

Un sistema de video IP que utiliza cámaras IP (fig.1.5) añade las ventajas siguientes:

- Cámaras de alta resolución (megapíxel)
- Calidad de imagen constante
- Alimentación eléctrica a través de Ethernet y funcionalidad inalámbrica
- Funciones de Pan/tilt/zoom PTZ[5], audio, entradas y salidas digitales a través de IP, junto con el vídeo
- Flexibilidad y escalabilidad completas

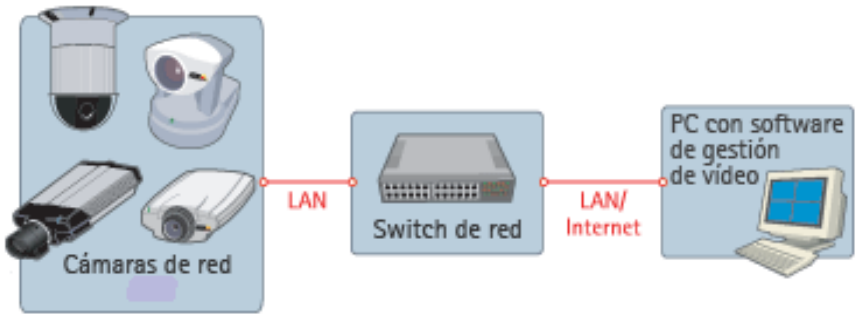


Fig.1.5 Sistema de video IP

Este diagrama muestra un verdadero sistema de video IP, donde la información del video se transmite de forma continua a través de una red IP, utilizando cámaras IP. Este sistema saca el máximo partido de la tecnología digital y proporciona una calidad de imagen constante desde la cámara hasta el visualizador, donde quiera que estén.

[5] **PTZ:** control de movimiento horizontal y vertical y control en el desplazamiento de foco(campo de la vista)

1.2 COMUNICACIÓN INALÁMBRICA

Las redes inalámbricas (wireless network) son aquellas que se comunican por un medio de transmisión no guiado (sin cables) mediante ondas electromagnéticas. La transmisión y la recepción se realizan a través de antenas.

Tienen ventajas como la rápida instalación de la red sin la necesidad de usar cableado, permiten la movilidad y tienen menos costos de mantenimiento que una red convencional. En la figura 1.6 se muestra un ejemplo de comunicación inalámbrica.

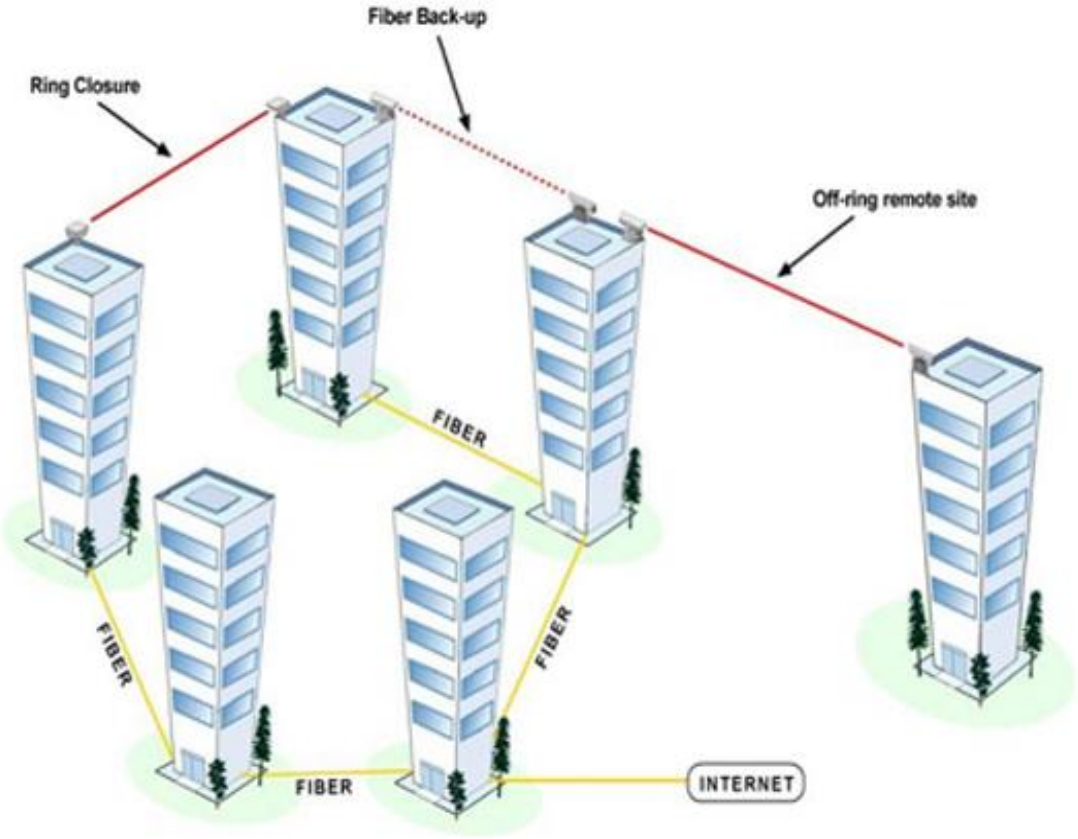


Fig.1.6 Comunicación inalámbrica por infrarrojo

1.2.1 CLASIFICACIÓN SEGÚN SU COBERTURA

WPAN (Wireless Personal Area Network).- En este tipo de red de cobertura personal, existen tecnologías basadas en HomeRF (estándar para conectar todos los teléfonos móviles de la casa y los ordenadores mediante un aparato central); Bluetooth (protocolo que sigue la especificación IEEE 802.15.1); ZigBee (basado en la especificación IEEE 802.15.4 y utilizado en aplicaciones como la domótica, que requieren comunicaciones seguras con tasas bajas de transmisión de datos y maximización de la vida útil de sus baterías, bajo consumo); RFID (sistema remoto de almacenamiento y recuperación de datos con el propósito de transmitir la identidad de un objeto similar a un número de serie único mediante ondas de radio).

WLAN (Wireless Local Area Network).- En las redes de área local podemos encontrar tecnologías inalámbricas basadas en HiperLAN (High Performance Radio LAN), un estándar del grupo ETSI, o tecnologías basadas en Wi-Fi, que siguen el estándar IEEE 802.11 con diferentes variantes.

WMAN (Wireless Metropolitan Area Network, Wireless MAN).- Para redes de área metropolitana se encuentran tecnologías basadas en WiMax (Worldwide Interoperability for Microwave Access, es decir, Interoperabilidad Mundial para Acceso con Microondas), un estándar de comunicación inalámbrica basado en la norma IEEE 802.16. WiMax es un protocolo parecido a Wi-Fi, pero con más cobertura y ancho de banda. También podemos encontrar otros sistemas de comunicación como LMDS (Local Multipoint Distribution Service).

WWAN (Wireless Wide Area Network, Wireless WAN).- En estas redes encontramos tecnologías como UMTS (Universal Mobile Telecommunications System), utilizada con los teléfonos móviles de tercera generación (3G) y sucesora de la tecnología GSM (para móviles 2G), o también la tecnología digital para móviles GPRS (General Packet Radio Service).

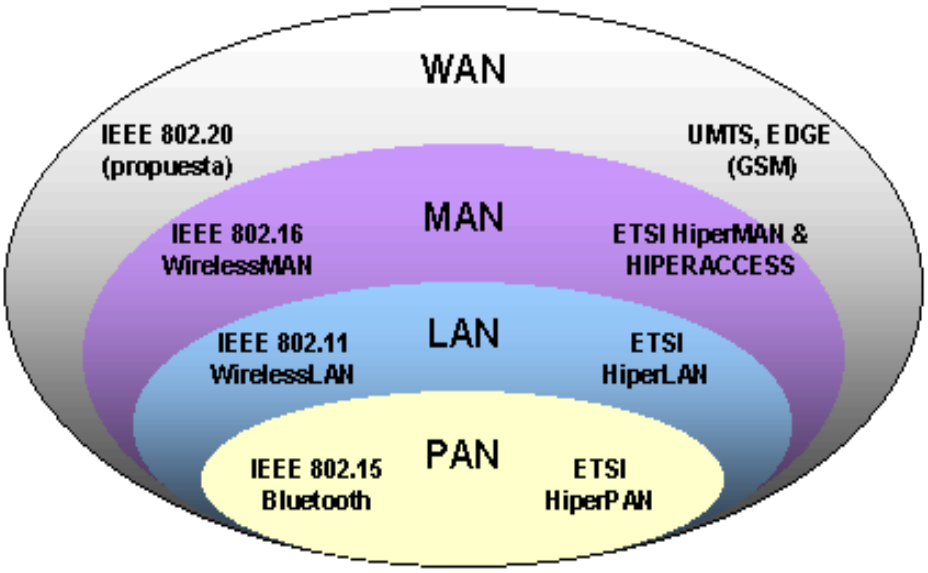


Fig.1.7 Posicionamiento de estándares wireless

1.2.2 CLASIFICACIÓN SEGÚN EL RANGO DE FRECUENCIAS

Ondas de radio: las ondas electromagnéticas son omnidireccionales, así que no son necesarias las antenas parabólicas. La transmisión no es sensible a las atenuaciones producidas por la lluvia ya que se opera en frecuencias no demasiado elevadas. En este rango se encuentran las bandas desde la ELF que va de 3 a 30 Hz, hasta la banda UHF que va de los 300 a los 3000 MHz, es decir, comprende el espectro radioeléctrico de 30 - 3000000 Hz.

Microondas terrestres: se utilizan antenas parabólicas con un diámetro aproximado de unos tres metros. Tienen una cobertura de kilómetros, pero con el inconveniente de que el emisor y el receptor deben estar perfectamente alineados. Por eso, se acostumbran a utilizar en enlaces punto a punto en distancias cortas. En este caso, la atenuación producida por la lluvia es más importante ya que se opera a una frecuencia más elevada. Las microondas comprenden las frecuencias desde 1 hasta 300 GHz.

Microondas por satélite: se hacen enlaces entre dos o más estaciones terrestres que se denominan estaciones base. El satélite recibe la señal

(denominada señal ascendente) en una banda de frecuencia, la amplifica y la retransmite en otra banda (señal descendente). Cada satélite opera en unas bandas concretas. Las fronteras frecuenciales de las microondas, tanto terrestres como por satélite, con los infrarrojos y las ondas de radio de alta frecuencia se mezclan bastante, así que pueden existir interferencias con las comunicaciones en determinadas frecuencias.

Infrarrojos: se enlazan transmisores y receptores que modulan la luz infrarroja no coherente. Deben estar alineados directamente o con una reflexión en una superficie. No pueden atravesar las paredes. Los infrarrojos van desde 300 GHz hasta 384 THz.

Aplicaciones: Las bandas más importantes con aplicaciones inalámbricas, del rango de frecuencias que abarcan las ondas de radio, son la VLF (comunicaciones en navegación y submarinos), LF (radio AM de onda larga), MF (radio AM de onda media), HF (radio AM de onda corta), VHF (radio FM y TV), UHF (TV).

Mediante las microondas terrestres, existen diferentes aplicaciones basadas en protocolos como Bluetooth o ZigBee para interconectar ordenadores portátiles, PDAs, teléfonos u otros aparatos. También se utilizan las microondas para comunicaciones con radares (detección de velocidad u otras características de objetos remotos) y para la televisión digital terrestre.

Las microondas por satélite se usan para la difusión de televisión por satélite, transmisión telefónica a larga distancia y en redes privadas.

Los infrarrojos tienen aplicaciones como la comunicación a corta distancia de los ordenadores con sus periféricos. También se utilizan para mandos a distancia, ya que así no interfieren con otras señales electromagnéticas, por ejemplo la señal de televisión. Uno de los estándares más usados en estas comunicaciones es el

IrDA[6] (Infrared Data Association). Otros usos que tienen los infrarrojos son técnicas como la termografía[7], la cual permite determinar la temperatura de objetos a distancia.

1.2.3 SISTEMAS DE COMUNICACIÓN INALAMBRICA

1.2.3.1 Wi-Fi

Wi-Fi es similar a la red Ethernet tradicional y como tal el establecimiento de comunicación necesita una configuración previa. Utiliza el mismo espectro de frecuencia que Bluetooth con una potencia de salida mayor que lleva a conexiones más sólidas. A veces se denomina a Wi-Fi la “Ethernet sin cables”. Aunque esta descripción no es muy precisa, da una idea de sus ventajas e inconvenientes en comparación a otras alternativas. Se adecua mejor para redes de propósito general: permite conexiones más rápidas, un rango de distancias mayor y mejores mecanismos de seguridad.

Fig.1.8 Punto de acceso inalámbrico.

[6] **IrDA (Infrared Data Association):** estándar para transmisión y recepción de datos por rayos infrarrojo
[7] **Termografía:** técnica que permite, a distancia y sin ningún contacto, medir y visualizar temperaturas de superficie con precisión.

1.2.3.2 Bluetooth

Bluetooth es una especificación industrial para Redes Inalámbricas de Área Personal (WPANs) que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia segura y globalmente libre (2,4 GHz.). Los principales objetivos que se pretende conseguir con esta norma son:

- Facilitar las comunicaciones entre equipos móviles y fijos
- Eliminar cables y conectores entre éstos
- Ofrecer la posibilidad de crear pequeñas redes inalámbricas y facilitar la sincronización de datos entre nuestros equipos personales

Los dispositivos que con mayor intensidad utilizan esta tecnología son los sectores de las telecomunicaciones y la informática personal, como PDAs, teléfonos móviles, computadoras portátiles, ordenadores personales, impresoras y cámaras digitales, en el ejemplo mostramos una forma de transmisión de datos por medio de bluetooth.

Fig.1.9 Teclado bluetooth enlazado a un computador de bolsillo

HomeRF

Existen el HomeRF y el HomeRF2.

La idea de este estándar se basa en el Teléfono inalámbrico digital mejorado (Digital Enhaced Cordless Telephone, DECT) que es un equivalente al estándar de los teléfonos celulares GSM. Transporta voz y datos por separado, al contrario que protocolos como el WiFi que transporta la voz como una forma de datos. Los creadores de este estándar pretendían diseñar un aparato central en cada casa que conectara los teléfonos y además proporcionar un ancho de banda de datos entre las computadoras.

Las prestaciones de este sistema son:

- Modulación FSK (Frecuency Shift Keying).
- Velocidad de datos variables de entre 800 Kbps y 1.6Mbps.
- Utiliza la banda de 2.4 Ghz.
- 75 canales de 1 Mhz para voz.

El HomeRF2:

- Velocidad de entre 5 y 10 Mbps.
- 15 canales de 5 MHz para voz

Cabe resaltar que el estándar HomeRF posee multitud de capacidades de voz (identificador de llamadas, llamadas en espera, regreso de llamadas e intercomunicación dentro del hogar).

1.2.3.3 ZigBee

ZigBee es el nombre de la especificación de un conjunto de protocolos de alto nivel de comunicación inalámbrica para su utilización con radios digitales de bajo consumo, basada en el estándar IEEE 802.15.4 de redes inalámbricas de área personal (wireless personal area network, WPAN). Su objetivo son las aplicaciones que requieren comunicaciones seguras con baja tasa de envío de datos y maximización de la vida útil de sus baterías.

En principio, el ámbito donde se prevé que esta tecnología cobre más fuerza es en domótica[8], la razón de ello son diversas características que lo diferencian de otras tecnologías:

- Su bajo consumo
- Su topología de red en malla
- Su fácil integración (se pueden fabricar nodos con muy poca electrónica)

1.3 DIGITALIZACIÓN DE VIDEO

La digitalización es el proceso mediante el cual, partiendo de una señal analógica, como es cualquiera de las imágenes que nos rodean en el mundo real, obtenemos una representación de la misma en formato digital (señal digital).

La digitalización de una imagen se basa a una división del espacio a modo de cuadrícula, donde la unidad más pequeña se denomina píxel. Para cada uno de los pixels que tenemos en una imagen hay que guardar la información referente a la luminancia (brillo o niveles de gris) y, si es en color, también al nivel de cada una de las componentes, R(rojo), G(verde) y B(azul). Por tanto para una imagen tendremos varias matrices de información.

Cuando hablamos de digitalización de video debemos tener en cuenta que entra en juego una tercera dimensión, el tiempo. Por tanto una secuencia de video se genera mediante la proyección de un número de imágenes en un tiempo determinado, que dependerá del sistema sobre el que trabajemos (24 imágenes/segundo en cine, 25/s en el sistema PAL[9]...). El problema de este planteamiento es el alto volumen de datos que se crean. Es por esto que se han desarrollado varios estándares de codificación y compresión como es la familia

[8] **Domótica:** Conjunto de sistemas que automatizan las diferentes instalaciones de un edificio.
[9] **PAL** (Phase Alternating Line-Línea Alternada en Fase): Sistema de codificación para transmisión de señales de televisión analógica en color.

MPEG entre otros que permiten obtener una alta calidad de video a la vez que diferentes tasas para diversas aplicaciones.
Pero para obtener una imagen digital debemos tener en cuenta varios pasos:

1.3.1 MUESTREO

La importancia de esta parte del proceso es evidente. Es el único momento en el que tenemos contacto con la imagen original, o señal analógica, y es cuando decidimos con cuánta información queremos quedarnos. Es irreversible, puesto que toda aquella información que desechemos ya no podremos recuperarla y, por tanto, la calidad de la imagen digital que generemos se verá afectada por el criterio que seleccionemos.

Antes de muestrear una señal analógica, para evitar el posible efecto aliasing[10] o solapamiento de los términos espectrales, debemos cumplir dos requisitos fundamentales:

- Limitar la imagen en una banda de frecuencias
- Cumplir que la frecuencia de muestreo sea como mínimo el doble de la máxima frecuencia de la imagen (Teorema de Nyquist)

Generalmente, pero dentro de ciertos límites, el aumento de la frecuencia de muestreo también ayuda a aumentar la resolución.

1.3.2 CUANTIFICACIÓN

Es el proceso mediante el cual se decide, para cada rango de colores (mundo analógico), cual va a ser el color con el que va a ser representado en la imagen final. Por tanto, cuantos más niveles se tengan definidos mejor será la calidad. El problema que presenta es que, a mayor nivel de definición, mayor será el

[10] **Aliasing:** Efecto que causa que señales continuas distintas se tornen indistinguibles cuando se les muestrea digitalmente.

volumen de datos que deberemos guardar por cada uno de los pixels[11]. La transformación realizada es también irreversible, perderemos colores.

1.3.3 CODIFICACIÓN

Es el proceso de conversión de los valores cuantificados al sistema binario donde la organización final de los "bits" dependerá del formato que se escoja.

Existen dos métodos de digitalización:

Luminancia (Y): representa el brillo de cada píxel, es decir blanco y negro.
Crominancia (U y V): representa el color y la saturación.

1.3.4 DIGITALIZACIÓN 4:4:4

Método que consiste en guardar toda la información de una imagen, con lo que ésta no sufre pérdidas.

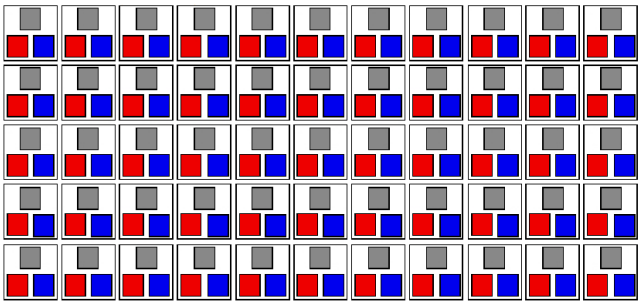


Fig.1.10 Representación del muestreo 4:4:4.

1.3.5 DIGITALIZACIÓN 4:2:2

El ojo humano es más sensible al brillo que al color por eso una opción que se puede aplicar al guardar la imagen, es reducir la información del color respecto a la de brillo.

[11] **Píxel** (picture element-elemento de imagen): Menor unidad homogénea en color que forma parte de una imagen digital

4:2:2 reduce la información cromática a la mitad, el color tiene la mitad de resolución (en horizontal), y el brillo sigue intacto. Por cada 4 muestras de Y, hay dos para U y V.

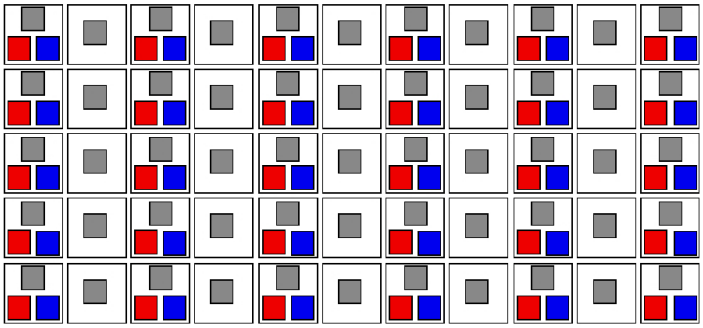


Fig.1.11 Representación del muestreo 4:2:2

1.3.6 DIGITALIZACIÓN 4:2:0

4:2:0 explora los colores en líneas alternas: en una línea recoge el rojo y en la siguiente, el azul, y así sucesivamente. Por tanto, reduce el color a la cuarta parte ya que lo hace en un factor de 2 en ambas direcciones, horizontal y vertical.

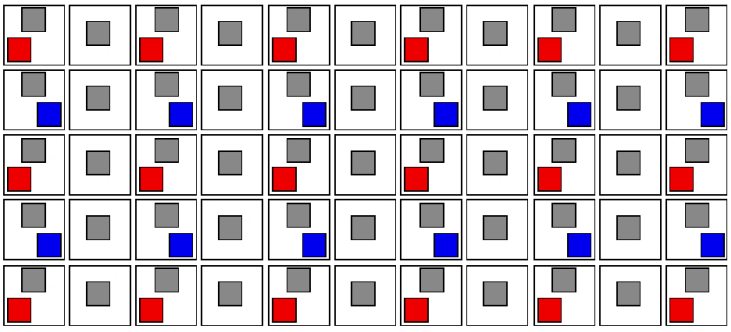


Fig.1.12 Representación del muestreo 4:2:0

1.3.7 DIGITALIZACIÓN 4:1:1

Las muestras de crominancia (U y V) son tomadas una vez cada cuatro muestras horizontales de luminancia (Y).

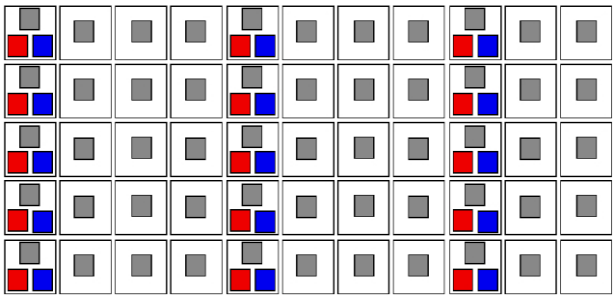


Fig.1.13 Representación del muestreo 4:1:1

1.3.8 FORMATO MPEG

MPEG (Grupo de Expertos en Imágenes en movimiento) es un estándar internacional, definido por un comité llamado MPEG formado por la ISO, para la representación codificada y comprimida de imágenes en movimiento y audio asociado, orientado a medios de almacenamiento digital. MPEG aplica la compresión temporal y la espacial. MPEG requiere una intensiva computación para su codificación, aunque se consiguen ratios[12] desde 50:1 hasta 200:1.

Los estándares MPEG fueron desarrollados para ser independientes de la red específica para proporcionar un punto de interoperabilidad en entornos de red heterogéneos.

1.3.8.1 MPEG-1

MPEG-1 guarda una imagen, la compara con la siguiente y almacena sólo las diferencias. Se alcanzan así grados de compresión muy elevados. Define tres tipos de fotogramas:

- Fotogramas I o Intra-fotogramas, son los fotogramas normales o de imagen fija, proporcionando una compresión moderada, en JPEG[13].

[12] **Ratio:** Indica en qué proporción ha sido reducida la información.
[13] **JPEG** (Joint Photographic Experts Group): método utilizado para la compresión de imágenes fotográficas.

- Fotogramas P o Predichos: son imágenes predichas a partir de la inmediatamente anterior. Se alcanza una tasa de compresión muy superior.
- Fotogramas B o bidireccionales: se calculan en base a los fotogramas inmediatamente anterior y posterior. Consigue el mayor grado de compresión a costa de un mayor tiempo de cálculo. Estándar escogido por Vídeo-CD: calidad VHS con sonido digital.

1.3.8.2 MPEG-2

Con una calidad superior al MPEG-1, MPEG-2 fue universalmente aceptado para transmitir vídeo digital comprimido con velocidades mayores de 1Mb/s aproximadamente. Con MPEG-2 pueden conseguirse elevados ratios de hasta 100:1, dependiendo de las características del propio vídeo.

1.3.8.3 MPEG4

Es un estándar relativamente nuevo orientado inicialmente a las videoconferencias, y para Internet. El objetivo es crear un contexto audiovisual en el cual existen unas primitivas llamadas AVO[14]. Se definen métodos para codificar estas primitivas que podrían clasificarse en texto y gráficos.

La comunicación con los datos de cada primitiva se realiza mediante uno o varios "elementary streams" o flujos de datos, cuya característica principal es la calidad de servicio requerida para la transmisión.

Ha sido especialmente diseñado para distribuir videos con elevados ratios de compresión, sobre redes con bajo ancho de banda manteniendo una excelente calidad para usuarios con buen ancho de banda. Ofrece un amplio rango de velocidades desde usuarios con modems de 10kbps a usuarios con anchos de banda de 10Mbps.

[14] **AVO** (Audiovisual object.-Objeto Audiovisual): Son los objetos de una escena, como objetos de video, imágenes y objetos 3D.

1.3.8.4 MPEG 2000

Basado en la tecnología Wavelet, este relativamente nuevo estándar está optimizado para imágenes que contienen pequeñas cantidades de datos. Su relativamente inferior calidad de imágenes está compensada con unas bajas necesidades de ancho de banda en el medio de transmisión.

1.3.8.5 Wavelet

Optimizado para imágenes que contienen pequeñas cantidades de datos. Su relativamente inferior calidad de imágenes está compensada con unas bajas necesidades de ancho de banda en el medio de transmisión. Actualmente no hay un estándar formal para Wavelet.

1.3.8.6 H.261/H.263

El H.261 y el H-263 no son Estándares Internacionales sino recomendaciones de la ITU. Ambos están basados en la misma técnica que los estándares MPEG y pueden ser interpretados como versiones simplificadas de la compresión de vídeo MPEG.

Fueron diseñados originalmente para video conferencia sobre líneas telefónicas con poco ancho de banda. En cualquier caso es un poco contradictorio que muestren carencia de alguna de las técnicas MPEG más avanzadas para ofrecer realmente un uso eficiente del ancho de banda.

1.3.8.7 Motion-JPEG

Motion-JPEG es una versión extendida del algoritmo JPEG que comprime imágenes. Básicamente consiste en tratar al vídeo como una secuencia de imágenes estáticas independientes a las que se aplica el proceso de compresión del algoritmo JPEG una y otra vez para cada imagen de la secuencia de vídeo.

Existen cuatro modos de operación para el JPEG: secuencial, progresiva, sin pérdida, y jerárquica. Normalmente se utiliza el modo secuencial.

1.3.9 PROTOCOLOS RTP/RTCP.

1.3.9.1 RTP (Protocolo en tiempo real)

El objetivo de RTP es brindar un medio uniforme de transmisión sobre IP de datos que estén sujetos a las limitaciones de tiempo real (audio, video, etc.). La función principal de RTP es implementar los números de secuencia de paquetes IP para rearmar la información de voz o de video, incluso cuando la red subyacente cambie el orden de los paquetes.

De manera más general, RTP permite:

- Identificar el tipo de información transmitida
- Agregar marcadores temporales y números de secuencia a la información transmitida
- Controlar la llegada de los paquetes a destino

Además, los paquetes de difusión múltiple pueden utilizar RTP para enrutar conversaciones a múltiples destinatarios.

1.3.9.2 RTCP (Protocolo de control en Real-Time)

El protocolo RTCP se basa en transmisiones periódicas de paquetes de control que realizan todos los participantes de la sesión. Es un protocolo de control para el flujo RTP, que permite transmitir información básica sobre los participantes de la sesión y la calidad de servicio.

1.4 REDES IP.

1.4.1 CONCEPTO Y NIVELES.

Una red informática o de computadoras es un conjunto de equipos de cómputo conectados entre sí a través de cables, señales ondas u otro medio de trasmisión de datos para compartir recursos entre sí. Para que esta comunicación entre equipos sea posible cuentan con normas para la transmisión y recepción de datos. Estos, deben estar diseñados de acuerdo a las normas OSI (Open Systems Interconection), establecida para estandarizar la forma de interconexión entre los equipos.

Esta cuenta con siete capas o niveles:

1.4.1.1 Nivel Físico

Es en el que se establecen los medios de trasporte, conexión y transmisión de los datos, la transmisión puede ser guiada, es decir por medio de cables como el par trenzado, coaxial, telefónico; o no guiada, es decir por medio de microondas, láser, infrarroja, cualquier método inalámbrico.

1.4.1.2 Nivel de Enlace

Aquí se establecerán las formas de enlace de la red, es decir, medios confiables para la transmisión de los datos, direccionamiento físico, topología, acceso a la red, notificación de errores y control de flujo de los datos.

1.4.1.3 Nivel de Red

En este nivel se determina la forma en que las señales se mantienen conectadas, aunque no sea de forma directa y la forma de realizarlo es a través de router ó encaminadores.

1.4.1.4 Nivel de transporte

Es el encargado del envío de los datos ya sea de manera completa o de ser necesario segmentarla y a estos segmentos se les llama paquetes, para llevarla a través de las capas superiores de la red.

1.4.1.5 Nivel de sesión:

Gestiona el inicio, transmisión y cierre de sesión de trabajo en la red, por lo que su trabajo es verificar que dos actividades no se realicen al mismo tiempo.

1.4.1.6 Nivel de presentación:

Se encarga de que la información llegue de manera reconocible y legible, aunque los sistemas tengan distintas tablas de códigos para la representación de los datos (pueden ser ASCII, EBCDIC, entre muchos otros).

1.4.1.7 Nivel de Aplicación:

Ofrece a las aplicaciones la forma de interactuar con las demás capas haciendo posible su comunicación estableciendo el protocolo de comunicación de datos para utilizar correo electrónico, administradores de bases de datos, entre muchas mas aplicaciones.

1.4.2 TIPOS DE RED Y CONEXIONES

Dentro del ámbito de las redes existen varios tipos:

PAN (Personal Area Network): Red de área personal, con la cual es posible la conexión de dispositivos personales, como computadoras, PDA[15], celulares etc.

[15] PDA (Personal Digital Assistant-Asistente Digital Personal): Computador de mano originalmente diseñado como agenda electrónica.

LAN (Local Area Network): La red de área local, que como su nombre lo dice es una interconexión a nivel local como una oficina, edificio, sin interconectarse a ningún otro lado fuera de ella.

MAN (Metropolitan Area Nerwork): Red de área metropolitana, con la cual es posible interconectar redes de una misma region geográfica.

WAN (Wide Area Network): Red de área amplia, que es con la que es posible realizar conexiones de red por miles de kilómetros con los cuales es posible interconectar países a través de una red.

1.4.3 TIPOS DE CONEXIÓN.

Dentro del ámbito de las redes hay varias formas de realizar una conexión entre las computadoras, a continuación presentaremos las más comunes:

1.4.3.1 Conexión de red en bus.

En este tipo de conexión los clientes o terminales de la red están conectadas a un solo canal o cable, por el cual pasan los datos, todos los clientes pueden ver la información en cualquier momento es decir un cliente envía información y los demás clientes escuchan la señal, es una de las conexiones más sencillas de realizar como se muestra en la figura 1.14:

Fig.1.14 Red bus

1.4.3.2 Conexión de red en Anillo.

Esta conexión consiste en que todos los nodos o clientes están conectados unos a otros y el primero y último nodo se conectan para cerrar el anillo, para el paso de la información a través de la red utiliza una señal testigo llamada token la cual se encarga de hacer llegar los paquetes de información a los demás clientes, el problema con esta red es que si un nodo se desconecta todas las demás terminales pierden la conexión. A continuación en la figura 1.15 se muestra el ejemplo:

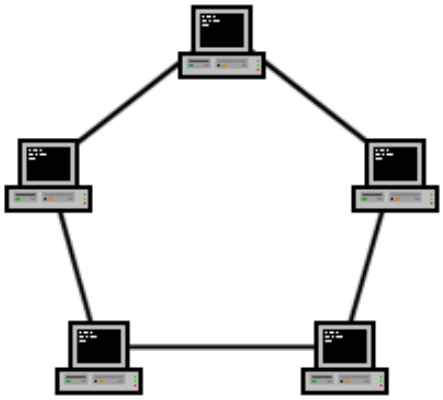


Fig.1.15 Red en anillo

1.4.3.3 Conexión de red en estrella.

En esta red todas las computadoras están conectadas a un punto central llamado concentrador, que se encarga de llevar la información a cada cliente, además de tener la función de amplificar la señal de comunicación. Las ventajas de esta conexión es que los nodos están directamente conectados al concentrador por lo que ningún nodo escucha la información de otro, la conexión para la instalación es más rápida, como el concentrador es el que lleva la información los datos no colisionan ya que cada uno tiene un cable independiente conectado al concentrador. Las desventajas que presenta esta es que la longitud de cable para conexión y número de nodos son limitados, en ocasiones el mantenimiento puede llegar a ser costoso, pero en los últimos años se ha convertido en la forma de

conexión de red más utilizada por su facilidad de manejo, ya que el concentrador también tiene la función de ser un monitor para supervisar el buen funcionamiento de la red. A continuación veremos en la figura 1.16 el ejemplo de esta conexión:

Fig. 1.16 Red en estrella

1.4.3.4 Conexiones Híbridas.

Es la combinación de las conexiones para redes, pueden ser una conexión en estrella y anillo, o bien en estrella y bus, o bien en estrella jerárquica; esta última mencionada consiste en varias redes en estrella con un cierto orden dependiendo un concentrador de otro y cada concentrador tiene sus clientes.

Para realizar estas conexiones se utilizan cables de par trenzado, coaxial, fibra óptica. En la actualidad se está utilizando el cable de par trenzado, y para comunicaciones a grandes distancias por cable se utiliza la fibra óptica.

También existen muchos artefactos que se utilizan para la conexión de las redes y conexión al exterior, es decir a internet e inclusive para interconectar redes, estos dispositivos son:

Ruteadores (Routers).- Estos son utilizados para la interconexión de redes donde internamente se le dice al dispositivo que ruta seguir para establecer el contacto con otra red.

Fig.1.17 Ruteador

Concentradores (Hubs).- Este dispositivo tiene la función de establecer el contacto entre los nodos de la red, administrando las solicitudes de flujo de datos entre el nodo solicitante y la información solicitada a los servidores de la información.

Fig.1.18 Hub para 4 puertos ethernet

Switch.- Este dispositivo además de ser un concentrador, tiene la gran posibilidad de ser un amplificador de de señal, con una administración eficiente de las solicitudes de datos de cliente al servidor, en la cual cada cliente puede solicitar información al mismo tiempo sin contratiempos o colapsos de la información gracias a su semáforo interno que identifica a donde debe llegar la información directamente.

Fig.1.19 Switch fast ethernet

Gateways (Puertas de enlace).- Son también utilizadas para interconexión de redes, pero esta puede ser a través de hardware o software por medio de protocolos como el TCP/IP para que identifique la ruta de conexión con otra red.

Fig.1.20 Gateways

Contrafuegos (Firewall).- Es un dispositivo diseñado para realizar encaminamientos de redes, con la diferencia es que este aparato principalmente protege las redes de ataques de virus o agentes ajenos a la red.

Fig.1.21 Contrafuegos

En la actualidad la tecnología inalámbrica esta tomando fuerza, por lo que para este tipo de conexión se cuentan con dispositivos llamados **Access Point (Punto de Acceso) o Ruteador Inalámbrico**, su función es distribuir la señal de conexión en una red de área local o ancha.

Fig.1.22 Ruteador inalámbrico

Los cables utilizados para cualquier conexión en los hubs, switch, access point, etc., actualmente son:

Par trenzado: es un cable con un número de conductores de cobre que van en pares; los más comunes son de 2, 3, 4 pares.

Fig.1.23 Par trenzado

Fibra óptica: que es un cable que cuenta con conductores de fibra de vidrio los cuales conduce la información a través de un haz de luz, lo que aumenta la confiabilidad y velocidad en que los datos son transportados.

Fig.1.24 Fibra Óptica

Cable Coaxial: aunque ya no es muy utilizado en redes de computadoras, consiste en un conductor central de cobre recubierto con una malla que permite la continuidad de la conexión y el flujo de los datos.

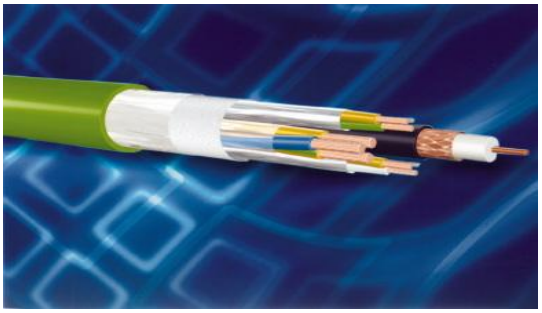


Fig.1.25 Cable coaxial

Estos elementos son con los que una red toma forma, en la figura 1.26 veremos un esquema de una red sencilla con conexión a Internet.

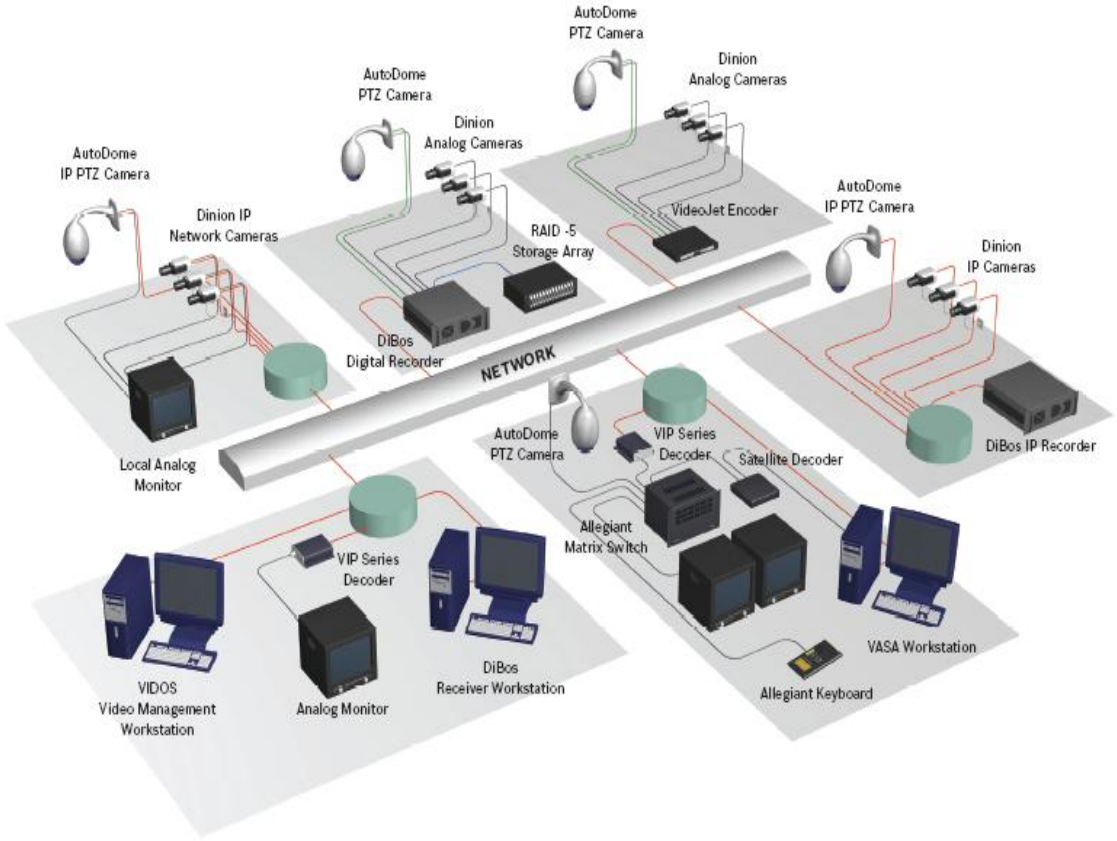


Fig.1.26 Esquema de una red

1.4.4 PROTOCOLOS

Los protocolos dentro del ámbito de red, son el conjunto de normas, reglas que se van a utilizar para el intercambio de los datos entre los equipos de una red. Es decir, que para que esto suceda es como darles un idioma para que se entiendan y puedan realizar la comunicación entre si.

No hay un solo protocolo y pueden residir diferentes protocolos en el mismo equipo sin que colisionen entre si. Los adaptadores de red son los encargados de recibir e identificar para llevarlos a su procesamiento en la computadora, existen varios tipos:

1.4.4.1 Protocolos de transporte

- ATP (Apple Talk Transición Protocol)
- NETBios (Network Basic Input/Output System)
- TCP (Transmission Control Protocol)

1.4.4.2 Protocolos de Red

- DDP (Delivery Datagram Protocol).
- IP (Internet Protocol)
- IPX (Internet Protocol Exchange)
- NetBEUI (Network Basic Extended User Interface)

1.4.4.3 Protocolos de Aplicación

- AFP (Apple File Protocol)
- FTP (File Transfer Protocol)
- HTTP (HyperText Trasfer Protocol)

1.4.5 PROTOCOLO TCP/IP

Dado el gran avance tecnológico en redes se han realizado diversos protocolos entre todos el que mas utilizado es el TCP/IP que proporciona comunicación y transporte de datos en las redes, es una agrupación de más de 100 protocolos conjuntos. Sus siglas significan Transmission Control Protocolo / Internet Protocol. Su más común uso es para comunicar en red computadoras con distintos sistemas operativos, por ejemplo UNIX, Windows, MAC OS, entre muchos.

Transmission Control Protocol (TCP) es un conjunto de programas que trabaja en el nivel de transporte, encargado de que la información llegue a su destino, es decir que lo que se envía sea lo que se recibe. Se interrumpirá si hay algún error que evite que la información sea fiable.

El **Protocolo de Internet (IP)** es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos.

Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, ésta es proporcionada por los protocolos de la capa de transporte, como TCP.

TCP/IP nos ofrece a nivel de aplicación servicios que utilizamos en la actualidad ya como parte de nuestra vida diaria como son:

- www o Servidor web: con la cual podemos tener nuestra página web publicada en internet
- Mail: conocido mejor como correo electrónico mediante los servicios
- Servidor para transferencia de archivos o servidor FTP

1.4.6 DIRECCIÓN IP

IP significa “Internet Protocol” y es un número que identifica un dispositivo en una red (un ordenador, una impresora, un router, etc…). Estos dispositivos al formar parte de una red serán identificados mediante un número IP único en esa red. La dirección IP está formada por 4 números de hasta 3 cifras separados por “.” (punto).

Los valores que pueden tomar estos números varían entre 0 y 255, por ejemplo, una dirección IP puede ser 192.168.66.254 (cuatro números entre 0 y 255 separados por puntos).

1.4.6.1 IP Pública

Se denomina IP pública a aquella dirección IP que es visible desde Internet. Suele ser la que tiene un router o modem. Es la que da “la cara” a Internet. Esta IP suele ser proporcionada por un ISP (empresa que da acceso a Internet: Ecuanet, Interactive, Easynet, etc).

1.4.6.2 IP Privada

La dirección IP privada es aquella que pertenece a una red privada. Suele ser la IP de la tarjeta de red del ordenador, de una impresora de red, del router de la red, etc.

En la figura 1.27 visualizamos la configuración de una red interna formada por 4 elementos: 1 router de acceso a Internet, 2 equipos y 1 impresora.

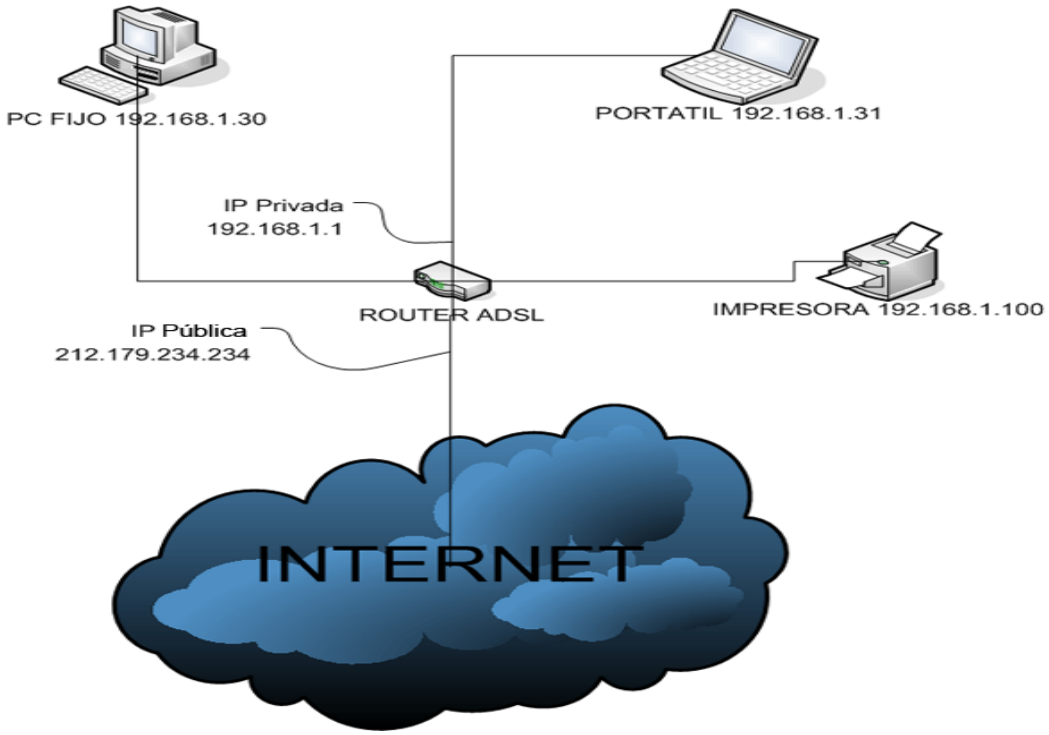


Fig.1.27 Red interna

1.4.6.3 Direciones IPv4

En su versión 6.55, una **dirección IP** se implementa con un número de 32 bits que suele ser mostrado en cuatro grupos de números decimales de 8 bits (IPv4). Cada uno de esos números se mueve en un rango de 0 a 255 (expresado en decimal), o de 0 a FF (en hexadecimal) o de 0 a 11111111 (en binario). Las *direcciones IP* se pueden expresar como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto

puede ser entre 0 y 255 (el número binario de 8 bits más alto es 11111111 y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255 en total).

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter ".". Cada uno de estos octetos puede estar comprendido entre 0 y 255, salvo algunas excepciones. Los ceros iniciales, si los hubiera, se pueden obviar. Ejemplo de representación de dirección IPv4: *164.12.123.65*

Hay tres clases de direcciones IP que una organización puede recibir de parte de la Internet Corporation for Assigned Names and Numbers (ICANN): clase A, clase B y clase C.

En la actualidad, ICANN reserva las direcciones de clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura como, por ejemplo, Hewlett Packard) y las direcciones de clase B para las medianas empresas. Se otorgan direcciones de clase C para todos los demás solicitantes. Cada clase de red permite una cantidad fija de equipos (hosts).

Cabe resaltar los siguientes aspectos:

- La dirección 0.0.0.0 es utilizada por las máquinas cuando están arrancando o no se les ha asignado dirección.
- La dirección que tiene su parte de host a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.
- La dirección que tiene su parte de host a unos sirve para comunicar con todos los hosts de la red en la que se ubica. Se denomina dirección de broadcast.
- Las direcciones 127.x.x.x se reservan para pruebas de retroalimentación. Se denomina dirección de bucle local o loopback.

1.4.6.4 Direciones IPv6

La función de la dirección IPv6 es exactamente la misma a su predecesor IPv4, pero dentro del protocolo IPv6. Está compuesta por 8 segmentos de 2 bytes cada uno, que suman un total de 128 bits, el equivalente a unos $3.4x10^{38}$ hosts direccionables. La ventaja con respecto a la dirección IPv4 es obvia en cuanto a su capacidad de direccionamiento.

1.5 VIDEOVIGILANCIA

En la actualidad, una de las tendencias más destacadas en la industria de la seguridad es el cambio evolutivo desde las primeras tecnologías de video vigilancia usados hace algunos años hacia los sistemas basados en red. Este cambio de los antiguos dispositivos analógicos por equipos digitales nuevos brinda una gran cantidad de beneficios económicos y funcionales para las instituciones que necesitan ofrecer una mejor protección, tanto a su personal como a sus bienes.

Gracias a la utilización de los avances en los microprocesadores y otras tecnologías, el monitoreo, la grabación y el análisis de las imágenes de video son aspectos que están a disposición del personal encargado de seguridad siempre que lo requieran. Las cámaras de alta calidad ahora pueden conectarse en cualquier lugar donde haya un puerto disponible, y los usuarios disfrutar así de la flexibilidad y administración de los sistemas informáticos y telefónicos actuales. También se puede acceder a los videos en vivo y los que ya están grabados desde cualquier computador que esté conectado a una red LAN o a Internet usando tecnologías ya conocidas, como Ethernet e IP.

1.5.1 VIDEOVIGILANCIA IP

El vídeo IP, a menudo conocido como vigilancia IP para determinadas aplicaciones en el ámbito de la vigilancia en seguridad y la monitorización remota,

es un sistema que ofrece a los usuarios la posibilidad de controlar y grabar en vídeo a través de una red IP (LAN/WAN/Internet).

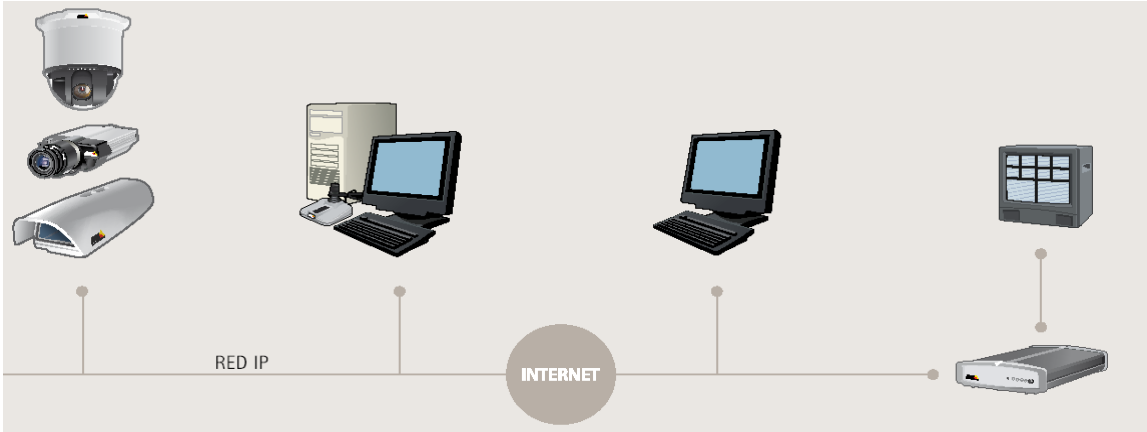


Fig.1.28 Sistema de Videovigilancia IP

1.5.1.1 Red LAN IP

A diferencia de los sistemas de vídeo analógicos, el vídeo IP no precisa cableado, ya que utiliza la red para transmitir la información. El término vídeo IP hace referencia tanto a las fuentes de vídeo como de audio disponibles a través del sistema. En una aplicación de vídeo en red, las secuencias de vídeo digitalizado se transmiten a cualquier punto del mundo a través de una red IP con cables o inalámbrica, permitiendo la monitoreo y grabación por vídeo desde cualquier lugar de la red.

El vídeo IP puede utilizarse en un número ilimitado de situaciones; no obstante, la mayoría de aplicaciones se incluyen en una de las dos categorías siguientes:

1.5.1.2 Vigilancia y seguridad

La avanzada funcionalidad del vídeo IP lo convierte en un medio muy adecuado para las aplicaciones relacionadas con la vídeo vigilancia y seguridad. La flexibilidad de la tecnología digital permite al personal de seguridad proteger mejor a las personas, las propiedades y los bienes. Por tanto, dichos sistemas

constituyen una opción especialmente interesante para las instituciones que en la actualidad están utilizando los sistemas CCTV[16] existentes.

1.5.1.3 Monitorización remota

El vídeo IP permite a los usuarios la posibilidad de reunir información en todos los puntos clave de una operación y visualizarla en tiempo real, lo que la convierte en la tecnología perfecta para la monitorización remota y local de equipos, personas y lugares. Ejemplos de aplicación son la monitorización del tráfico y de líneas de producción y la monitorización de múltiples sectores.

Los principales mercados donde los sistemas de vídeo IP se han instalado satisfactoriamente son educación, transporte, banca, gobierno, comercios minoristas e industrial.

1.6 SISTEMA DE VIDEOVIGILANCIA A TRAVÉS DE IP

Los edificios se encuentran con una serie de problemáticas particulares a la hora de cubrir los aspectos de seguridad. El uso de sistemas de vídeo ha demostrado su capacidad para reducir el número de acciones delictivas y criminales en establecimientos y lugares públicos. Las posibilidades que en este sentido puede ofrecer el vídeo IP y las soluciones de Vigilancia IP mejoran las capacidades de las instalaciones de CCTV existentes y las dota de nuevas e interesantes funcionalidades.

Como principales elementos diferenciadores entre los sistemas analógicos de CCTV y los sistemas IP tenemos que las cámaras IP y los servidores de vídeo incorporan procesadores, sistemas operativos y servidores Web que aumentan la inteligencia del sistema de vídeo vigilancia y su capacidad de procesamiento. Las cámaras IP y los servidores de vídeo digitales se conectan directamente a la red Ethernet y no precisan ningún otro elemento o software para funcionar. Siendo

[16] **CCTV:** Circuito Cerrado de Televisión.

muy importante ya que esto hace que bajo ciertas condiciones y en determinadas circunstancias preestablecidas, los dispositivos de vídeo IP sean capaces de tomar decisiones.

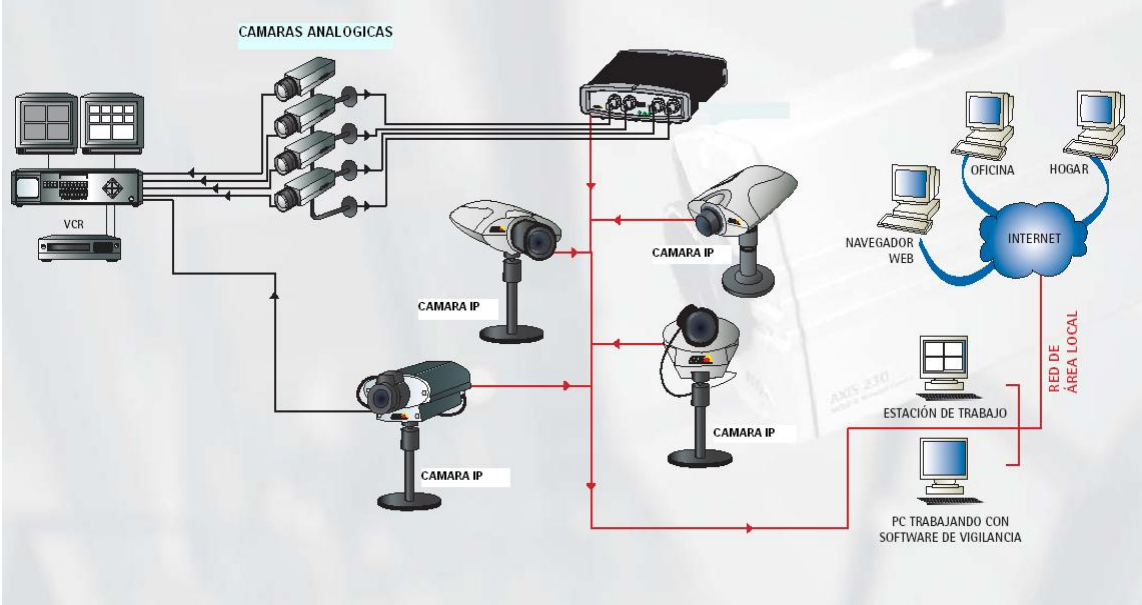


FIG.1.29 Sistema analógico vs. Sistema IP

En este sentido también cabe destacar que otro de los principales beneficios que aportan las soluciones de vídeo en red es que las cámaras IP proporcionan una calidad de imagen superior y constante. Que la calidad de las imágenes sea mayor representa los siguientes beneficios de cara a los usuarios.

- Mejoras en el seguimiento de detalles y en los cambios en las imágenes, permitiendo una toma de decisiones más rápida y mejor en lo relacionado con la seguridad de propiedades y personas.
- Mejoras en el análisis automatizado y en el uso de herramientas de alarma, como el reconocimiento de caras, reduciendo el número de falsos positivos.

Frente a las tradicionales cámaras analógicas, las cámaras de red están equipadas con capacidad de procesamiento, no solo para capturar y presentar las imágenes, sino también para gestionarlas digitalmente y comprimirlas para su transporte a través de la red. La calidad de las imágenes puede variar

considerablemente y depende de la elección de la óptica y del sensor de imagen, de la capacidad de proceso disponible y del nivel de sofisticación de los algoritmos del chip de procesamiento de imágenes. Además las cámaras de red ofrecen las imágenes digitales en los formatos de compresión estándares más avanzados y de mayor calidad: Motion JPEG, MPEG-2 y MPEG-4.

Los sistemas de vídeo IP están basados en estándares abiertos. Esto provoca varios beneficios fundamentales para los usuarios: por una parte aseguran la independencia de los fabricantes de equipamiento (ya no es preciso depender de un único proveedor), por otra aseguran la capacidad de integración de estos sistemas con el resto de subsistemas del edificio en cuestión (control de accesos, iluminación, anti-incendios, calefacción, etc.), y finalmente hace que estos sistemas estén preparados para cualquier potencial mejora que pueda darse en el continuo desarrollo tecnológico. Esta integración de los sistemas hace que aumenten los niveles de seguridad, el ahorro en el mantenimiento y control del edificio y también el nivel de confort de las instalaciones.

Los sistemas de CCTV analógico están basados en cableados coaxiales y en monitores dedicados con lo que las instalaciones resultan “rígidas” y cualquier modificación en su estructura o cualquier cambio resulta complicado de acometer. Además estos sistemas analógicos dependen de “matrices de conmutación” que, en ocasiones en las que es preciso incorporar otra matriz, no permiten la adición sencilla de nuevos dispositivos, además de resultar poco económico.

Por el contrario los dispositivos de vigilancia IP resultan extremadamente flexibles. En lo relacionado con la ubicación de los dispositivos ofrecen muchas opciones entre las que se incluyen las cámaras IP inalámbricas y la posibilidad de hacer llegar a las cámaras la energía eléctrica a través del cable de red (Power over Ethernet). Finalmente los sistemas de vídeo IP resultan ilimitados en cuanto a cantidad de dispositivos que se pueden ir incorporando al sistema de uno en uno y en función de las necesidades.

El uso de sistemas de vídeo IP aumenta el nivel de movilidad de los vigilantes. Ya no es necesario que estén físicamente localizados en el centro de control ya que los dispositivos de vídeo IP permiten acceso remoto y son capaces de transmitir las imágenes a dispositivos móviles e inalámbricos (PDA, laptop, teléfono móvil). Esta circunstancia hace que el centro de control de los edificios alcance la movilidad y pueda ir allá donde estén los vigilantes o incluso a centrales receptoras externas a través de Internet.

Los sistemas de vídeo IP incorporan funciones de grabación y usan discos duros convencionales para el almacenamiento de las imágenes. Hay dos beneficios principales derivados de esta circunstancia. Por una parte que la información esté almacenada en formato digital supone que es mucho más rápida y sencilla su localización usando mecanismos de búsqueda avanzados y, por otra parte, que el almacenamiento se realiza a través de la red y por tanto no es imprescindible que se lleve a cabo allí donde esté el sistema sino que por razones de seguridad o conveniencia estas grabaciones se pueden llevar a cabo en lugares remotos.

Como hemos podido apreciar a lo largo del presente capítulo son numerosos los beneficios que aporta el uso de sistemas de vídeo IP a los edificios respecto al uso de sistemas de CCTV analógico.

II. CAPITULO

ANÁLISIS Y DISEÑO DEL SISTEMA

2.1 INTRODUCCIÓN

La llegada de la tecnología IP ha dado un gran avance al terreno de la videovigilancia que se encontraba estancado en la era analógica.

La videovigilancia IP trae consigo una serie de ventajas muy a tener en cuenta, así pues, podemos destacar aspectos tan importantes como el acceso al vídeo desde cualquier lugar y en el momento en que se desee. Esto es posible gracias a que los archivos se almacenan en ubicaciones remotas por diversos motivos, a las que se puede llegar por Internet o mediante una red de área local.

Por otra parte, existe el hecho del ahorro de costos. Esto es porque se trata de una tecnología que requiere una inversión inicial menor que si optáramos por una solución tradicional. Y es que no hay necesidad de utilizar una estructura cableada, pudiendo incluso aprovechar los equipos informáticos que la organización ya tiene. Además, los elementos necesarios para poner en marcha una red de videovigilancia IP son menores, lo que implica el consiguiente ahorro de costos.

Adicionalmente, las opciones de utilización que nos ofrecen estos equipos son mayores ya que al no estar sujetas a cables hace posible colocar las cámaras en lugares hasta hace poco inaccesibles y que ofrecerán al usuario mejor visión de aquello que se quiere grabar. Asimismo, las posibilidades de hacer crecer las instalaciones son mucho mayores y más sencillas.

2.1.1 PLANTEAMIENTO DEL PROBLEMA

Durante el levantamiento de información se pudo constatar que en el edificio no existe conexión de Red para las dependencias que allí funcionan, por otro lado, existen dependencias que aún cuando cuentan con computadores algunos de estos no cumplen con los requerimientos mínimos de hardware y software para ser conectados a la red,

En función de cubrir a las distintas dependencias del HB-11 “GALAPAGOS”, planteamos el diseño de un sistema de seguridad basado en IP que abarque todas las zonas comprendidas dentro del área de seguridad que estableceremos para este efecto.

Con la realización de este proyecto, se pretende diseñar un sistema de vigilancia con el que se podrá brindar un ambiente más cómodo y seguro tanto para el personal que labora como para los usuarios (militares y civiles) de los servicios que presta el HB-11 “GALAPAGOS”.

Este sistema abrirá una nueva perspectiva dentro de la seguridad y control institucional. Con él se podrán controlar las actividades desarrolladas por el personal del hospital, la calidad del servicio prestado así como los materiales y equipos existentes dentro del edificio. Todo el sistema ha sido diseñado para facilitar la comunicación con su entorno, otorgándole al usuario (Director, Oficial o Clase de guardia) ojos y oídos de largo alcance.

2.1.2 OBJETIVOS

2.1.2.1 General

Realizar el estudio y diseño del Sistema de Seguridad por Videovigilancia IP para el HOSPITAL DE BRIGADA No. 11 ¨GALAPAGOS¨.

2.1.2.2 Específicos

- Consultar al Sr. Oficial de Operaciones (P-3) acerca del personal militar disponible para realizar el servicio de guardia.
- Realizar encuestas al personal que cumple funciones de Oficial y Subalterno de guardia, sobre los grupos de guardia y los diferentes puestos a cubrirse ya sea con centinelas fijos o móviles.
- Estudiar las necesidades de interconexión que presenta el edificio del HB-11 "GALAPAGOS" y los beneficios que esto podría aportar.
- Con la ayuda del plano del edificio esquematizar el cableado a instalarse.
- Identificar físicamente los lugares del edificio donde se requiere puntos de vigilancia.
- Determinar los dispositivos de interconexión que serán necesarios para el diseño de la red.
- Identificar la ubicación que deberán tener los dispositivos de interconexión
- Diseñar el cableado estructurado para el edificio.
- Ubicar en el edificio un sitio estratégico donde podría funcionar el Cuarto de Comunicaciones y el Cuarto de Equipos.
- Estudiar la cobertura en las distintas áreas.
- Priorizar cada área de acuerdo a su vulnerabilidad y al material existente en cada una de ellas.
- Definir el Sistema Operativo que se va a utilizar.
- Instruir al personal que va a hacer uso del sistema.

2.1.3 FACTIBILIDAD

El estudio de factibilidad requerido para efectos de diseño del Sistema de Seguridad por Videovigilancia, se basa en tres aspectos o niveles: técnico, económico y operativo.

A continuación, evaluaremos cada una de estas factibilidades por separado:

2.1.3.1 Factibilidad Técnica

Hay que destacar que nuestro sistema básicamente será diseñado como una red LAN, por lo tanto desde el punto de vista técnico es realizable, ya que están a la disposición en el mercado los diferentes equipos y dispositivos que darán soporte al diseño y posterior implementación del sistema.

Además existe en la actualidad el personal técnico capacitado para manejar los equipos que requerirá el sistema, éstos corresponden al personal de especialistas (informáticos o electrónicos) y/o al personal del arma de Comunicaciones, cuyo perfil profesional los hace aptos para desempeñar esta función.

El hecho de contar con ese personal disponible en el orgánico del HB-11 “GALAPAGOS” implica que no será necesaria la contratación de personal externo, lo que evitará un gasto adicional.

2.1.3.2 Factibilidad Económica

El costo que genera el diseño del sistema que proponemos es bajo, ya que la tecnología ha emplearse al utilizar equipo más costoso que el tradicional en contrapropuesta nos presenta un significativo ahorro en lo que ha cableado se refiere.

Por otro lado tomando en cuenta que en tecnología la calidad es proporcional al precio, se establecerán las características de los mejores equipos que se ajusten al presupuesto asignado.

En función de estos aspectos y de los beneficios que aportaría esta red, consideramos que el proyecto es, económicamente factible.

2.1.3.3 Factibilidad Operacional

El levantamiento de información realizado determinó que, en el HB-11 “GALAPAGOS” un sistema de vigilancia solucionaría múltiples inconvenientes que en la actualidad se presentan como son la falta de personal para cubrir los puestos de guardia o la dificultad que tiene el personal de guardia para cumplir sus funciones en condiciones adversas (oscuridad, lluvia, etc.) sobre todo en exteriores.

Este sistema al ser explotado en toda su capacidad y operado por personal idóneo garantiza un nivel altamente confiable de seguridad con uso mínimo de personal, lo que lo hace altamente operativo.

2.2 ANÁLISIS DEL SISTEMA

En la actualidad, los sistemas de vídeo ya no se limitan a una función de grabación y almacenamiento de enormes volúmenes de información de forma pasiva (la mayoría de la cual es inútil). En realidad, pueden evaluar una situación y consecuentemente tomar las medidas oportunas.

Con todas estas nuevas capacidades y los muchos métodos que se encuentran disponibles para gestionar el vídeo, es de suma importancia considerar cuáles son las necesidades de aplicación y el nivel de funcionalidad.

Tras haber realizado una evaluación de las necesidades, deberían tenerse en cuenta un número de factores para establecer un sistema que saque el máximo provecho del vídeo IP.

Dichos factores se tratan a continuación.

2.2.1 ANCHO DE BANDA

El ancho de banda utilizado por los equipos de videovigilancia depende de la configuración de éstos. Por ejemplo, el uso de ancho de banda de una cámara depende de factores tales como:

- El tamaño de la imagen
- La compresión
- La frecuencia de imagen por segundo
- La complejidad de la imagen

Hay varias formas de aprovechar al máximo el sistema de vigilancia IP y administrar el consumo de ancho de banda, entre ellas se incluyen las siguientes técnicas:

Conmutación de redes: Mediante la conmutación de redes (una técnica de conexión utilizada con frecuencia hoy en día) puede dividirse un ordenador y una red de vigilancia IP físicos en dos redes lógicas autónomas. Las redes siguen conectadas físicamente, pero el conmutador de red las divide lógicamente en dos redes virtuales independientes.

Redes más rápidas: El precio de los conmutadores y enrutadores baja constantemente, por lo que las redes con capacidad para gigabytes son cada día más asequibles. Al reducir el efecto de la limitación del ancho de banda, las redes más rápidas aumentan el valor potencial de la vigilancia remota sobre red.

Frecuencia de imagen condicionada a sucesos: En la mayoría de las aplicaciones no es necesario disponer de 30 imágenes por segundo (ips) en todo momento en todas las cámaras. Las posibilidades de configuración y los sistemas inteligentes incorporados a las cámaras de red o el servidor de vídeo permiten establecer frecuencias de imagen menores (por ejemplo, 1-3 ips), reduciendo drásticamente el consumo de ancho de banda.

En caso de alarma, si está activada la detección de movimiento, la frecuencia de imagen de la grabación puede aumentarse automáticamente hasta un nivel superior. En la mayoría de los casos, la cámara sólo enviará vídeo a través de la red si merece la pena grabar las imágenes, lo que por regla general únicamente supone el 10% del tiempo. El 90% restante no se transmite nada a través de la red.

2.2.2 ALMACENAMIENTO

La aparición de sistemas de vídeo IP exige un uso incrementado del almacenamiento en disco duro. Esto plantea un número de preguntas que van desde que capacidad de disco duro es necesario hasta cómo crear un almacenamiento en el disco duro a prueba de errores.

2.2.2.1 Espacio necesario en disco duro

Los factores que deberán tenerse en cuenta al calcular las necesidades de almacenamiento son los siguientes:

- El número de cámaras
- El número de horas por día en que la cámara estará grabando
- Durante cuánto tiempo deberán guardarse los datos
- Detección de movimiento (Evento) únicamente o grabación contínua
- Otros parámetros tales como velocidad de imagen, compresión, calidad de la imagen y complejidad

2.2.2.2 JPEG/Motion JPEG

Para JPEG/Motion JPEG donde se reciben archivos únicos, los requisitos de almacenamiento variarán cambiando la velocidad de imagen, la resolución y la

compresión. Las cámaras 1, 2 y 3 de la tabla 2.1 poseen requisitos de almacenamiento distintos según sus ips y los parámetros de resolución.

Cálculo: Tamaño de la imagen x imágenes por segundo x 3.600 seg. = 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.

Tabla 2.1 Espacio en disco duro necesario para formato JPEG

Cámara	Resolución	Tamaño de la imagen (KB)	Imágenes por segundo	MB por hora	Horas de funcionamiento	GB por 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

2.2.2.3 MPEG-4

En MPEG-4, las imágenes se reciben en una transmisión continua de datos y no en archivos individuales. Es la tasa de bits (que mide la cantidad de datos de vídeo transmitidos) la que determina los correspondientes requisitos de almacenamiento. La tasa de bits es el resultado de una velocidad de imagen, resolución y compresión específicas, así como del nivel de movimiento en la escena. En la tabla 2.2 podemos ver un ejemplo en el caso de tres cámaras de características distintas.

Cálculo: Tasa de bits / 8 (bits en un byte) x 3.600 seg. = 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.

Tabla 2.2 Espacio en disco duro necesario para formato MPEG-4

Cámara	Resolución	Bit Rate (kBit/s)	Imágen por segundo	MB por hora	Horas de funcionamiento	GB por 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

2.2.3 REDUNDANCIA

2.2.3.1 El disco duro RAID[17]

Es básicamente un método para extender los datos sobre múltiples unidades de disco duro con suficientes datos redundantes en todos los discos a fin de que puedan recuperarse de los discos restantes en caso de avería de la unidad.

Fig.2.1 Unidad RAID

2.2.3.2 La replicación de los datos

Es una característica común de muchos sistemas operativos de la red, los servidores de archivos en la red están configurados para replicar datos entre sí.

[17] **RAID:** Matriz redundante de discos independientes

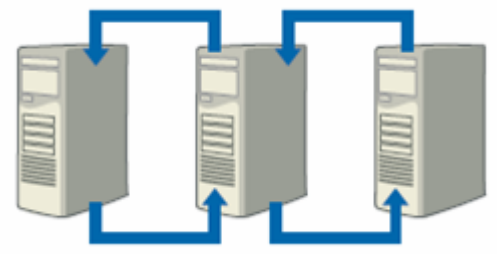


Fig.2.2 Replicación de datos

2.2.3.3 Realizar copias de seguridad en cinta

Es un método alternativo o complementario. Existen diversos equipos de hardware y software disponibles en el mercado y las políticas de copia de seguridad normalmente incluyen sacar las cintas del lugar habitual como medida preventiva en caso de incendio o robo.

2.2.3.4 Agrupamientos de los servidores

Existen muchos métodos de agrupamiento de los servidores. Uno de los más habituales en los servidores de bases de datos y de correo electrónico es cuando dos servidores funcionan con el mismo dispositivo de almacenamiento, normalmente un dispositivo RAID, cuando un servidor sufre una avería, el otro (que está idénticamente configurado) se hace cargo de la aplicación (normalmente, estos servidores incluso comparten la misma dirección IP), haciendo que la llamada conmutación por error se convierta en totalmente transparente para el usuario.

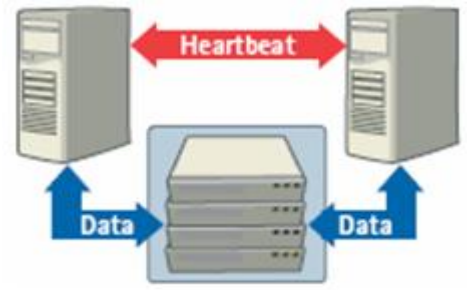


Fig.2.3 Agrupamiento de servidores

2.2.3.5 Múltiples destinatarios de vídeo

Es un método habitual para garantizar una recuperación de desastres y un almacenamiento fuera de la instalación habitual en el vídeo IP es el envío simultáneo del vídeo a dos servidores distintos que se encuentran en emplazamientos diferentes. Evidentemente, estos servidores pueden a su vez estar equipados con RAID, funcionar en agrupamientos o replicar sus datos con servidores que incluso se encuentren mucho más lejos.

2.2.4 ESCALABILIDAD DEL SISTEMA

La escalabilidad varía en función del tipo de sistema elegido y, por tanto, debe tenerse en cuenta durante la fase de diseño de un sistema de vídeo.

2.2.4.1 Etapas de la escalabilidad

Un sistema DVR normalmente se suministra con 4, 9 ó 16 entradas de cámara, por tanto, se convierte en escalable en incrementos de 4, 9 ó 16. Si un sistema incluye 15 cámaras, no supone ninguna desventaja, pero sí que se convierte en un problema si son necesarias 17 cámaras. Añadir una única cámara generaría la necesidad de un DVR complementario. Los sistemas de vídeo IP son mucho más flexibles y pueden ampliarse en incrementos de una cámara a la vez.

2.2.4.2 Número de cámaras por grabador

En un sistema de vídeo IP, un servidor de PC graba y gestiona el vídeo. El servidor de PC puede seleccionarse en función del rendimiento necesario. A menudo, el rendimiento se especifica como el número total de imágenes por segundo del sistema. Si se necesitan 30 ips para cada cámara, un servidor sólo puede grabar 25 cámaras. Si son suficientes 2 ips, 300 cámaras pueden ser gestionadas a través de un servidor. Esto significa que el rendimiento del sistema se usa de forma eficiente y puede optimizarse.

2.2.4.3 Tamaño del sistema

Para instalaciones más grandes, un sistema de vídeo IP es fácil de ampliar. Cuando se necesitan velocidades de imagen de grabación mayores o tiempos de grabación superiores, podrá añadirse más capacidad de procesamiento y/o memoria al servidor de PC que gestiona el vídeo. O bien, aún más sencillo, puede añadirse otro servidor de PC situado en una ubicación central o en ubicaciones remotas.

2.2.5 CONTROL DE LA VELOCIDAD DE IMAGEN

El vídeo IP permite el control de la velocidad de imagen, a diferencia del vídeo analógico donde todo el vídeo se transmite desde la cámara de forma permanente. El control de la velocidad de imagen en los sistemas de vídeo IP significa que el servidor de vídeo/cámara IP únicamente envía imágenes a la velocidad de imagen especificada, sin tener que transferir vídeo innecesario a través de la red.

El servidor de vídeo/cámara de red o el software de aplicación de vídeo puede configurarse para elevar esta velocidad de imagen si, por ejemplo se detecta actividad. En la figura 2.4 podemos comparar la velocidad de imagen de un sistema analógico y un sistema IP.

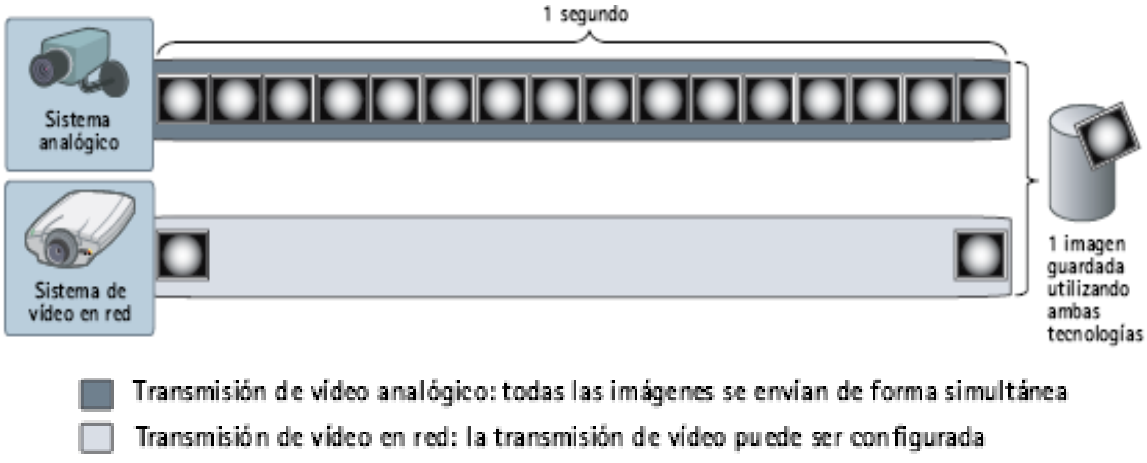


Fig.2.4 Velocidad de imagen

También es posible enviar vídeo con velocidades de imagen distintas a destinatarios diferentes, lo que supone una ventaja especialmente en aquellos casos en que se utilizan enlaces de ancho de banda mínimos para ubicaciones remotas, podemos observar este método en la figura 2.5.

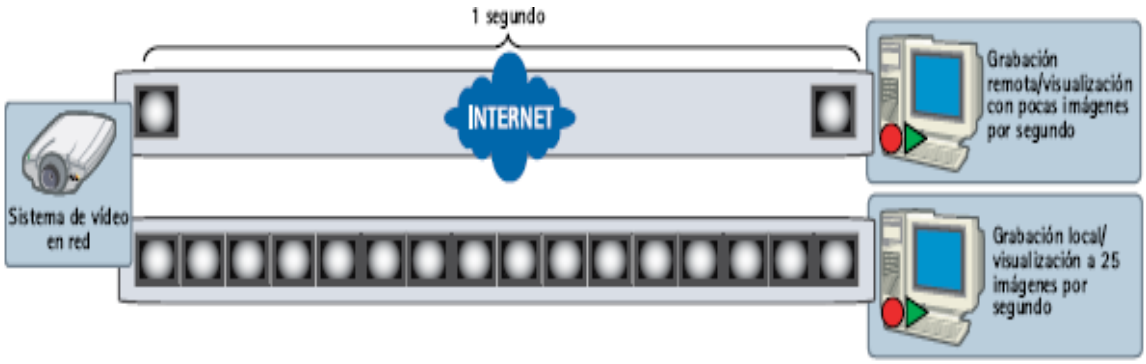


Fig.2.5 Visualización por número de ips

2.2.6 CONSIDERACIONES DE ALMACENAMIENTO

2.2.6.1 Soluciones de disco duro distintas

Existen dos formas de enfocar el almacenamiento en disco duro, una es tener el almacenamiento asociado al servidor real que ejecuta la aplicación, la otra es una solución de almacenamiento individual donde el almacenamiento se encuentra separado del servidor que ejecuta la aplicación.

2.2.6.2 Almacenamiento Directamente Conectado (Direct attached storage)

Probablemente esta es la solución más habitual para el almacenamiento en discos duros en instalaciones de tamaño medio y pequeño. El disco duro se encuentra en el mismo PC que ejecuta el software de gestión de vídeo (servidor de aplicación). La disponibilidad de espacio viene determinada por el PC y el número de discos duros que puede admitir. La mayoría de ordenadores pueden incluir 2 discos y algunos hasta 4. Cada disco puede almacenar 300 Gbytes

aproximadamente, lo que supone una capacidad de disco duro total aproximada de 1,2 Tbytes.

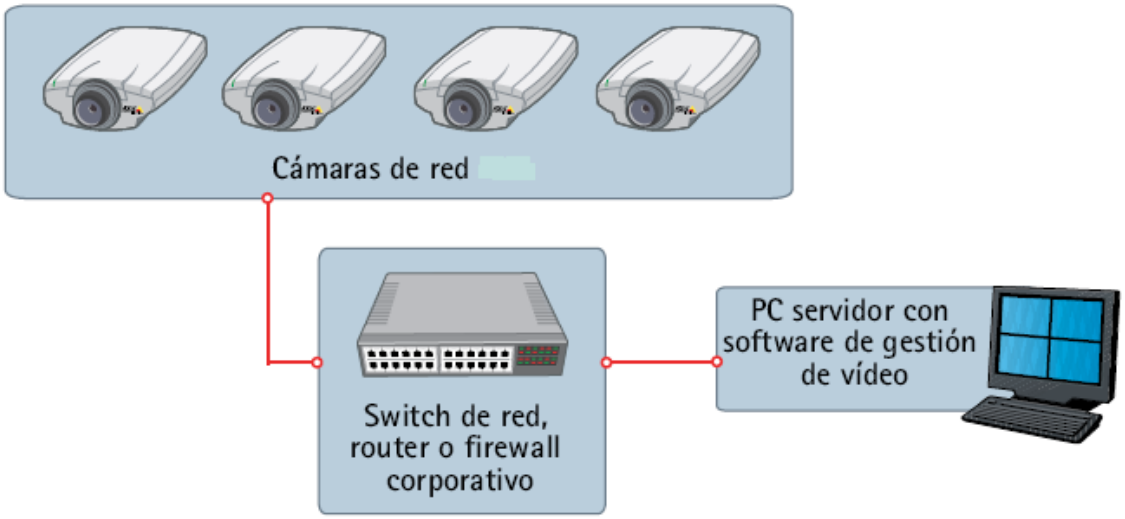


Fig.2.6 Almacenamiento Directamente Conectado

2.2.6.3 Almacenamiento NAS (Network Attached Storage) y SAN (Storage Area Network)

En las aplicaciones donde la cantidad de datos almacenados y los requisitos de gestión superen los límites de almacenamiento directamente conectado, se utiliza un sistema de almacenamiento separado. Estos sistemas son el almacenamiento NAS y SAN.

NAS: El Almacenamiento NAS ofrece un dispositivo único de almacenamiento que se conecta directamente a una LAN y permite un almacenamiento compartido a todos los clientes de la red. Un dispositivo NAS es fácil de instalar y gestionar, ofreciendo una solución económica para los requisitos de almacenamiento, pero un caudal limitado para los datos entrantes.

SAN: Las redes de almacenamiento SAN son unas redes especiales de alta velocidad para almacenamiento, conectadas por fibra a uno o más servidores. Los usuarios pueden acceder a cualquiera de los dispositivos de almacenamiento en

SAN a través de los servidores y el almacenamiento es escalable a cientos de Tbytes. El almacenamiento centralizado de datos reduce la administración exigida y ofrece un conjunto de almacenamiento flexible de alto rendimiento para ser utilizado por entornos de multiservidores.

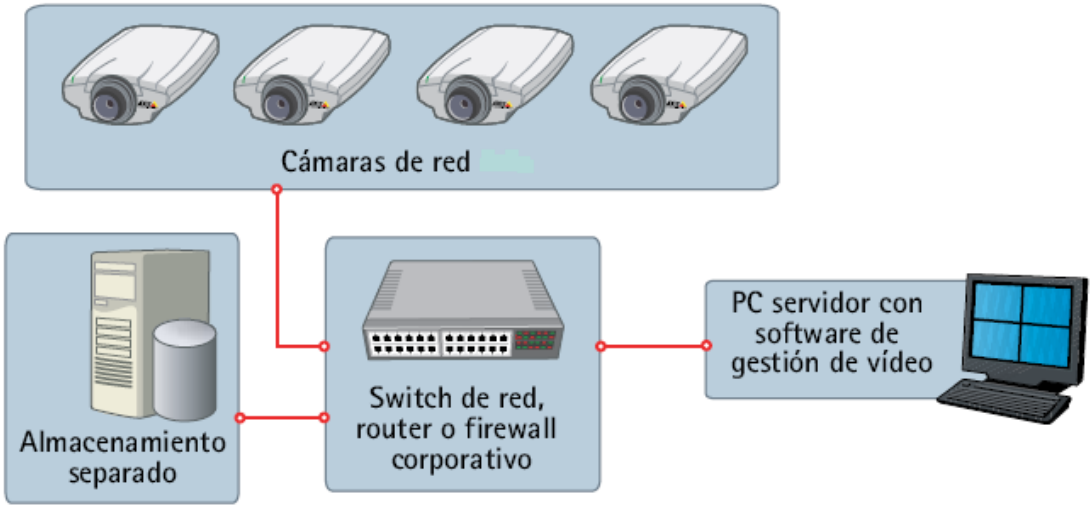


Fig.2.7 Almacenamiento NAS

La diferencia entre los dos es que NAS es un dispositivo de almacenamiento donde el archivo entero se almacena en un único disco duro, mientras que SAN consiste en un número de dispositivos donde el archivo puede almacenarse por bloques en múltiples discos duros.

Este tipo de configuración de discos duros permite disponer de soluciones de gran capacidad y escalables que pueden almacenar grandes cantidades de datos con un alto nivel de redundancia. Hay soluciones de ambos tipos disponibles para el software de gestión de vídeo.

2.2.6.4 RAID (Matriz redundante de discos independientes)

RAID es un método de distribución de varios discos duros estándar que, ante el sistema operativo funcionan como una gran unidad lógica.

Hay distintos niveles de RAID que ofrecen niveles de redundancia diferentes, desde prácticamente ninguna redundancia hasta una solución completa de duplicación de discos “intercambiables en caliente” donde no existe una interrupción del funcionamiento del sistema ni pérdida de datos en caso de una avería del disco duro.

Tabla 2.3 Niveles de RAID más habituales

Nivel RAID	Características
RAID-0	Los datos se reparten a través de dos o varios discos duros, para mejorar la velocidad de lectura/grabación pero sin redundancia.
RAID-1	También conocido como „disk mirroring“ (duplicación de discos). Como mínimo dos discos duplican los datos. Sin entrelazado de bloques. Ambos discos pueden leerse a la vez. Rendimiento de grabación como en el almacenamiento único de discos.
RAID-5	Incluye una matriz de paridad giratoria que permite que todas las funciones de lectura y escritura se superpongan. Almacena información de paridad para la reconstrucción de los datos perdidos.

2.2.7 TECNOLOGÍAS DE RED IP

Hoy en día, el protocolo de Internet (IP) constituye el protocolo de comunicación informática más ampliamente utilizado. Es el protocolo básico empleado para la comunicación por Internet, como el correo electrónico, web y multimedia. Una de las razones de la aceptación de este protocolo es su escalabilidad. En otras palabras, funciona perfectamente tanto en instalaciones muy pequeñas como en instalaciones muy grandes y es compatible con una gama cada vez más amplia de tecnologías y equipos de gran rendimiento, bajo coste y gran eficacia.

A continuación tendremos una visión general de las distintas tecnologías empleadas, basadas en IP, para sacar el máximo partido de un sistema de vídeo IP.

2.2.7.1 Ethernet

Ethernet ofrece una red rápida a un precio razonable. La mayoría de ordenadores modernos se suministran con una interfaz Ethernet integrada o permiten alojar fácilmente una tarjeta de interfaz de red Ethernet (NIC, Network Interface Card).

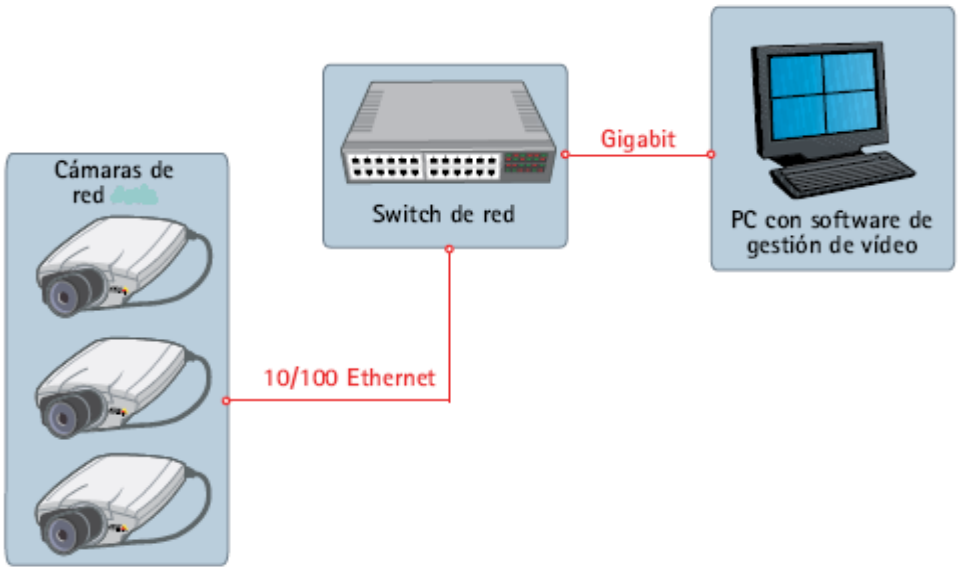


Fig.2.8 Red Ethernet

10 Mbit/s (10 Mbps) Ethernet: Este estándar raramente se usa en las actuales redes de producción debido a su baja capacidad, y ha sido sustituido por Ethernet 100 Mbit/s desde finales de la década de los 90. La topología más habitual para Ethernet 10 Mbit/s es 10BaseT, y utiliza 4 cables (dos pares trenzados) en un cable categoría 3 ó categoría 5. Un hub o switch se encuentra en el centro y posee un puerto para cada nodo. Se emplea la misma configuración para Fast Ethernet y para Gigabit Ethernet.

Fast Ethernet (100 Mbit/s): Con tasas de transferencia de datos de hasta 100 Mbit/s, Fast Ethernet es el tipo de Ethernet más utilizado en las redes informáticas actuales. El estándar principal se llama 100BaseT. Aunque es más actual y rápido que Ethernet 10 Mbit, es idéntico en todos los otros aspectos. El estándar 100BaseT puede subdividirse en:

- 100BASE-TX: Utiliza cableado de cobre de par trenzado (cat 5).
- 100BASE-FX: Ethernet 100 Mbit/s a través de fibra óptica.

Nota: *la mayoría de los swithches de red 100 Mbit admiten 10 y 100 Mbits para garantizar una compatibilidad con versiones anteriores (normalmente llamado switch de red 10/100).*

Gigabit Ethernet (1000 Mbit/s): Este es el estándar actual recomendado por los distribuidores de equipos de redes para los ordenadores de sobremesa. Sin embargo, en la actualidad se emplean más frecuentemente para las redes troncales entre los servidores de red y los conmutadores de red. 1000 Mbit/s es ampliamente usado y puede subdividirse en:

- 1000BASE-T: 1 Gbit/s a través de cableado de cobre cat 5e ó cat 6.
- 1000BASE-SX: 1 Gbit/s a través de fibra multimodo (hasta 550 m).
- 1000BASE-LX: 1 Gbit/s a través de fibra multimodo (hasta 550 m). Optimizado para distancias superiores (hasta 10 km.) a través de fibra de modo único.
- 1000BASE-LH: 1 Gbit/s a través de fibra de modo único (hasta 100 km.). Una solución para distancias largas.

10 Gigabit Ethernet (10 000 Mbit/s): Se considera la nueva opción de red troncal en las redes de empresas. El estándar 10 Gigabit Ethernet utiliza siete tipos de soportes distintos para LAN, WAN y MAN *(Red de Área Metropolitana)*. Está actualmente especificado por una norma suplementaria, IEEE 802.3ae, y se incorporará a una futura revisión de la norma IEEE 802.3.

2.2.7.2 Alimentación a través de Ethernet

La alimentación a través de Ethernet *(Power over Ethernet, PoE)* es una tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite que la alimentación eléctrica se suministre al dispositivo de red como, por ejemplo, un teléfono IP o una cámara IP, usando el mismo cable que

se utiliza para una conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones de la cámara y permite una aplicación más sencilla de los sistemas de alimentación ininterrumpida (SAI) para garantizar un funcionamiento las 24 horas del día, 7 días a la semana.

Power over Ethernet se regula en una norma denominada IEEE 802.3af y está diseñado de manera que no haga disminuir el rendimiento de comunicación de los datos en la red o reducir el alcance de la red. La corriente suministrada a través de la infraestructura LAN se activa de forma automática cuando se identifica un terminal compatible y se bloquea ante dispositivos preexistentes que no sean compatibles. Esta característica permite a los usuarios mezclar en la red con total libertad y seguridad dispositivos preexistentes con dispositivos compatibles con PoE.

El estándar proporciona una alimentación de hasta 15,4 W en el lado del conmutador o midspan[18], lo que se traduce en un consumo eléctrico máximo de 12,9 W en el lado del dispositivo (cámara), haciendo que resulte perfecto para cámaras de interior. Las cámaras de exterior así como las cámaras domo y PTZ[19] poseen un consumo eléctrico superior a éste, por lo que la funcionalidad PoE resulta menos adecuada.

Algunos fabricantes ofrecen también productos patentados que no son estándar y que proporcionan un suministro adecuado a esas aplicaciones, aunque debería tenerse en cuenta que, al tratarse de productos no estándar, no es posible una interoperabilidad entre marcas distintas.

La norma 802.3af proporciona soporte para la llamada clasificación de energía eléctrica, que permite una negociación del consumo eléctrico entre la unidad PoE y los dispositivos, lo que significa que un conmutador inteligente puede garantizar

[18] **Midspan:** Dispositivo que transmite la electricidad a un cable de red.
[19] **PTZ:** Cámaras con movimiento vertical/horizontal/zoom

un suministro suficiente y no superfluo para el dispositivo (cámara), ofreciendo la posibilidad de que el conmutador pueda permitir más salidas PoE.

2.2.7.3 Cómo usar Power over Ethernet

PoE funciona a través de un cableado de red estándar (cat 5) para suministrar alimentación directamente desde los puertos de datos a los que están conectados los dispositivos de red. Hoy en día, la mayoría de los fabricantes ofrecen switches de red con soporte PoE incorporado.

Si se dispone de una estructura de red/conmutador existente, los clientes pueden beneficiarse de la misma funcionalidad añadiendo al switch el llamado Midspan, que añadirá alimentación al cable de red. Todas las cámaras de red que no disponen de PoE incorporado, pueden integrarse en un sistema PoE usando un Active Splitter[20].

La figura 2.9 muestra cómo una cámara IP puede recibir alimentación a través de un cable de red y es capaz de seguir funcionando cuando se produce un fallo eléctrico.

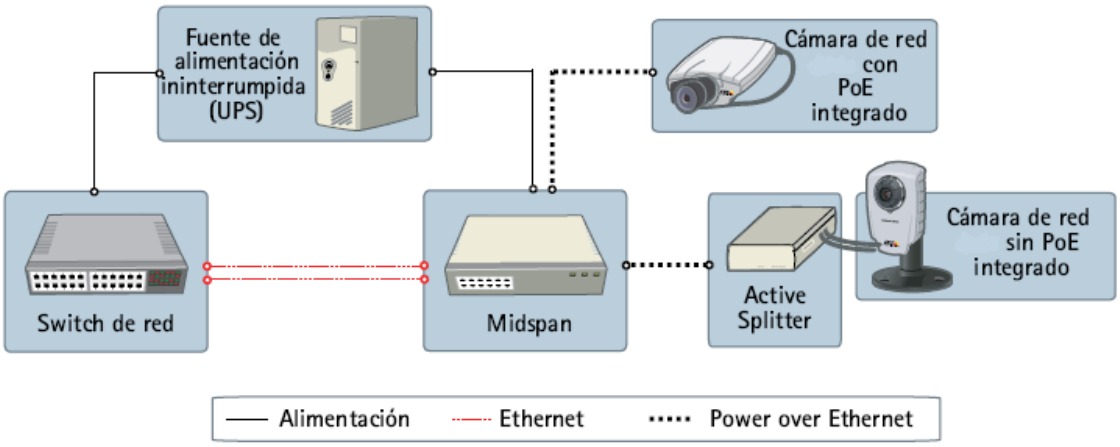


Fig.2.9 Modos de alimentación de Cámaras IP

[20] **Active Splitter:** Dispositivo que separa en un cable ethernet los datos de la electricidad

2.2.7.4 Redes inalámbricas

Aunque en la actualidad las redes con cables están presentes en la mayoría de los edificios, en algunas ocasiones una solución sin cables presenta algunas ventajas, tanto desde el punto de vista económico como funcional. Por ejemplo, puede ser útil en un edificio, donde no es posible la instalación de cables sin dañar el interior, o bien, en una instalación donde sea necesario trasladar la cámara a otras ubicaciones de forma regular sin tener que añadir nuevos cables cada vez, como en los comercios. Otro uso habitual de la tecnología inalámbrica es unir dos edificios o lugares sin tener que realizar trabajos complejos y caros en la infraestructura de los edificios.

La tecnología inalámbrica existe tanto para los sistemas de vídeo IP como para los analógicos. Existen dos categorías principales para las comunicaciones inalámbricas:

LAN inalámbrica (también conocida como WLAN): Por definición, una LAN es una Red de Área Local, es decir, cubre distancias cortas y normalmente interiores. Hoy en día, los estándares LAN inalámbricos están bien definidos y los dispositivos de distintas marcas funcionan bien juntos.

Puentes inalámbricos: Cuando es necesario conectar edificios o lugares con enlaces de alta velocidad, se precisará un enlace de datos punto a punto con capacidad para distancias largas y velocidades altas. Dos tecnologías utilizadas habitualmente son microondas y láser.

2.2.7.5 Normas para LAN inalámbricas

802.11a: Norma que usa una banda de 5 GHz y proporciona un rendimiento real de hasta 24 Mbps a 30 m (100 pies) en entornos exteriores. Existe una gama limitada de productos que lo admiten. El ancho de banda teórico es 54 Mbps.

802.11b: La norma proporciona un rendimiento real de hasta 5 Mbps a 100 m (300) pies en entornos exteriores. Usa la banda de 2,4 GHz. El ancho de banda teórico es 11 Mbps.

802.11g: La norma utilizada más habitualmente que ofrece un rendimiento mejorado en comparación con la norma 802.11b. Rendimiento real de hasta 24 Mbps a 100 m (300 pies) en entornos exteriores. Usa la banda de 2,4 GHz. El ancho de banda teórico es 54 Mbps.

802.11n: La nueva generación de la norma LAN 802.11 inalámbrica. El rendimiento real será superior a 100 Mbps.

2.2.7.6 Puentes inalámbricos

Algunas soluciones pueden utilizar también estándares distintos a la norma 802.11 predominante, proporcionando un rendimiento mejorado y distancias mucho mayores en combinación con una seguridad elevada.

Esto incluye también el uso de otros medios de radiofrecuencia como, por ejemplo los enlaces de microondas. Otra tecnología habitual son los sistemas ópticos tales como los enlaces láser.

Un enlace de microondas puede ofrecer hasta 1.000 Mbps para distancias de hasta 80 km (130 millas).

Para ubicaciones fuera del alcance de todos estos sistemas, existe la posibilidad de una comunicación por satélite, debido a la forma en que este sistema funciona, el tiempo de espera de la transmisión hasta el satélite y su regreso a la tierra puede ser largo (hasta varios segundos), lo que la convierte en menos adecuada para funciones como el control domo manual y la videoconferencia, donde es necesario un tiempo de espera menor.

Si se precisa un ancho de banda mayor, el uso de sistemas por satélite se vuelve también muy caro.

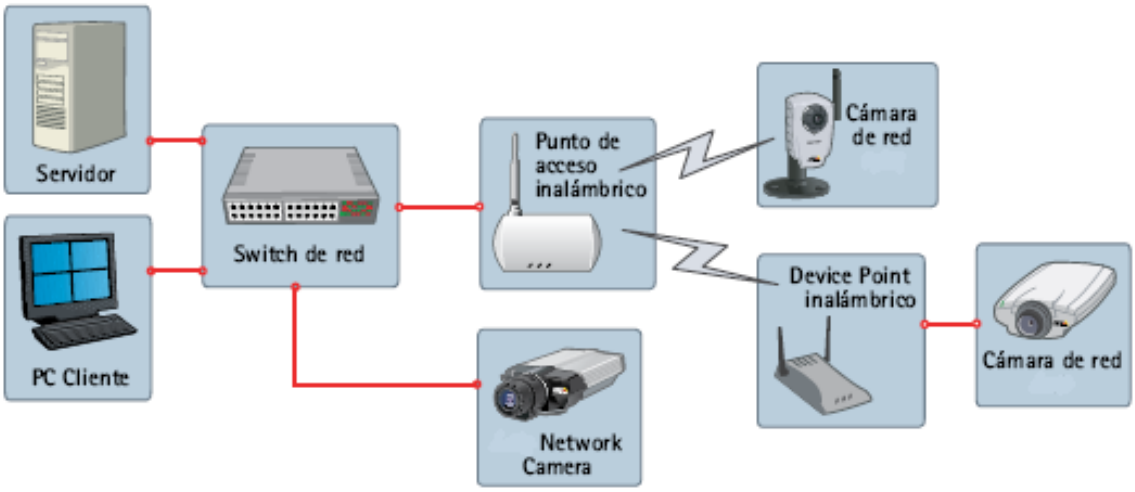


Fig.2.10 Red típica incluyendo conexiones inalámbricas y con cables

2.2.8 GESTIÓN DE VIDEO

La calidad de las cámaras IP depende directamente de la selección y configuración de los sistemas de gestión de vídeo que las controlan. Los sistemas deberán permitir a los usuarios controlar, analizar y almacenar eficazmente la salida de vídeo. Los sistemas que se basan en una plataforma de vídeo IP resultan adecuados para la integración en otros sistemas tales como el control de acceso o la gestión de edificios, y la información de esos sistemas puede ser utilizada para activar funciones en el sistema de vídeo IP, como por ejemplo, almacenar imágenes relativas a eventos.

2.2.8.1 Plataformas de hardware

Existen dos tipos distintos de plataformas para la gestión de vídeo IP: las plataformas de servidor de PC y las plataformas de NVR *(Grabador de vídeo en red)*. Ambos tipos se basan en un PC, pero presentan algunas diferencias destacables.

Una plataforma de servidor de PC se ejecuta en un hardware estándar donde se han seleccionado componentes de hardware para obtener un rendimiento superior. Con una plataforma de servidor de PC es posible aprovechar los componentes estándar, tales como un almacenamiento externo o mayor, estaciones de operadores remotos adicionales y ejecutar un software adicional en paralelo a la aplicación de vídeo, como un cortafuegos y una protección contra virus.

La diferencia más obvia entre una solución de tipo plataforma de NVR y una plataforma de servidor de PC es que un NVR se presenta como una caja de hardware con la funcionalidad de gestión de vídeo preinstalada. Por definición, está dedicado a tareas específicas de grabación, análisis y reproducción de vídeo IP. El NVR no permite que ninguna otra aplicación se conecte a éste. El propio hardware de NVR se 'bloquea' con esta aplicación y la unidad en raras ocasiones puede modificarse para alojar algún componente fuera de su especificación original.

Los sistemas diseñados en una plataforma IP son completamente escalables. Se pueden añadir cámaras y licencias, y el hardware del sistema se puede ampliar para satisfacer nuevas necesidades de rendimiento. Esta plataforma resulta adecuada para escenarios de sistemas en los cuales se utilizan un gran número de cámaras o cuando el departamento de informática posee especificaciones estándar para el hardware y el software de servidor permitidas en la red.

2.2.8.2 Plataformas de servidor de PC

La solución de plataforma de servidor de PC (fig.2.11), como ya se ha comentado anteriormente, se ejecuta en un hardware estándar donde se han seleccionado componentes de hardware que permiten obtener un rendimiento superior para el diseño específico del sistema, como un almacenamiento desconectado o sistemas de dos procesadores.

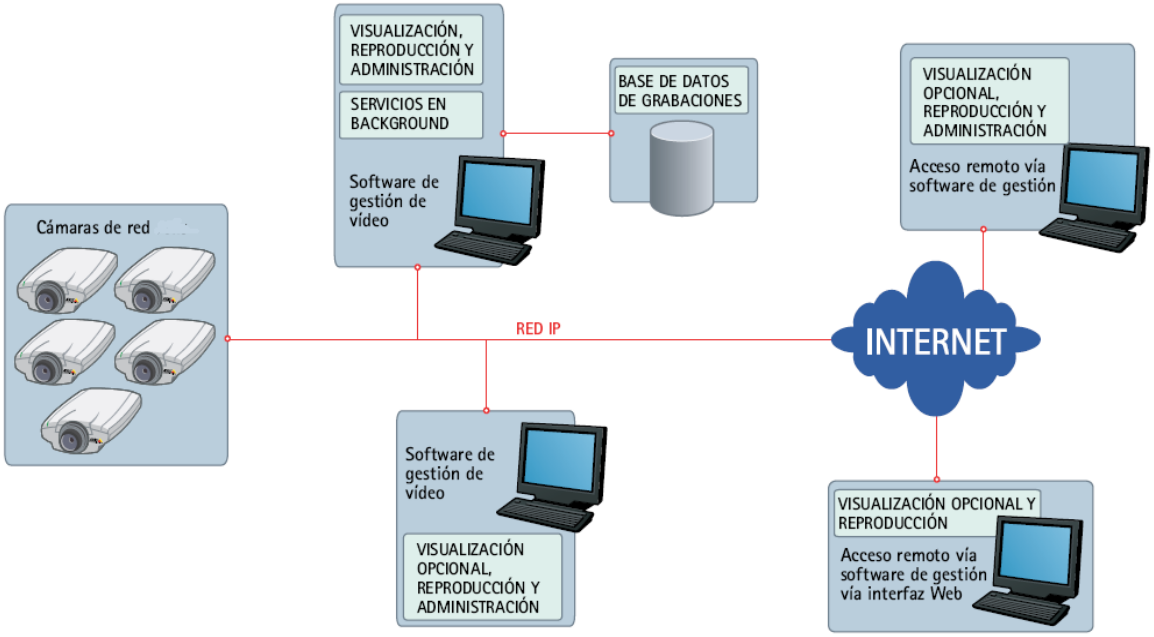


Fig.2.11 Plataforma de servidor de PC

Puesto que el sistema de plataforma de servidores de PC se basa en componentes de hardware estándar, es posible seguir usando la elección de hardware preferida por el usuario final así como las marcas existentes de equipos informáticos y servicios de mantenimiento.

2.2.8.3 Plataformas de NVR

Un NVR posee algunas similitudes con el Grabador de vídeo digital (DVR) en cuanto a grabación y reproducción. De hecho, un DVR es un sistema híbrido que puede alojar cámaras analógicas y almacenar el vídeo en un disco duro en formato digital. Un NVR (fig.2.12) es un verdadero sistema digital que recibe imágenes digitales y transmisiones de vídeo a través de la red y las graba en un disco duro en un formato digital.

Algunos DVR poseen una interfaz rudimentaria en la red que ofrece capacidades de visualización remotas. Un NVR no dispone de un monitor y un teclado exclusivos. Toda la visualización y gestión del NVR tiene lugar de forma remota a través de la red mediante un PC.

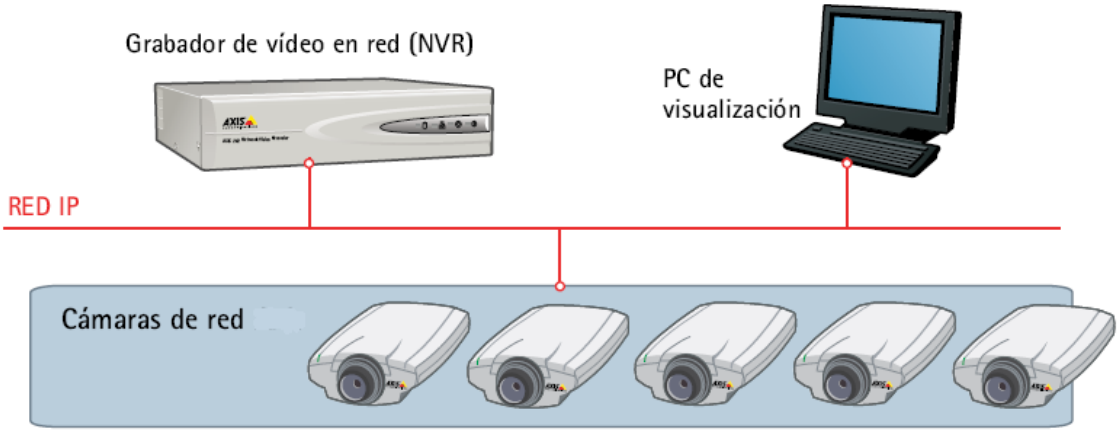


Fig.2.12 Plataformas de NVR

Un NVR está diseñado para ofrecer un rendimiento óptimo para un conjunto de cámaras, convirtiéndolo en menos escalable que un sistema de plataforma de servidor de PC. Esto permite que la unidad resulte más adecuada para configuraciones del sistema más pequeñas donde el número de cámaras se encuentra dentro de los límites de la capacidad de diseño del NVR. La ventaja es que un NVR es más fácil de instalar que una plataforma de servidor de PC.

2.2.9 AUDIO

El audio puede integrarse fácilmente en el vídeo IP ya que la red permite cualquier tipo de datos, lo que reduce la necesidad de cableado adicional, a diferencia de los sistemas analógicos donde se debe instalar un cable de audio de un extremo a otro. Una cámara IP sólo captura el audio en la cámara, integrándolo en la transmisión de vídeo y devolviéndolo a continuación para la supervisión y/o grabación a través de la red, lo que permite que se use audio desde ubicaciones remotas.

Se puede interactuar con lugares remotos desde la central mediante audio. Pueden informar al personal que están siendo vigilados y escuchados en aquellas situaciones en las que se usa el audio como un método de confirmación complementario. El audio también puede utilizarse en cámaras o servidores IP

como un método de detección independiente, que activa las grabaciones de vídeo y alarmas cuando se detectan niveles de audio por encima de un determinado umbral.

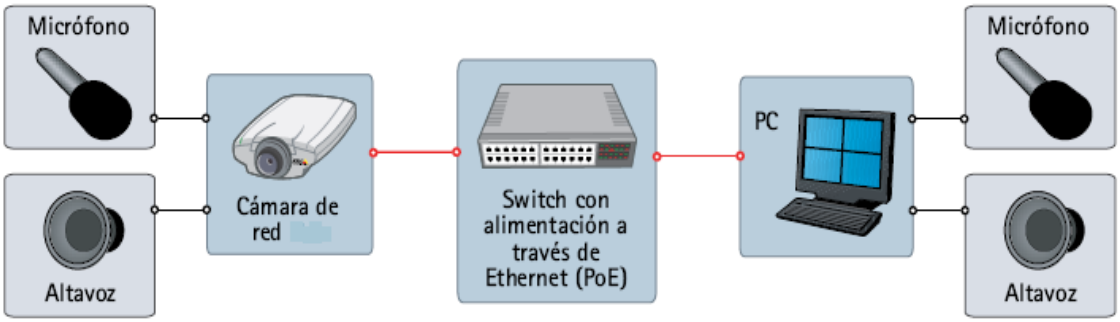


Fig.2.13 Componentes implicados en una solución de vídeo en red con audio

2.2.9.1 Transmisión de audio

El audio puede comprimirse y transmitirse como una parte integral de la transmisión de vídeo, si se emplean MPEG-1/MPEG-2/MPEG-4 ó cualquiera de los estándares de videoconferencia. También puede transmitirse en paralelo si se utiliza un estándar de imágenes fijas, como por ejemplo JPEG. Sin embargo, si se prioriza el audio y vídeo sincronizados, MPEG se convierte en la elección adecuada. No obstante, existen muchas situaciones en las cuales el audio sincronizado no es tan importante e incluso no es adecuado (por ejemplo, si el audio debe supervisarse pero no grabarse).

2.2.9.2 Compresión de audio

La compresión de audio digital permite una transmisión y almacenamiento eficientes de los datos de audio. Al igual que ocurre con el vídeo, existen muchas técnicas de compresión de audio que ofrecen distintos niveles de calidad del audio comprimido. En general, los niveles de compresión superiores
incluyen más tiempo de espera. El audio en forma digital ofrece muchas ventajas como, por ejemplo, inmunidad frente a ruidos fuertes, estabilidad y facilidad de reproducción. También permite una implementación eficaz de muchas funciones

de procesamiento posterior de audio como, por ejemplo, el filtrado de ruidos y la ecualización.

Los formatos de compresión de audio más conocidos incluyen:

- G.711 PCM que proporciona audio de calidad superior a una tasa de bits de 64 kbit/s.
- G.726 ADPCM que proporciona audio a una tasa de bits de 32 ó 24 kbit/s.
- MP3 (que equivale a ISO-MPEG Audio Layer-3), un conocido formato orientado hacia la música, con tasas de bits de aproximadamente 100 kbit/s.

2.2.9.3 Modos de audio

Al utilizar cámaras de red, se puede elegir entre varios modos de audio:

Fig.2.14 Modo Simplex

Fig.2.15 Modo Simplex

Fig.2.16 Modo Half Duplex

Fig.2.17 Modo Full Duplex

2.2.10 ENTRADAS Y SALIDAS DIGITALES (I/O)

Una característica única de los productos de vídeo IP es sus entradas y salidas digitales integradas que se pueden manejar en la red. La salida puede utilizarse para activar mecanismos, bien sea desde un PC remoto o automáticamente, haciendo uso de la lógica incorporada a la cámara, mientras que las entradas pueden configurarse para reaccionar ante sensores externos tales como los PIR (detectores de infrarrojo) o pulsar un botón que inicie las transferencias de vídeo.

Las I/O pueden usarse por ejemplo junto con sensores de alarma para eliminar transferencias de vídeo innecesarias, a menos que el sensor conectado a la cámara se active.

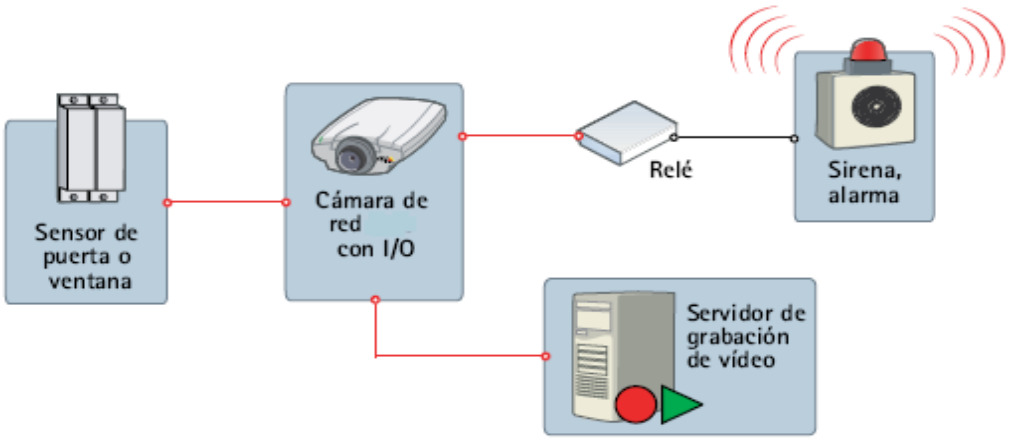


Fig.2.18 Cámara conectada a un sensor de ventana y a un sistema de alarma

2.2.10.1 Entradas digitales

La gama de dispositivos que pueden conectarse al puerto de entrada de una cámara IP es casi infinita. La regla básica es que cualquier dispositivo que puede conmutar entre un circuito abierto y cerrado puede conectarse a una cámara IP o servidor de vídeo.

Tabla 2.4 Ejemplos de dispositivos de alarma y su uso

Dispositivo	Descripción	Uso
Contacto en puertas	Un simple switch magnético que detecta la apertura de puertas y ventanas	Cuando un circuito se rompe (la puerta se abre) la cámara actúa produciendo una imagen animada a pantalla completa y enviando notificaciones
Detector de infrarrojos pasivo (PIR)	Un sensor que detecta movimiento basándose en la emisión de calor	Cuando se detecta movimiento, el PIR rompe el circuito y la cámara actúa produciendo una imagen animada a pantalla completa y enviando notificaciones
Detector de rotura de cristales	Un sensor activo que mide la presión del aire en una habitación y detecta bajadas de presión repentinas (puede ser activado por la cámara)	Cuando se detecta una bajada de la presión del aire, el detector rompe el circuito y la cámara actúa produciendo una imagen animada a pantalla completa y enviando notificaciones

2.2.10.2 Salidas digitales

La función principal del puerto de salida es permitir que la cámara active los dispositivos externos, bien sea de forma automática o mediante control remoto por parte de un operador humano o una aplicación de software.

Tabla 2.5 Ejemplos de dispositivos que se pueden conectar al puerto de salida

Dispositivo	Descripción	Uso
Relé en las puertas	Un relé (solenoide) que controla la apertura y cierre de las cerraduras de las puertas	La apertura/cierre con llave de una puerta de entrada puede controlarse mediante un operador remoto (a través de la red)
Sirena	La sirena de la alarma configurada para sonar cuando se detecte la alarma	La cámara puede activar la sirena cuando se detecte un movimiento usando el VMD integrado o usando "información" procedente de la entrada digital
Sistema de alarma/intrusión	Sistema de seguridad con alarma que supervisa permanentemente un circuito de alarmas normalmente abierto o normalmente cerrado	La cámara puede actuar como una parte integrada del sistema de alarma sirviendo de sensor y mejorando el sistema de alarma con transferencias de vídeo activadas por eventos

2.3 DISEÑO DEL SISTEMA

2.3.1 DEFINICIÓN DEL ESCENARIO

El HOSPITAL DE BRIGADA No. 11 ¨GALAPAGOS¨, es una Institución con un alto nivel de aceptación dentro de la región central que presta sus servicios al personal militar y por su gran desempeño y labor social también a extendido su ayuda a la ciudadanía en general de la provincia de Chimborazo atendiendo en todas sus áreas disponibles con total predisposición. Para viabilizar de forma adecuada su atención se ha visto en la necesidad de mejorar en su infraestructura, para lo cual esta previsto la reubicación del mismo en las nuevas

instalaciones que se encuentran dentro de la BRIGADA DE CABALLERIA BLINDADA No. 11 ¨GALAPAGOS¨ en la parte Nor-Oeste.

Al existir muchos requerimientos por parte del HOSPITAL DE BRIGADA No. 11 ¨GALAPAGOS¨, y para el óptimo funcionamiento de dichas instalaciones, entre sus principales prioridades se a puesto de manifiesto la seguridad y vigilancia electrónica de manera que garanticen todo lo existente en el hospital y al mismo tiempo llevar un control de las personas que a diario circularan por sus instalaciones. Para este efecto se realiza el presente estudio en el mencionado edificio.

2.3.1.1 Descripción del Edificio

El edificio del Hospital de Brigada No. 11 “GALAPAGOS” (HB-11) está ubicado en la parte nor-oeste del Fuerte Militar “TAPI” , es de una planta construido en hormigón con cubierta de estructura de hierro y steel panel[21], consta de tres bloques (ver anexo A) distribuidos de la siguiente manera:

- Bloque A:
    - Consulta Externa
    - Emergencia
    - Administrativo
- Bloque B:
    - Hospitalización
    - Centro Quirúrgico
- Bloque C:
    - Servicios
    - Centro de Rehabilitación
    - Dormitorios del Personal

[21] **STEEL PANEL:** Panel de acero.

Estos bloques se encuentran conectados entre si por un pasillo principal y dos laterales, existen espacios verdes entre cada bloque. Consta también de un amplio parqueadero en el sector sur del edificio. Adicionalmente está construida una casa de máquinas en el sector nor-oeste a 9.2m de los bloques principales.

Su zona perimetral está constituida por un muro de bloque en la parte oeste al lado de la Avenida de los Héroes, en este sector es donde se ubican las entradas (vehicular y peatonal) para el público en general. En las partes norte y este está colocado un cerramiento de malla que separa las instalaciones del HB-11 de las instalaciones pertenecientes a diferentes unidades orgánicas de la Brigada de Caballería Blindada No. 11 "·GALAPAGOS". En la parte sur se encuentra ubicada la zona comercial del Fuerte Militar "TAPI" (banco, comisariato, etc.) la cual se planes que tenga un acceso controlado al público.

2.3.2 DETERMINACIÓN DE LAS ZONAS A VIGILAR

Para nuestro estudio dividiremos al edificio en zonas (ver anexo B):

- Zona 1: lado sur:
- Zona 2: lado oeste:
- Zona 3: lado norte:
- Zona 4: lado este:
- Zona 5: pasillo principal.
- Zona 6: pasillo bloque A.
- Zona 7: pasillo bloque B.
- Zona 8: casa de máquinas.

La distribución eficaz de los puntos de videovigilancia se establecerán en base a:

- Valorización del material y equipo en cada dependencia.
- Cantidad de tráfico en cada zona.
- Nivel de seguridad existente.

- Los riesgos estimados.
- Las características físicas (tamaño, forma, profundidad, etc.) de la zona a vigilar.
- Un alto control perceptivo de la zona a vigilar.

2.3.2.1 Zona 1 (lado sur)

En esta zona estarán ubicados los ingresos (vehicular y peatonal) y los parqueaderos, no hay existencia de insumos ni equipo pero el valor material está considerado en los vehículos que se aparcarán en este sitio. Se estima un muy alto tráfico tanto de vehículos como de personas.

El nivel de seguridad es óptimo en los ingresos donde existirá la presencia de policías militares para el control de entrada y salida, en cambio en el parqueadero el nivel de seguridad es nulo ya que no está prevista la colocación de centinelas en el sector. El principal riesgo radica en la posible sustracción de implementos de los vehículos. La zona a cubrir está libre de obstáculos tiene 73.59m de frente x 37.04m de profundidad. Para obtener un óptimo nivel de vigilancia se establecerán dos puntos de videovigilancia.

2.3.2.2 Zona 2 (lado oeste)

En esta zona se destacan la puerta de ingreso de heridos en ambulancia y la puerta de ingreso del personal médico residente, no existe material ni equipo de gran valor pero existe valioso capital humano. En la puerta de emergencia se estima una alta circulación de personal (médico, auxiliar, heridos, etc.), en el otro ingreso únicamente estará permitida la circulación al personal autorizado.

El nivel de seguridad es medio ya que se dispondría solamente de un centinela móvil. Los riesgos en este caso radicarían en la continua circulación de personas y la posible infiltración de elementos indeseables por el muro oeste en especial en

la noche. Esta zona cubre un frente de 63.04m. Para solventar estos problemas se establecerán dos puntos de videovigilancia.

2.3.2.3 Zonas 3 y 4 (lado norte y este)

Corresponden principalmente los ingresos al área de servicios (cocina, lavandería, etc.), al área administrativa (dirección, dpto. de logística, etc.) y a los dormitorios del personal militar, en estos sitios existen enseres de apreciable valor sobre todo en el campo informático. Se prevé la circulación únicamente de personal de servicio (cocina, mantenimiento, etc.) y personal militar.

El nivel de seguridad es alto ya que se dispondrán centinelas y se tendrá la continua presencia de personal militar en el sector. Los riesgos en estas zonas son mínimos ya que fuera del perímetro se cuenta con la vigilancia de centinelas designados por las unidades en sus respectivos sectores de responsabilidad.

Al no existir mayores problemas de seguridad no se dispondrán de puntos de videovigilancia en estas zonas.

2.3.2.4 Zona 5 (pasillo principal)

En esta se encuentra el acceso principal para el público en general y se constituye en el principal nexo entre los bloques hospitalarios. La circulación por la zona será a gran escala en virtud de lo cual existe el riesgo de que se infiltren elementos indeseables.

El nivel de seguridad es nulo ya que no existe control alguno. Esta zona comprende un frente promedio de 2.5m y una profundidad de 63.04m. En esta zona se establecerá un punto de videovigilancia.

2.3.2.5 Zona 6 (pasillo bloque A)

Aquí se dispondrán los servicios de consulta externa y laboratorio clínico, debido a la existencia de insumos y equipos de gran valor en esta zona se debe establecer un alto nivel de seguridad, el cual puede ser proporcionado por el personal de guardia, sin embrago al tener previsto una aceptable afluencia de público se necesita llevar un control tanto del personal que presta servicio como del personal que hace uso de este.

Tiene un frente que varía entre 1.84m y 4.04m con una profundidad de 72.77m. Debido a la no existencia de linealidad en el pasillo se deben establecer dos puntos de videovigilancia.

2.3.2.6 Zona 7 (pasillo bloque B)

Esta comprende el área de hospitalización y el centro quirúrgico, aquí encontramos material y equipo de alta precisión y tecnología, por ende de alto valor económico y operativo. Se debe conseguir un alto nivel de seguridad y al mismo tiempo salvaguardar la intimidad de los pacientes.

Debido a que existirá un alto tráfico de personal sobre todo a la hora de visitas, se necesita de una ayuda extra de vigilancia a más de la proporcionada por el centinela móvil. Se debe cubrir un frente de 2.20m y una profundidad de 60.08m. para este efecto se necesitará de un punto de videovigilancia.

2.3.2.7 Zona 8 (casa de máquinas)

Corresponde a la sala de máquinas, tanque de combustible e incinerador, se constituye en un área restringida en donde no debe haber circulación de personal alguno. Debido al riesgo por la maquinaria y sustancias existentes debe establecerse un alto nivel de seguridad el cual será proporcionado por un

centinela fijo (24 horas). Por la presencia de sustancias inflamables es recomendable no instalar dispositivos eléctricos.

En resumen analizados diferentes factores y para establecer un balance armónico entre costo, operabilidad y eficiencia del sistema de videovigilancia se ha determinado la colocación de 8 cámaras IP en apoyo a la seguridad del HB-11 "GALAPAGOS", su ubicación y características se tratarán a continuación.

2.3.3 CONSIDERACIONES SOBRE LAS CÁMARAS

El sistema de vigilancia por vídeo que se va a instalar es un sistema nuevo, la mejor elección en este caso es la utilización de cámaras IP, que se encuentran disponibles en el mercado en diversos modelos que satisfacen una amplia variedad de necesidades. Se deben aplicar algunas reglas básicas al buscar maximizar el rendimiento de un sistema de vídeo IP. Trataremos algunas de estas reglas, en particular la posición e instalación de la cámara y demás factores a tener en cuenta con tal de lograr el mejor detalle y calidad de imagen posibles, tanto en el interior como en el exterior.

Número de cámaras: Se proyecta la colocación de 8 cámaras, 4 exteriores y 4 interiores.

Necesidad de audio: Es recomendable aprovechar esta ventaja que nos proporciona una cámara IP ya que posee micrófono incorporado, de modo que puede escuchar lo que está viendo.

Con cable o inalámbricas: La elección correcta depende del lugar donde va a colocar la cámara:

- Las que llevan cable quedan fijas en un lugar y deben instalarse en un lugar donde el cable no moleste. Ofrecen mejores garantías de obtener una imagen de calidad.

- Las cámaras inalámbricas pueden cambiarse de lugar con facilidad y pueden instalarse en sitios diversos, pero la transmisión de la señal puede verse interferida por otros dispositivos (como teléfonos inalámbricos, intercomunicadores y algunas redes de computación).

La fuente de luz: Para obtener imágenes claras, es necesario que la luz del entorno o la de la propia cámara sea estable y fiable. El nivel de lux[22] de una cámara mide su capacidad para capturar imágenes en la oscuridad. Cuanto menor sea el nivel de lux, menos luz se necesita para obtener una imagen nítida. Se puede realizar una vigilancia discreta en la oscuridad o en la penumbra por medio de una luz infrarroja, que es invisible al ojo humano, esta es otra de las ventajas que presenta la tecnología de las cámaras IP.

Tabla 2.6 Nivel de Lux en el Entorno

Entorno	Lux
Fuerte luz del sol	100,000
Luz de día	10,000
Luz de oficina	500
Habitación poco iluminada	100

Control del Iris: 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. En las cámaras convencionales, el tiempo de exposición es fijo. El papel del iris es el de ajustar la cantidad de luz que pasa a través del objetivo. El control puede ser manual o automático.

Fuente de energía: En el caso de las cámaras con instalación alámbrica la energía es suministrada a través del PoE que lo realiza por el mismo cable de la red (UTP cat.5). Algunas cámaras en especial las inalámbricas poseen un adaptador que debe conectarse a un tomacorriente.

[22] **LUX:** unidad estándar para la medición de la cantidad de luz

2.3.4 CÁMARAS EXTERIORES

2.3.4.1 Tipo de Cámara

Se recomiendan las cámaras IP PTZ (fig.2.19), son cámaras con movimiento vertical/horizontal/zoom (PTZ) poseen la ventaja de obtener una visión panorámica, inclinada, alejada o de cerca de una imagen manual o automáticamente. Para un funcionamiento manual, la cámara PTZ puede, por ejemplo, utilizarse para seguir los movimientos de una persona en un determinado sector.

Fig.2.19 Cámara IP PTZ

Las cámaras PTZ se utilizan principalmente en aquellos lugares donde resulte apropiado ver la dirección hacia la cual apunta la cámara. La mayoría de cámaras PTZ no disponen de un movimiento horizontal completo de 360 grados, y tampoco están hechas para un funcionamiento automático continuo conocido como “recorrido protegido”. El zoom óptico oscila entre 18x y 26x.

2.3.4.2 Recomendaciones para el montaje de una cámara en el exterior

Para obtener imágenes de alta calidad de una cámara, se aplicarán unas cuantas reglas básicas. Dichas reglas se aplican por igual tanto a las cámaras IP como a cualquier otro tipo de cámara. A continuación algunos aspectos a tomar en cuenta para obtener buenas imágenes:

Cantidad de luz: Para las aplicaciones en el exterior, se debería utilizar un objetivo con iris automático. Un objetivo con iris automático ajusta automáticamente la cantidad de luz que llega al sensor de imagen, lo que optimiza la calidad de la imagen y protege el sensor contra los daños causados por la luz solar intensa.

Luz solar directa: Debería evitarse siempre exponer una imagen a la luz solar directa ya que “deslumbrará” a la cámara y blanqueará de forma permanente los pequeños filtros de color del chip sensor. Si es posible, la cámara debería colocarse mirando en la misma dirección que el sol.

Contraste: Visualizar una porción demasiado grande del cielo produce demasiado contraste. La cámara se ajustará a fin de lograr un nivel de luz adecuado para el cielo. En consecuencia, el objeto o paisaje enfocado aparecerá demasiado oscuro. Una forma de solucionar este problema es montar la cámara a gran distancia del suelo, usando un poste si fuera necesario. Siempre debería utilizarse un equipo de fijación resistente para evitar las vibraciones causadas por el viento fuerte.

Reflejos: Si la cámara se monta detrás de un cristal como, por ejemplo, en una carcasa, el objetivo deberá colocarse cerca del cristal. En caso contrario, los reflejos de la cámara y el fondo aparecerán en la imagen. Para reducir los reflejos, pueden aplicarse recubrimientos especiales a cualquier cristal que se use delante del objetivo.

Iluminación: Cuando se usan cámaras por la noche, se puede necesitar una iluminación externa adicional. Esto debería prepararse para evitar reflejos y/o sombras. Para la seguridad encubierta, en lugar de la iluminación normal se pueden utilizar iluminadores de infrarrojos (IR), conocidos como “luz blanca“. La luz IR es imperceptible, lo que significa que aunque sea suficiente para captar imágenes desde cámaras IR, no es visible para el ojo humano. Las cámaras a color no funcionan con luz infrarroja.

Algunas cámaras pueden cambiar automáticamente entre un modo de color diurno y un modo IR adecuado para la visión nocturna donde la imagen aparecerá sin colores.

Nota: *Las cámaras de vigilancia de exteriores necesitan cubiertas especiales que las protejan de las inclemencias del tiempo. Aquellas que pueden ser objeto de actos de vandalismo requieren cubiertas reforzadas que resistan los golpes.*

2.3.4.3 Ubicación de las Cámaras

Nuestro diseño considera la colocación de 4 cámaras exteriores (ver anexo C) cuya ubicación se detalla a continuación:

Cámara 1: Se ubicará en la cornisa, a 15m de la esquina inferior derecha del bloque A como se muestra en la figura 2.20.

Fig.2.20 Ubicación Cámara 1

Esta cámara deberá cubrir al menos el 60% de la zona 1 como se muestra en la figura 2.21.

Fig. 2.21 Zona de cobertura Cámara 1

Cámara 2: Se ubicará en la cornisa en la esquina inferior izquierda del bloque A como se muestra en la figura 2.22.

Fig.2.22 Ubicación Cámara 2

El 40% del área de la zona 1 debe ser cubierta por esta cámara así como los ingresos vehicular y peatonal como se ve en la figura 2.23.

Fig.2.23 Zona de cobertura Cámara 2

Cámara 3: La ubicación de esta cámara será en la entrada de heridos en ambulancia, entre el bloque A y el bloque B al lado oeste. Ver figura 2.24.

Fig.2.24 Ubicación Cámara 3

El área a cubrir es el 50% de la zona 2. Ver figura 2.25.

Fig.2.25 Zona de cobertura Cámara 3

Cámara 4: Su colocación se la deberá realizar en el ingreso de personal médico residente, esto lo observaremos en la figura 2.26.

Fig.2.26 Ubicación Cámara 4

Esta cámara debe cubrir el 50% restante de la zona 2. Ver figura 2.27.

Fig.2.27 Zona de cobertura Cámara 4

2.3.5 CÁMARAS INTERIORES

2.3.5.1 Tipo de Cámara

Se sugiere para interiores el uso de cámaras IP fijas (fig.2.28). Las cámaras fijas formadas por un cuerpo y un objetivo representan el tipo de cámara tradicional.

En algunas aplicaciones, resulta sumamente útil que la cámara sea muy visible puesto que también será visible la dirección hacia la cual apunta. Otra ventaja es que la mayoría de cámaras fijas disponen de dispositivos intercambiables sobre todo en lo que a lentes se refiere.

Fig.2.28 Cámara IP fija

2.3.5.2 Recomendaciones para el montaje de una cámara en el Interior

Se deben tomar en cuenta algunos aspectos al parecer simples para maximizar el rendimiento de un sistema de vídeo IP para interiores, entre estos tenemos:

Cantidad de Luz: La razón más habitual de que las imágenes tengan baja calidad es la falta de luz. Generalmente, cuanta más luz haya, mejores serán las imágenes.

Con poca luz, las imágenes se vuelven borrosas y de color mate. Se necesitan como mínimo 200 Lux para captar imágenes de buena calidad. Una cámara de alta calidad puede ajustarse para que funcione a 1 Lux. Esto significa que una imagen puede ser captada a 1 Lux, pero no quiere decir que sea buena. Se recomienda un objetivo de iris manual el cual se configura normalmente cuando se instala la cámara para adaptarse a las condiciones de luz reinantes.

Estos objetivos no pueden reaccionar ante cambios en la iluminación de la escena, por tanto el iris se ajusta a un valor “medio”, que se usa en condiciones de luz variable.

Evitar el contraluz: Deberían evitarse las zonas brillantes en las imágenes. Las imágenes brillantes pueden sobreexponerse (blanco brillante) y en consecuencia

los objetos pueden aparecer demasiado oscuros. Este problema ocurre normalmente al intentar captar un objeto desde detrás de una ventana.

Reducir el contraste: La cámara ajusta la exposición para obtener un nivel medio de luz en la imagen. Al intentar captar una imagen de una persona que permanece de pie delante de una pared blanca, la persona generalmente suele aparecer demasiado oscura. Este problema se puede solucionar fácilmente si el color de fondo se sustituye por gris en lugar de blanco.

2.3.5.3 Ubicación de las Cámaras

Se ha considerado en el diseño la colocación de 4 cámaras interiores (ver anexo D), a continuación detallamos su ubicación:

Cámara 5: Se ubicará detrás de la puerta del acceso principal al bloque A, cerca de la esquina superior izquierda, podemos observarla en la figura 2.29.

Fig.2.29 Ubicación Cámara 5

Esta cámara nos permitirá tener una visión completa de la zona 5. Ver figura 2.30.

Fig.2.30 Zona de cobertura Cámara 5

Cámara 6: Se colocará esta cámara en el lado izquierdo del pasillo del bloque A, sobre la puerta de ingreso al laboratorio clínico, donde indica la figura 2.31.

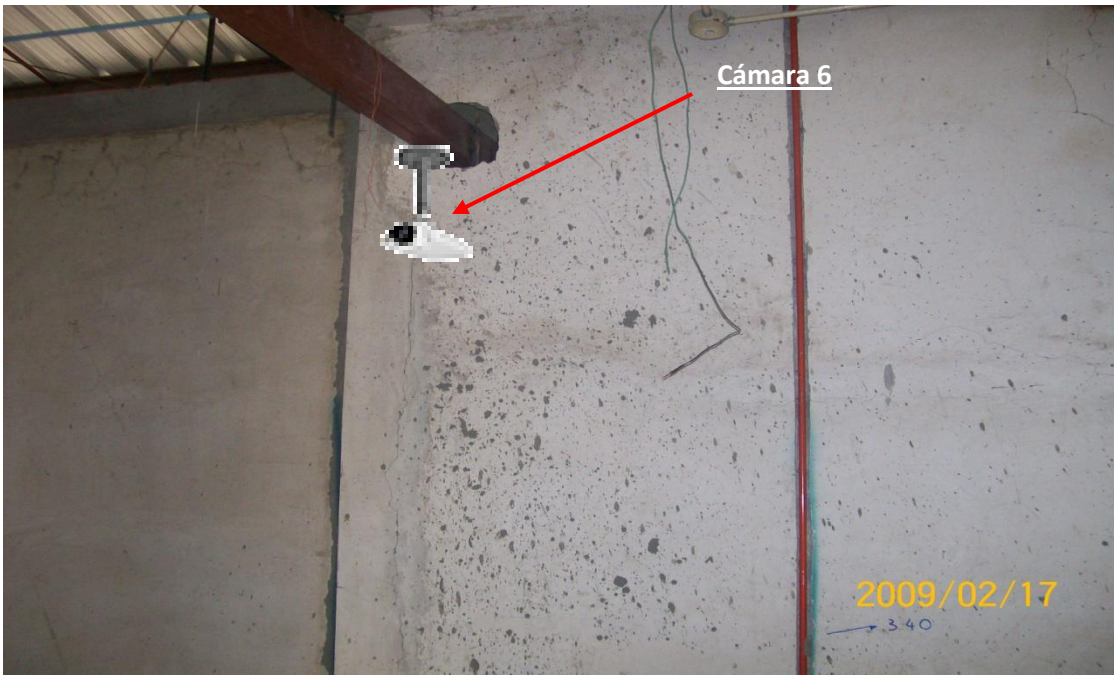


Fig.2.31 Ubicación Cámara 6

Con esta cámara podremos cubrir el 40% de la zona 6. Ver figura 2.32.

Fig.2.32 Zona de cobertura Cámara 6

Cámara 7: La colocaremos al lado izquierdo del pasillo del bloque B, sobre la puerta del centro odontológico, como se ve en la figura 2.33.

Fig.2.33 Ubicación Cámara 7

La cobertura de esta cámara será del 60% de la zona 6. Ver figura 2.34

Fig.2.34 Zona de cobertura Cámara 7

Cámara 8: Esta cámara se colocará en la parte izquierda del pasillo del bloque B, sobre la puerta de la zona de aislamiento, así se muestra en al figura 2.35.

Fig.2.35 Ubicación Cámara 8

Con esta cámara tendremos una completa visión de la zona 7. Ver figura 2.36.

Fig.2.36 Zona de cobertura Cámara 8

2.4 CABLEADO ESTRUCTURADO

2.4.1 CONSIDERACIONES PARA EL CABLEADO

Una vez conocidas las distintas posibilidades existentes técnicamente, vamos a diseñar nuestro sistema como una red de área local, para este propósito debemos tener en cuenta las siguientes consideraciones:

2.4.1.1 Estándar de red a utilizar

El estándar que se utilizará en el diseño de la red será Fast Ethernet según la norma IEEE 802.3u. Esta tecnología presenta como ventajas principales el bajo costo de su implementación y la capacidad proteger las estaciones conectadas a la red del riesgo que implica la posibilidad de que un usuario desconecte intencionalmente o no, una estación o cable; esto debido a que el tipo de topología física que emplea es en estrella. Adicional este estándar define el uso del cable UTP categoría 5, el cual permite velocidades de hasta 100 Mbps, lo cual

se adapta a los requerimientos de velocidad de la red; por otro lado el método de acceso al medio que específica la norma es el CSMA/CD[23]. Este método consiste en comprobar si la línea esta libre antes de comenzar la transmisión, verificando si se a producido una colisión durante la transmisión, de haberse producido una colisión se detiene la transmisión y se vuelve a transmitir el bloque de dato después de un tiempo de espera aleatorio. Asimismo, el tipo de conector que específica este estándar es el RJ-45.

2.4.1.2 Topología de la red

Para este proyecto consideramos conveniente adoptar como topología de red la tipo estrella, debido a las numerosas ventajas que esta puede proporcionar al diseño, siendo la principal de ellas el permitirnos centralizar la administración de la red de modo que si se requiere desconectar un terminal de la misma no es necesario suspender el funcionamiento de la red. Además, en este tipo de topologías la tasa de transferencia de datos es muy alta y el fallo en una de las estaciones de la red no afecta o perjudica al resto de las estaciones que la conforman.

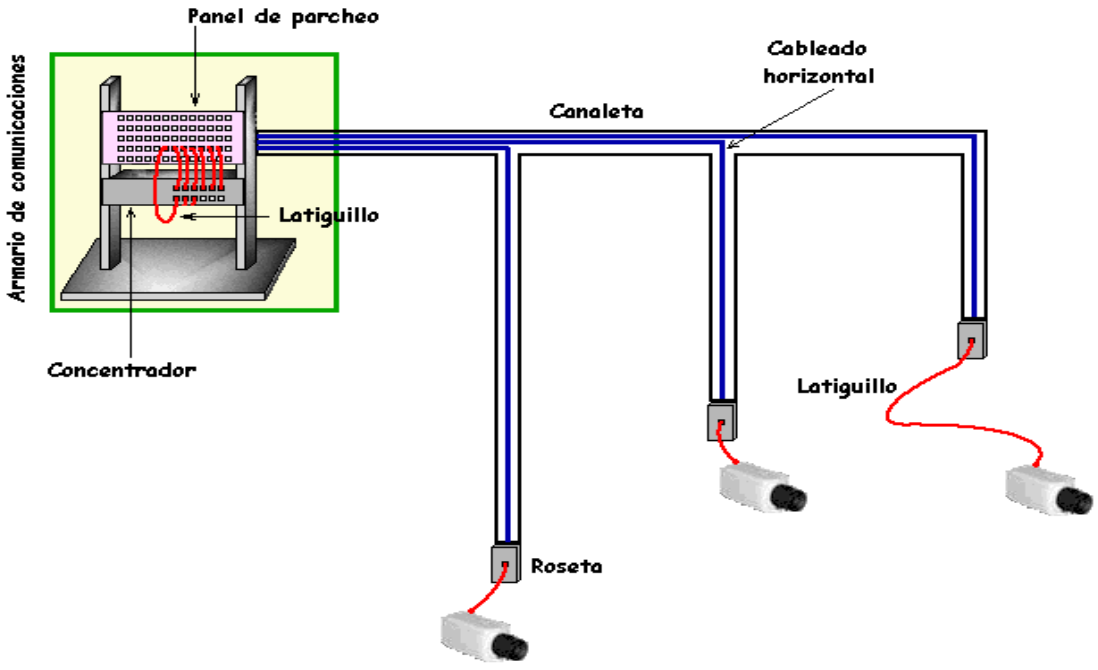


Fig.2.37 Topología del sistema (estrella)

[23] **CSMA/CD:** Acceso Múltiple por Detección de Portadora con Detección de Colisiones.

Básicamente consistirá en un concentrador principal a donde llegarán todos los cables de los distintos puntos de videovigilancia. Realmente los cables llegarán al panel de parcheo donde serán etiquetados e identificados. Se colocará una roseta en cada una de los puntos de videovigilancia y mediante las respectivas canaletas se conducirán los cables hasta el armario de comunicaciones. La conexión entre el panel de parcheo y el concentrador, así como entre las rosetas y las cámaras, se realizarán mediante los correspondientes latiguillos.

2.4.1.3 Plataforma a utilizar

La plataforma a utilizar es Microsoft Windows XP, se ha hecho esta elección por la compatibilidad entre aplicaciones y hardware, además la confiabilidad del sistema operativo y la seguridad, incluidas las actualizaciones más recientes que resuelven los problemas de seguridad detectados en Windows XP.

2.4.1.4 Protocolo de comunicación

El protocolo de comunicación a utilizar en el sistema para permitir la conexión a Internet, la conexión de múltiples redes y además el manejo de los errores en la transmisión de los datos, es el TCP/IP, el cual administra el enrutamiento y el envío de datos, y controla la transmisión por medio del uso de señales de estado predeterminados. Dicho protocolo es comúnmente utilizado por todos los Computadores conectados a Internet, de manera que éstos puedan comunicarse entre sí. Son estos los principales motivos que nos llevan a definir en nuestro diseño a TCP/IP como protocolo de comunicación.

2.4.1.5 Conexión a Internet

Cualquier tipo de conexión a Internet ADSL, Cable o wifi (Ecuanet, Interactive, Easynet, etc.). El tipo de conexión debe ser monousuario en el caso de tecnología ADSL. Puede ser conexión por Tarjeta de red o por puerto USB. La velocidad

ideal para visualizar el sistema es un mínimo de 256 kbps para las 8 cámaras (considerando solo el uso de ancho de banda para transmisión de video)

2.4.1.6 Dirección IP

Cualquier tipo de dirección IP siempre y cuando sea publica, este tipo de dirección está generalizada ya que el 90% de las IP's asignadas por los proveedores de Internet son públicas.

2.4.2 ELEMENTOS PASIVOS

2.4.2.1 Cable UTP categoría 5

Además de lo indicado por el estándar en lo que al cable se refiere debemos tomar en cuenta:

- Número de equipos a conectar:
    - 8 cámaras IP
    - 2 PC (1 servidor y 1 de visualización)
    - 1 switch
    - 1 router
- Su distribución física:
    - distancia de separación máxima 77m
    - distancia de separación mínima 19m
    - su instalación será en diferentes bloques

El cable UTP está compuesto por cuatro pares de hilos trenzados, individualmente y entre ellos con un ciclo de trenzado de menos de 38 mm. El hilo usado es de 0.5 mm y está indicado para ser utilizado a temperaturas entre -10ºC a 60ºC. Los colores con los que se identifican cada uno de los pares son:

- Par 1: Blanco-Azul/Azul

- Par 2: Blanco-Naranja/Naranja
- Par 3: Blanco-Verde/Verde
- Par 4: Blanco-Marrón/Marrón

Fig.2.38 Cable UTP cat.5

2.4.2.2 Rosetas

En el mercado existen varios tipos de rosetas con sus respectivos conectores, habrá que vigilar a la hora de escoger cualquiera de ellas que cumplan con la reglamentación. En nuestro caso deben ser de categoría 5, además que no necesiten de herramientas adicionales para su conexionado.

2.4.2.3 Panel De Parcheo

Son estructuras metálicas con placas de circuitos que permiten interconexión entre equipos, los conectores usados en el panel de parcheo son RJ-45 hembra y habrá tantos como rosetas repartidas por los distintos puntos de videovigilancia. Posee conectores en donde se ponchan las cerdas de los cables provenientes de las rosetas. La idea del panel de parcheo además de seguir estándares de redes, es la de estructurar o manejar los cables que interconectan equipos en una red, de una mejor manera. Para ponchar las cerdas de un cable en el panel de parcheo se usa una ponchadora al igual que en las rosetas. Es conveniente prever las posibles ampliaciones y disponer de más conectores de los que vamos a utilizar actualmente.

En nuestro caso el panel de parcheo que usaremos estará constituido por una caja de superficie que albergará en su interior a 12 conectores, además debemos prever la posibilidad de poder ampliar en un futuro el número de conectores disponibles.

Fig.2.39 Panel de Parcheo

2.4.2.4 Conectores

Los conectores usados son los RJ45 macho y los usaremos para la construcción de los latiguillos de conexión externa de todos los dispositivos. Es importante saber que en el mercado existen conectores de varias calidades y que en muchos casos, un mal contacto producido por un mal conector, nos puede bajar el rendimiento de una LAN.

Fig.2.40 Conector RJ45 macho

Para el presente proyecto se ha elegido un conector de categoría 5 y de la calidad suficiente para que permita contactos seguros. Se pueden destacar las siguientes características:

- La calidad de sus contactos es alta.
- El conector tiene una capucha para la sujeción final del cable, que ayuda a tener una mejor sujeción del cable al conector.
- Dispone de un contacto de tierra para conseguir más protección de datos ante interferencias externas. En nuestro caso no se usará este contacto ya que no se ha visto necesario para las características de nuestro sistema.

2.4.2.5 Rack o Soporte metálico

Necesitamos una estructura de metal muy resistente, de forma cuadrada de aproximadamente 1.5 mts de alto por 1 mt de ancho, en donde se colocarán el servidor, el router, el switch y el panel de parcheo, deberán poseer orificios laterales para la sujeción mediante tornillos.

2.4.2.6 Canaletas

Las canaletas a usar son de dos cavidades con un tabique central para poder separar en dos grupos los cables que vayan por su interior.

Fig.2.41 Canaleta

2.4.3 ELEMENTOS ACTIVOS

2.4.3.1 Switch

Es muy similar a los hubs, solo que no se comparte el ancho de banda. Un switch mediante memoria no volátil, permite que cada uno de sus puertos posea su propio ancho de banda. Además de esto, son equipos que transmiten la información solo al puerto o puertos que requieran de la misma. Un switch puede soportar múltiples conversaciones y permite movilizar mayor tráfico que un hub.

Para el proyecto se necesita un switch de 16 tomas RJ45 para la conexión de los distintos nodos, con una velocidad de 10 Mbits/s. Como se indicó anteriormente tanto la tarjeta de red como el cableado, los conectores y rosetas, soportan 100 Mbits/s de velocidad pero es el concentrador el que la limita a 10 Mbits/s. Esto significa que simplemente con poner los concentradores o Switch adecuados se podrán conseguir velocidades muy superiores en nuestra red o en algún segmento de ésta que nos interese.

2.4.3.2 Router

Necesitaremos un router RDSI de fácil conexión, configuración y mantenimiento, que permita que con una única línea telefónica, y con una sola cuenta de acceso a Internet, puedan conectarse todos los puntos de la red a Internet.

Para los ordenadores locales (servidor y visualizador) será totalmente transparente la conexión con Internet, ya que en el momento que necesiten cualquier servicio de ésta, será el router el encargado de provocar una llamada e interconectar nuestro sistema con el resto del mundo. De igual forma cuando pase un tiempo razonable sin que se esté solicitando servicios externos, el propio router desconectará la llamada para gastar sólo el tráfico telefónico necesario.

2.4.3.3 PC

Los computadores deben cumplir las siguientes características mínimas:

- Pentium IV
- 256 MB RAM
- Disco duro de 10 Gb
- 1 Ranura PCI Libre Para instalar tarjeta capturadora
- Windows XP

2.4.4 DISEÑO DEL CABLEADO ESTRUCTURADO

Para definir el sistema de cableado por el cual se regirá nuestro proyecto, consideraremos las normas que establece el sistema de cableado estructurado, específicamente adoptaremos la norma 568-A[24] la cual se fundamenta en que permite diseñar e instalar el cableado contando con poca información acerca de los productos que posteriormente se instalarán.

2.4.4.1 Cuarto de Equipos

El cuarto de equipos estará dedicado al uso específico de equipo de telecomunicaciones tal como central telefónica, equipo de cómputo y/o conmutador de vídeo. El espacio del cuarto de equipos no debe ser compartido con instalaciones eléctricas que no sean de telecomunicaciones. El área donde funcionará el cuarto de equipos es la ubicada en el pasillo principal a 13.2m de la entrada principal entre Información y el Departamento de Optometría (ver anexo E). Este cuarto administrará y controlará toda la red del Edificio.

En este cuarto estará instalado el rack en cuyo interior tendremos presente el siguiente hardware:

[24] **568-A:** Norma que estandariza el cableado estructurado en redes de datos

- Panel de parcheo
- Switch
- Router
- PC servidor y grabador de video

Cabe destacar que el sitio para el cuarto de equipos ya estaba estipulado previamente en el diseño hecho por los constructores del edificio, por esta razón en este sitio están previstas una toma de la línea RDSI y una toma de alimentación de 110Vac. A pesar de no estar ubicado en el lugar más céntrico del edificio, la ubicación del cuarto de equipos nos presta las facilidades necesarias para recorrer con el cableado hasta los distintos puntos de videovigilancia.

Aunque se encuentra en una área accesible a todo el público presta todas las seguridades del caso ya que la puerta tendrá candados y cerrojos cuyas llaves estarán en poder del oficial de operaciones y del oficial de logística, adicionalmente se colocará una puerta de seguridad en el rack de videovigilancia cuya llave estará en manos del clase mas antiguo de comunicaciones el mismo que será el encargado directo del sistema de videovigilancia.

2.4.4.2 Cuarto de visualización

Es el sitio donde se instalará el PC de visualización, se ubicará en la Recepción ya que aquí está establecido el puesto de guardia para el encargado del monitoreo, esta labor estará a cargo del personal militar de comunicaciones. En este lugar se instalarán el PC de visualización (con software de gestión de video) y un monitor de 21”.

2.4.4.3 Cableado Vertical

En vista de que se trata de una construcción de una planta, y no estar considerada una proyección para mas pisos, no se considerará un diseño de cableado vertical.

2.4.4.4 Cableado Horizontal

El cableado horizontal esta formado por los cables que se extienden a través del techo del edificio del HB-11 “GALAPAGOS”, desde el cuarto de telecomunicaciones hasta cada punto de videovigilancia del edificio.

Nota: *Al no existir cableado vertical el* ***Backbone*** *estará constituido únicamente por el cableado horizontal.*

Las canaletas son utilizadas para distribuir y soportar el cableado horizontal y conectar hardware entre la salida del cuarto de equipos y cada punto de videovigilancia así como también con el equipo terminal de visualización. Cada punto terminal de conexión deberá estar conectado al panel de parcheo, el mismo que se encontrará en el cuarto de equipos (en el rack).

Antes de realizar el diseño se han hecho las siguientes consideraciones:

- Los cables deben estar al menos a 30cm de distancia de las luces fluorescentes.
- La distancia entre los cables de la red y los de la corriente eléctrica debe de ser superior a 30cm. Si tienen que cruzarse, deberán de hacerlo en ángulo recto para evitar el acoplamiento.
- En el caso de no poder evitar el que estén en paralelo cables de corriente eléctrica junto con cables de la red, habrá que tener en cuenta que:
    - La separación mínima será de 2cm para recorridos en paralelo menores de 2.5m.
    - La separación mínima será de 4cm para recorridos en paralelo menores de 10m.
- Se debe de evitar pasar cerca de tomas de agua o fuentes de humedad así como zonas de altas temperaturas.
- Deben de estar al menos a 1.2 metros de aires acondicionados, ventiladores o calentadores.

- Se intentará buscar recorridos comunes para compartir la canaleta.
- También hay que cuidar el aspecto estético. Se intentará pasar las canaletas por sitios lo menos visibles posible.
- No deberán de estar en lugares ni demasiado accesibles por cuestiones de seguridad, ni en lugares de difícil acceso para facilitar el montaje y el mantenimiento.

Una vez considerados estos aspectos se realizó el diseño que se muestra en el anexo E, se ha adoptado este diseño a fin de evitar posibles interferencias producidas por agentes externos a la red (corrientes eléctricas, humedad, etc.) y además porque va a permitir disminuir la cantidad de canaletas y cable a usar, también es conveniente recordar que mientras más cortos sean los cables más capacidad de transmisión tendrán.

El cableado horizontal del edificio cumple con la máxima distancia horizontal permitida entre el Patch Panel y el terminal de conexión que es de 90 metros y con la longitud máxima del punto terminal hasta la estación de trabajo (cámara o PC) que es de 3 metros.

2.4.5 MONTAJE

2.4.5.1 Colocación de canaletas

Una vez que hemos decidido el recorrido por el que van a transcurrir las canaletas, procederemos a su colocación. Se comenzará por un extremo y se deberán de prever en que puntos van a confluir cada una de las canaletas finales que llevan tan solo los cables de cada una de las rosetas, con las de distribución por las que van varios cables hasta llegar al panel de parcheo.

El proceso a seguir será:

1) Medir la distancia que se quiere cubrir:

- Cámara 1: 33m
- Cámara 2: 50m
- Cámara 3: 60m
- Cámara 4: 77m
- Cámara 5: 19m
- Cámara 6: 43m
- Cámara 7: 40m
- Cámara 8: 51m
- PC de visualización: 28m

2) Cortar las canaletas a la medida apropiada. En el caso de tener que realizar algún ángulo de 90º, cortaremos los extremos de las canaletas a unir en inglete[25] con lo que se conseguirá un ajuste perfecto. La canaleta siempre se corta con la tapa puesta, con esto nos evitaremos tener que realizar dos cortes por separado, uno para el cuerpo de la conducción y otro para la tapa.

3) Pegar con varios trozos pequeños de cinta adhesiva de doble cara la canaleta a la pared. Este paso nos servirá solo de sujeción previa.

4) Sobre la canaleta prefijada taladrar los puntos necesarios para garantizar su perfecta sujeción a la pared. El número de agujeros dependerá de la longitud del tramo a fijar pero podría servir de referencia realizar un agujero cada metro o metro y medio.

5) Introducir los tacos fisher en cada uno de los agujeros realizados.

6) Poner los tornillos en cada uno de los tacos colocados con lo que dejaremos perfectamente sujeta la canaleta a la pared.

2.4.5.2 Fijación de las rosetas y el panel de parcheo

Las rosetas deben ser fijadas a la pared y el panel de parcheo deberá estar fijado en el respectivo rack con sus respectivos tornillos. Se tendrá en cuenta que la canaleta llegue justo hasta el borde de la caja para conseguir que no se vean ninguno de los cables que lleva en su interior.

[25] **Inglete:** corte transversal de 45º

El proceso a seguir es el siguiente:

1) Señalar en la pared con un lápiz los lugares donde se va a taladrar.
2) Realizar los agujeros necesarios.
3) Colocar los tacos en los agujeros pertinentes.
4) Atornillar las cajas a la pared.

2.4.5.3 Cableado

Para empezar habrá que llevar un cable desde cada una de las rosetas de conexión hasta el panel de parcheo. Las normas a tener en cuenta a la hora de trabajar con los cables son:

- No se deberá someter a los cables a tracciones fuertes. Nunca superiores a 10kg.
- Nunca debe doblarse un cable en un ángulo menor de 90º.
- En los lugares donde el número de cables sea elevado, se pueden usar presillas[26] para garantizar su inmovilidad pero sin presionar demasiado.
- No se debe trenzar el cable.

El proceso a seguir es:

1) Medir la distancia de cada uno de los tramos de cable a introducir en las canaletas. Es conveniente prever que hay que dejar un trozo de cable en cada uno de los extremos para permitir el trabajo de conexionado.
2) Cortar los cables a las medidas adecuadas.
3) Comenzar a introducir cables en la canaleta por el extremo de la roseta.
4) Conforme que el cable está siendo introducido en la canaleta, es conveniente ir poniendo la tapa a la canaleta para conseguir que no se salga con los movimientos y tracciones lógicas del proceso de trabajo.

[26] **Presillas:** Pequeño dispositivo que sirve para ejercer presión.

5) Cuando estemos trabajando en los tramos de distribución, o sea, en los lugares donde son varios los cables que hay que embutir, es conveniente introducirlos todos a la vez para no tener que abrir varias veces las tapas de las canaletas.

2.4.5.4 Conexión de las rosetas

El mecanismo usado en las rosetas esta compuesto por un conector RJ-45 hembra en su parte frontal con nueve conexiones para otros tantos hilos en su parte trasera. De los nueve, ocho son hilos para datos de información y el noveno se usa para conexión de masa.

Existen cables en el mercado que llevan protección de masa con una malla envolviendo a los hilos. Sin embargo en la mayoría de los casos no se usa esta protección ya que el propio trenzado de los hilos entre sí, protege de interferencias externas a la información transmitida por el cable. El proceso a seguir en la conexión del cable al mecanismo del conector es el que sigue:

1) Pelar el cable aproximadamente 3 cm, en este paso habrá que cuidar el no perforar el aislante que protege a los hilos de datos.
2) Abrir las trampillas con las que se cubren los contactos del mecanismo.
3) Comprobar la posición en la que conectaremos cada hilo del cable. El código de colores de cableado está regulado por la norma T568A.

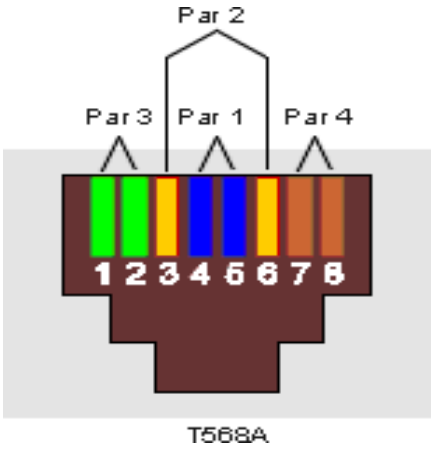


Fig. 2.42 Distribución de los pares en el conector

Tabla 2.7 Código de Colores T568A

Contacto	T568A
1	Blanco/verde
2	Verde
3	Blanco/naranja
4	Azul
5	Blanco/azul
6	Naranja
7	Blanco/marrón
8	Marrón
9	Masa

4) Realizar el destrenzado de los pares individuales del cable en un tramo menor a 1.25cm. Es interesante respetar esta norma por cuestión de protección de los datos.

5) La conexión de los distintos hilos a su respectivo contacto lo haremos de uno en uno. Para ello, tomaremos uno de los hilos y lo colocaremos en su contacto correspondiente entre las pequeñas cuchillas que tiene y llegando hasta el fondo donde encontraremos un hueco para apoyar el hilo.

6) Una vez el hilo en su sitio, cerrar la trampilla hasta escuchar un click, de esta forma conseguiremos que el hilo penetre entre las cuchillas del contacto y quede totalmente grimpado entre ellas, asegurando la conexión correcta.

Nota: *Debemos recordar que el hilo no hay que pelarlo ya que las propias cuchillas del contacto lo harán.*

2.4.5.5 Conexionado del panel de parcheo

La conexión de los distintos cables que llegan al panel, se realizará por su parte posterior en los distintos mecanismos de conexión de los que dispone, que son los mismos que los usados en la conexión de las rosetas, por lo que el proceso de conexión es el mismo.

Es conveniente recordar que hay que respetar el código de colores escrupulosamente, ya que de no ser así nos podremos encontrar con que el sistema no funcione o que funcione mal. De igual forma que con las rosetas usaremos la norma T568A. Es imprescindible que se use siempre la misma. No funcionaría la red si usamos un código de colores en las rosetas y otro en el panel de parcheo.

2.4.5.6 Construcción de los latiguillos

Los latiguillos son los cables que nos van a permitir conectar entre el panel de parcheo y el hardware del sistema (switch, router, Pc servidor). También se les llama latiguillos a los cables que van a servir para conectar cada uno de los elementos de la red (cámaras y PC's) a sus correspondientes rosetas de conexión, generalmente estos vienen incluidos en cada equipo.

Para la construcción de los latiguillos se puede usar el mismo tipo de cable UTP que se ha usado para la interconexión de dependencias, o sea el que va dentro de las canaletas, pero es recomendable usar uno multifilar en vez del unifilar usado en el cableado horizontal.

Este tipo de cable se adapta mejor a las cuchillas de los conectores RJ45 macho, por lo que se consigue mejor contacto y además es más flexible para soportar los movimientos.

El proceso de construcción del latiguillo es el siguiente:

1) Se corta un trozo de cable de la medida necesaria para cubrir cómodamente la distancia entre el panel de parcheo y el respectivo dispositivo. La práctica nos aconseja que el corte sea totalmente perpendicular al cable, ya que de esta manera se garantiza que la longitud de los hilos es siempre la misma.
2) Introducir en el cable la capucha de plástico del conector que va a cumplir funciones de sujeción y a su vez de protección.

3) Se cortará aproximadamente 1 cm del aislante de la cubierta en ambos extremos.

4) Se separan los hilos y se colocan en el orden determinado por el código de colores (norma 568-A) a usar. La numeración de los pines se hace tomando el conector con los contactos hacia arriba, el pin 1 es el de la izquierda (fig.2.43).

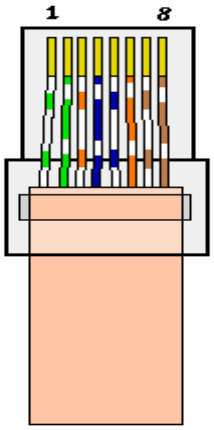


Fig.2.43 Pines Conector RJ45 macho

5) Se introducen los hilos en el conector RJ-45 macho hasta el final de éste respetando el orden de los hilos.

6) Introducir el conector en la herramienta de grimpar y presionar hasta escuchar el click que nos indica que el conector está seguro.

Fig.2.44 Herramienta de grimpar

7) Cubrir el conector con la capucha de plástico que ayudará a sujetar más el cable al conector.

2.4.5.7 Conexionado del switch

El switch estará apoyado en el rack cerca del panel de parcheo, las conexiones a realizar en el switch consisten en unir mediante latiguillos cada uno de los conectores usados en el panel del parcheo con una de las entradas del mismo. Esta es una de las grandes ventajas del sistema de cableado estructurado, ya que incorporar a la red local a cualquiera de las dependencias remotas es tan fácil como unir con un latiguillo su correspondiente conector en el panel de parcheo con el switch. El switch a usarse en este proyecto debe disponer de 16 entradas de conexión RJ45, 8 en cada uno de los laterales.

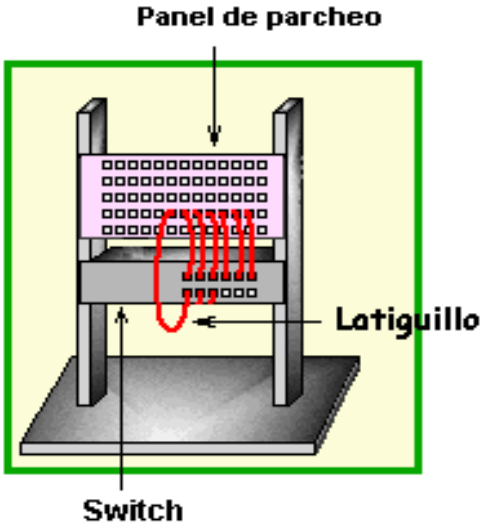


Fig.2.45 Colocación del Switch

Puede darse el caso de tener un switch con 16 entradas y necesitar más por la evolución natural del tamaño de la red, para ampliar el número de conexiones disponibles, se recurre a la interconexión de varios switch o concentradores.

2.4.5.8 Conexionado del router

El router irá colocado en el rack correspondiente a nuestro sistema. Las conexiones a realizar en el router son muy pocas. Hay que pensar que este dispositivo nos va a servir para interconectar nuestra red local con Internet a través de una línea telefónica del tipo RDSI.

El propio router trae los cables que debemos de usar para su interconexión. Para su conexión con la RDSI lo uniremos mediante un cable en cuyos extremos tiene conectores RJ45. Con respecto a su conexión con nuestra red, se integra como un dispositivo más, por lo que se conectará a una entrada del switch, la misma que está etiquetada "10 Base-T". Ambos cables en realidad pueden ser sustituidos por latiguillos normales y corrientes como los que hemos utilizado para conectar el switch o los de la unión de los dispositivos con las rosetas.

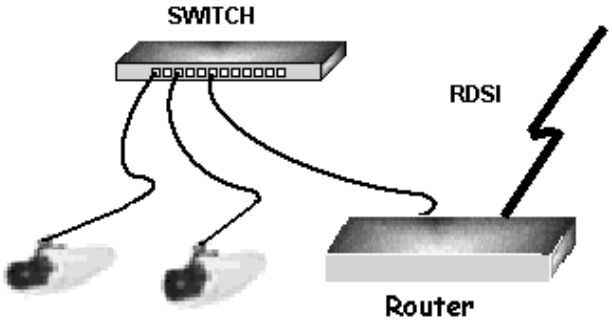


Fig.2.46 Conexión del router

A continuación presentamos un diagrama aproximado del sistema de videovigilancia IP a instalarse en el HB-11 “GALAPAGOS”.

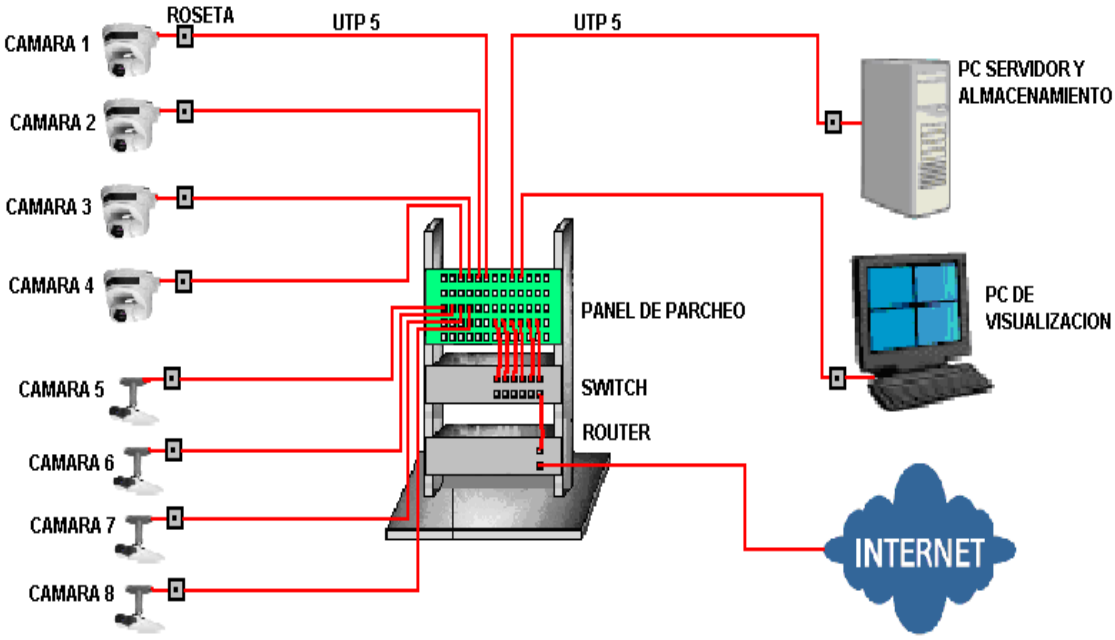


Fig.2.47 Sistema de Videovigilancia del HB-11

2.4.6 SOFTWARE

2.4.6.1 Sistema operativo

Como indicamos anteriormente usaremos Windows XP.

Fig.2.47 Sistema operativo

2.4.6.2 Configuración del servidor (HOST) a Internet

Para la conexión del Servidor a la Gran Red (Internet), debemos realizar los siguientes pasos:

1) Dar un clic en el Botón **Inicio**
2) Ubicarnos sobre **Panel de Control**, daremos clic

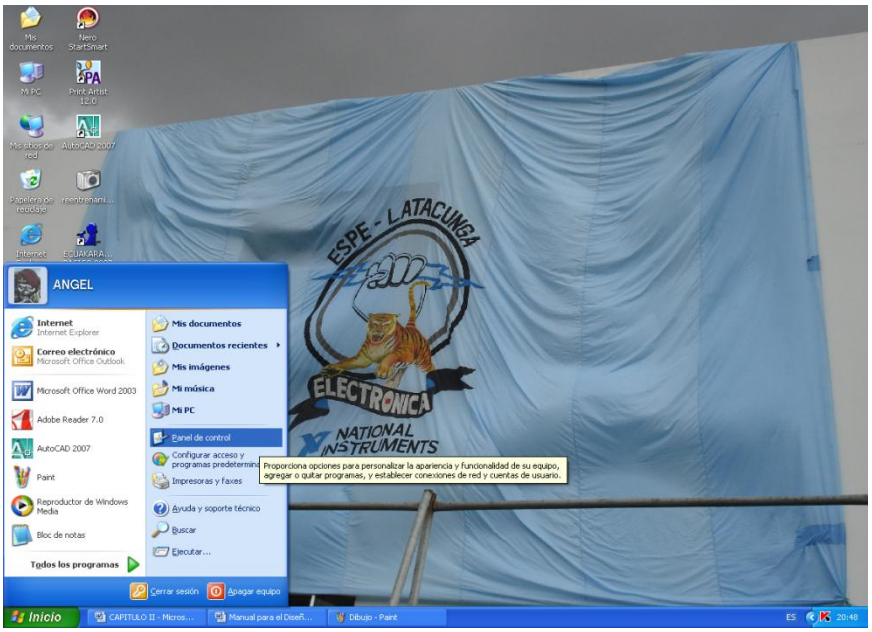


Fig.2.48 Ventana principal

3) Una vez allí nos posicionaremos sobre el Incono **Opciones de Internet**, daremos doble clic.

4) Luego saldrá una pequeña ventana, nos ubicaremos sobre la opción **Conexiones**.

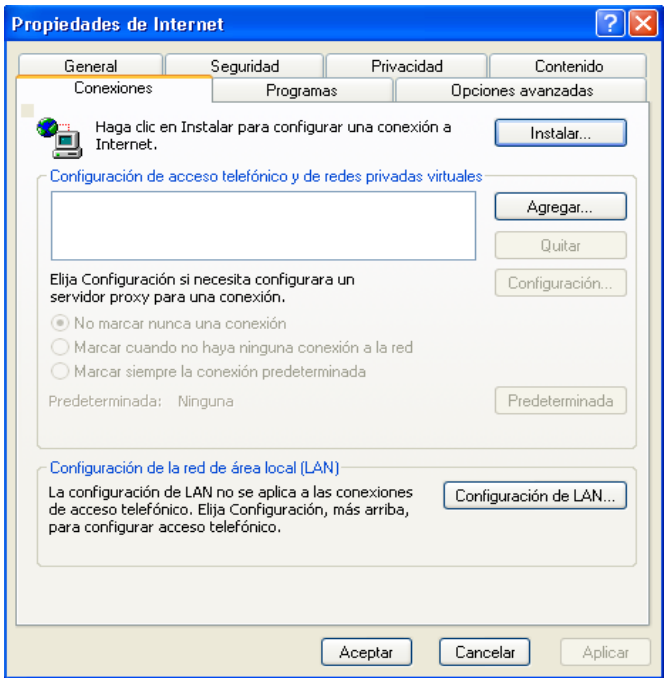


Fig.2.48 Ventana de propiedades de Internet

5) A continuación damos un clic en la opción **Instalar.**

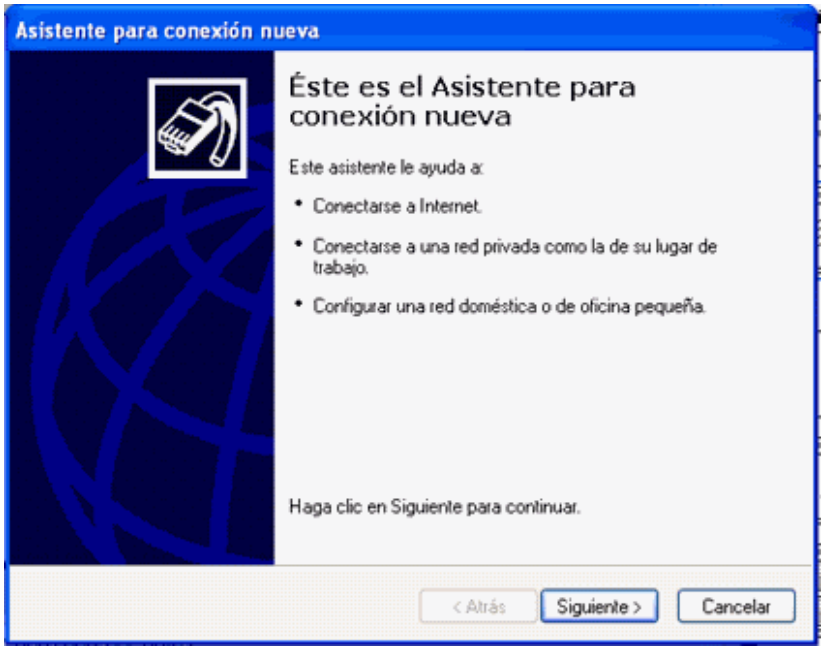


Fig.2.49 Asistente para conexión nueva

6) El siguiente cuadro muestra las diferentes conexiones que podemos utilizar, en este espacio solamente tomaremos la primera Opción que es **Conectarse a Internet** y le daremos un Clic en Siguiente.

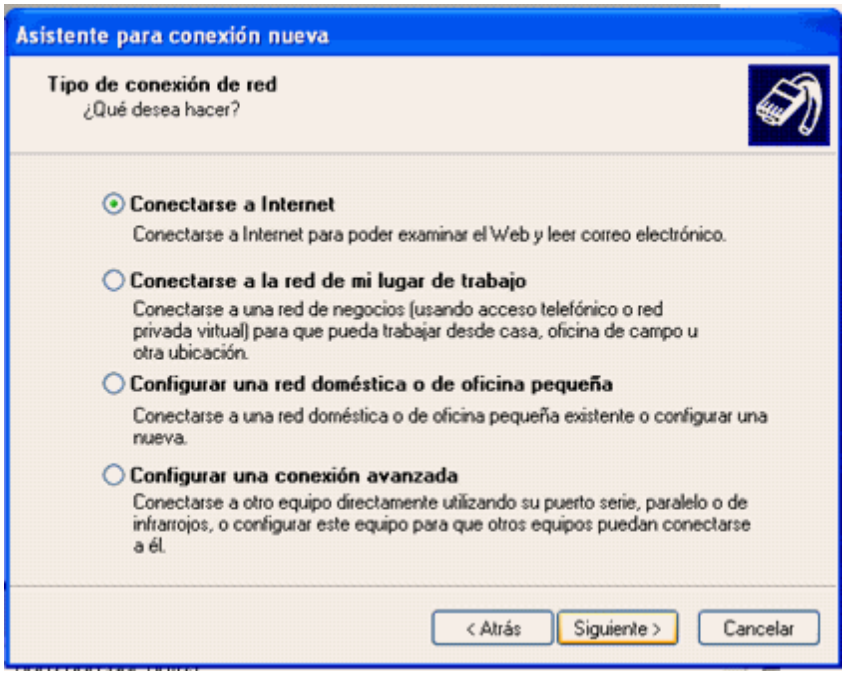


Fig.2.50 Opciones de conexión

7) A continuación se presentarán tres opciones de las cuales marcamos **Elegir una lista de proveedores de Servicios de Internet** (según el servicio que tengamos disponible).

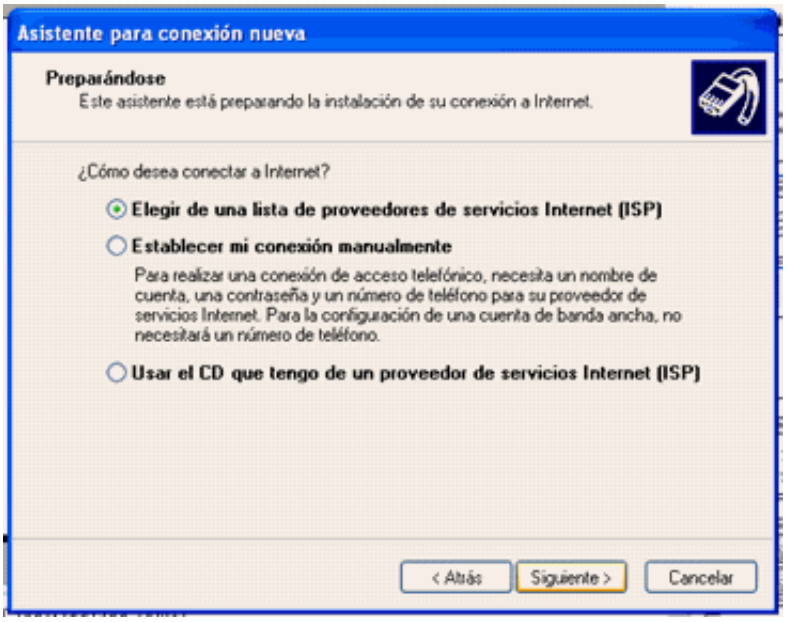


Fig.2.51 Elección de proveedor de Internet

8) Luego de haber tomado la decisión daremos un clic en **Siguiente** para continuar con la conexión.

Fig.2.52 Finalización del asistente

9) Luego que aparezca el siguiente cuadro daremos un clic en **Finalizar** para terminar la instalación.

2.4.6.3 Configuración del Servidor (HOST)

La configuración de HOST es muy sencilla solamente se debe proporcionar algunos códigos o protocolos que nos exige el computador para comenzar a programar nuestro servidor así como las estaciones de trabajo.

A continuación los pasos a seguir para esta configuración:

1) Abrir la barra de menú Inicio, dar un clic en la opción de **Panel de Control**.
2) Hecho esto ubicaremos el icono de **Conexiones de Red**, dando doble clic.

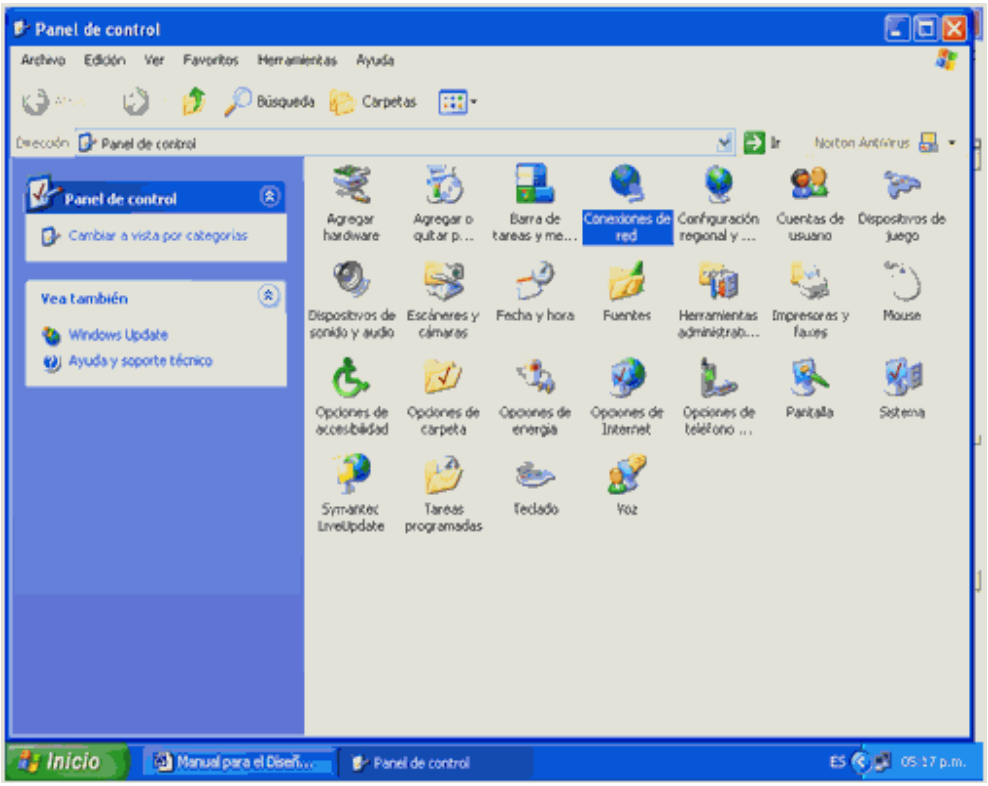


Fig.2.53 Panel de control

3) Luego nos enfocaremos en la parte superior izquierda de la pantalla, en un icono llamado **Configurar una Red domestica o para Oficina**. Nos posicionaremos sobre este icono y daremos doble clic sobre el mismo.

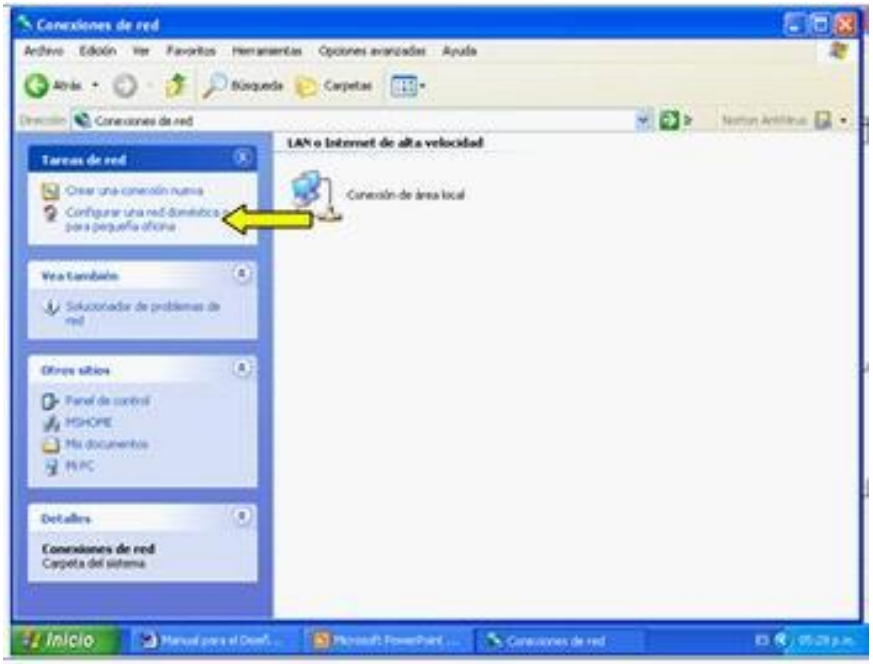


Fig.2.54 Ventana Conexión de red

4) A continuación seguiremos las instrucciones que nos indique el Ordenador. Luego tendremos una ventana que nos preguntara como deseamos conectar el equipo, tendremos tres opciones solamente tomaremos la primera opción **Este equipo se conecta directamente a Internet. Los otros equipos se conectan a Internet a través de mi Equipo.**

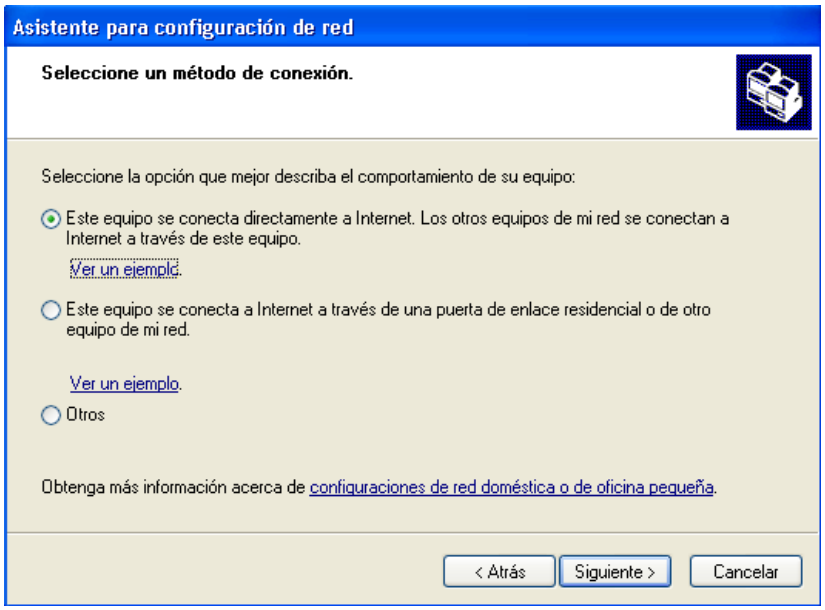


Fig.2.55 Ventana método de conexión Servidor

5) Seguidamente continuaremos dando un clic en el botón **Siguiente**, aparecerá otra pantalla que pedirá nombre y descripción del equipo.

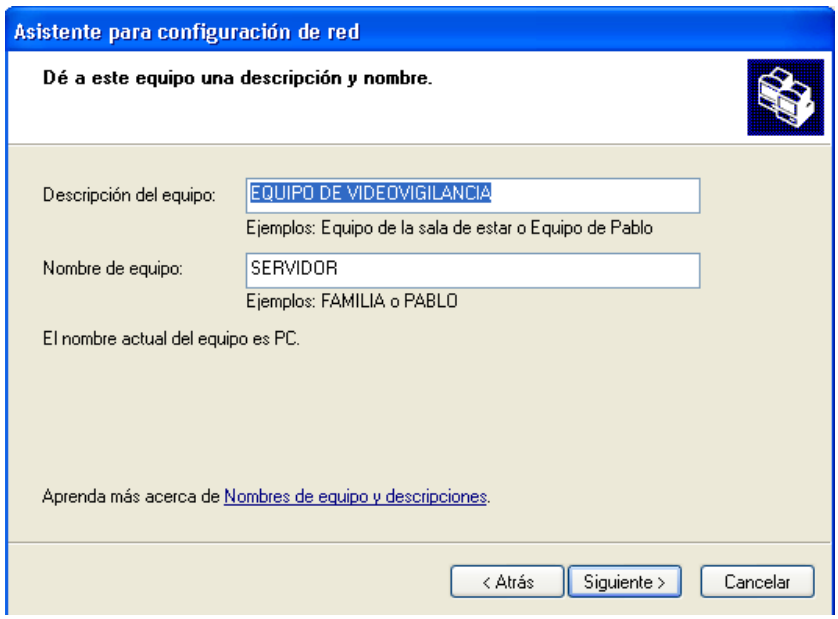


FIG.2.56 Descripción y nombre de equipo

6) Luego aparecerá otra pantalla que pedirá Nombre del Grupo de Trabajo.

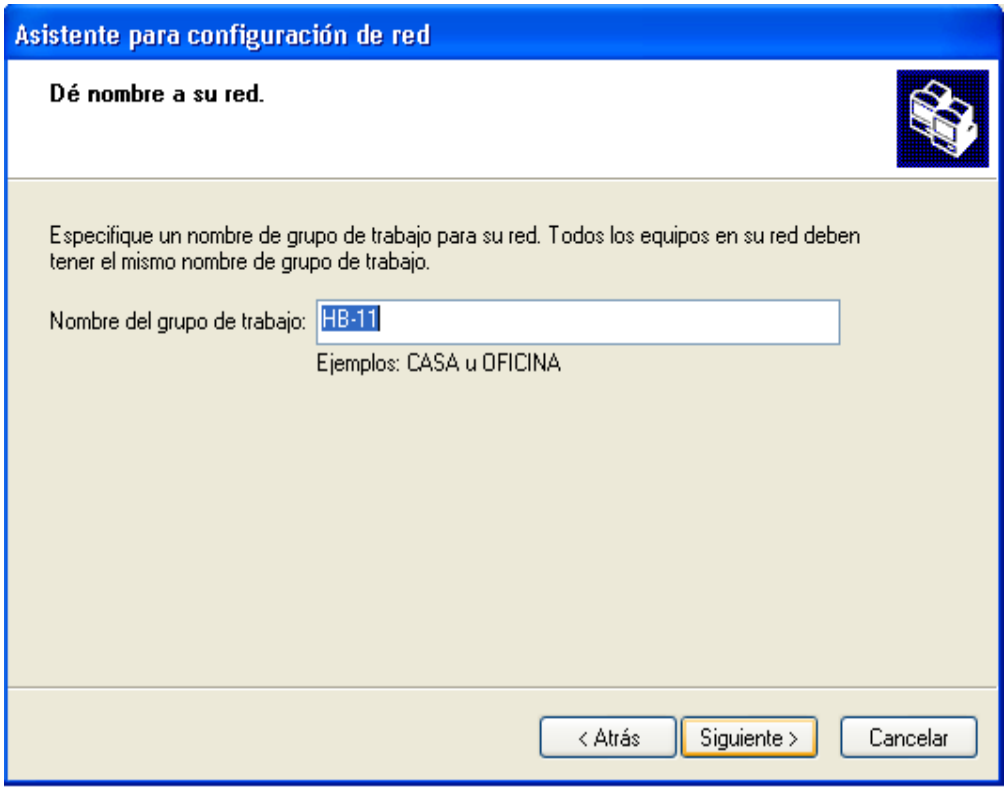


Fig.2.57 Ventana para el Acceso a Nombre de la Red

7) Una vez terminados de configurar los datos del ordenador pulsamos el botón **Siguiente**, aparecerá otra pantalla que proporcionará todos los datos que recientemente se configuraron, ya confirmados todos los datos pulsaremos el botón **Siguiente** y seguiremos las instrucciones del Ordenador para culminar la instalación del Servidor (HOST).

8) Después de haber hecho esto saldrá una ventana que pedirá espera, eso es porque está terminando de configurar los datos de la red, esto puede tardar varios minutos.

9) Luego de que el Ordenador termine de configurar los datos saldrá otra pantalla que dará una serie de opciones, tomaremos solamente la opción **Finalizar el Asistente.**

2.4.6.4 Configuración de los protocolos (IP), Mascara de Subred y Puerta de Enlace para el Servidor

1) Para realizar estas configuraciones tendremos que abrir la ventana **Conexiones de Red** ubicada en el **Panel de Control**, como ya lo habíamos hecho en la ocasión anterior.

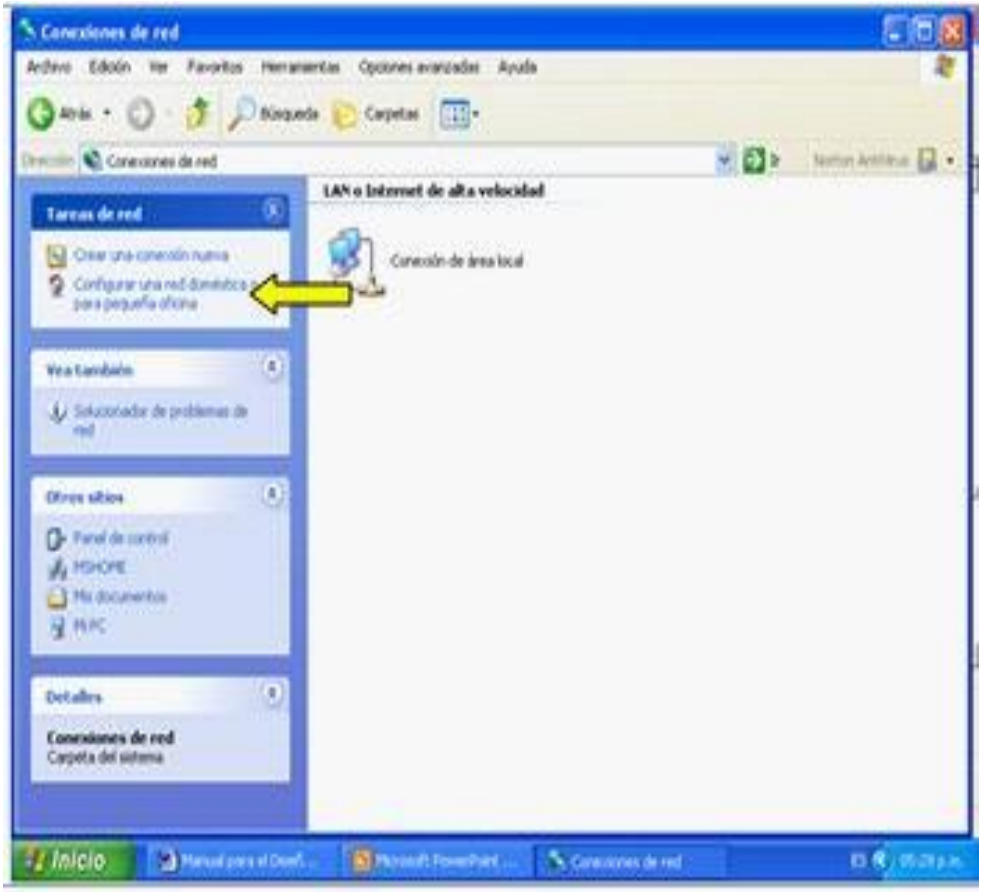


Fig.2.57 Ventana Conexión de red

2) Daremos un clic con el botón derecho del Mouse en el icono **Conexión de Área Local**, luego aparecerá una pequeña ventana, daremos un clic en el botón **Propiedades**.

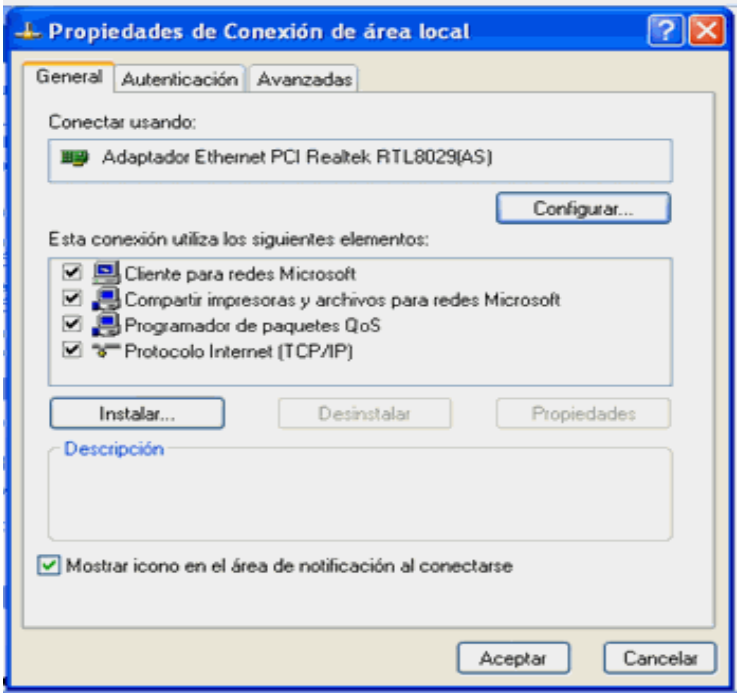


Fig.2.58 Propiedades de conexión de área local

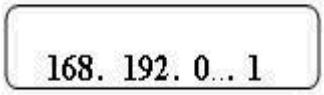
3) Luego buscaremos la opción que dice **Protocolo Internet (TCP/IP)**, nos ubicaremos sobre del mismo y a continuación daremos doble clic. Una vez hecho esto tendremos una pequeña pantalla que dirá. Propiedades de Protocolo Internet (TCP/IP).

Fig.2.59 Propiedades de Protocolo Internet (TCP/IP)

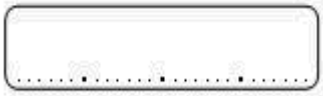
4) En esta pantalla tendremos la dirección IP, la mascara de Subred y la puerta de Enlace predeterminada. En cada opción procederemos de la siguiente manera:

En la dirección IP aparecerá de esta forma……

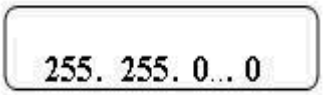
La rellenaremos de esta manera……



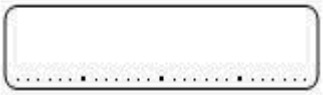
La Mascara de Subred aparecerá……



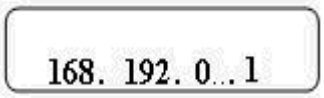
Quedará de esta forma…….



Puerta de Enlace predeterminada……..



Quedará así ……...



Una vez que terminada esta operación podemos proseguir con la configuración de la Estación de Trabajo (PC de visualización).

2.4.6.5 Configuración de la Estación de Trabajo (PC de visualización)

Para realizar esta configuración procederemos como en el caso de la configuración del servidor (HOST), con la diferencia que en el asistente para configuración de red en la selección de método de conexión seleccionaremos la opción **Este equipo se conecta a Internet a través de una puerta de enlace residencial o de otro equipo de mi red.**

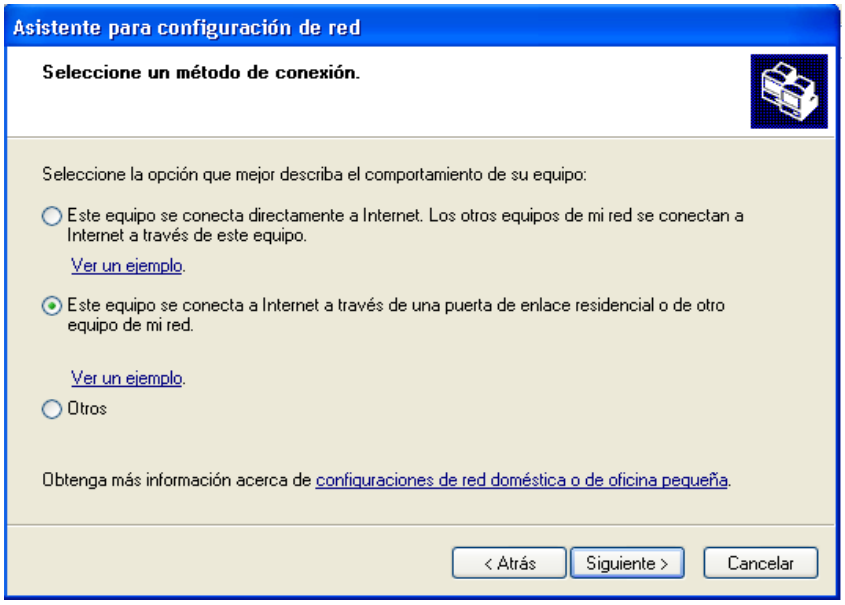
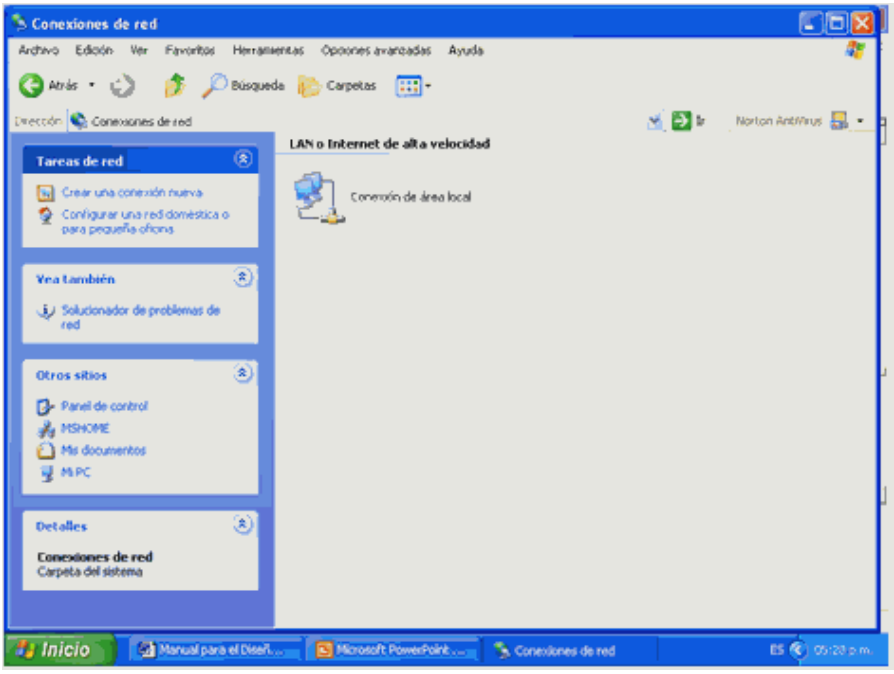


Fig.2.60 Método de conexión Estación de trabajo

2.4.6.6 Configuración de los protocolos (IP), Mascara de Subred y Puerta de Enlace para las Estaciones de Trabajo

1) Tendremos que abrir la ventana **Conexiones de Red** ubicada en el **Panel de Control**, como lo hicimos en la ocasión anterior.



2.61 Ventana conexiones de red

2) Daremos un clic con el botón derecho del Mouse en el icono **Conexión de Área Local**, luego aparecerá una pequeña ventana, que dirá **Estado de conexión de Área Local**.

Fig.2.62 Estado de conexión de área local

3) Luego que aparezca esta ventana, daremos un clic en el botón **Propiedades** ubicado en la parte inferior izquierda de la ventana. Después que aparezca esta pantalla buscaremos la opción que dice **Protocolo Internet (TCP/IP)**. Nos ubicaremos encima del mismo y a continuación daremos doble clic

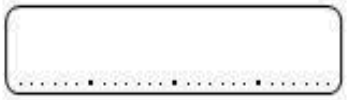
Fig.2.63 Propiedades de conexión de área local

4) Una vez que hayamos hecho esto tendremos una pequeña pantalla que dirá **Propiedades de Protocolo Internet (TCP/IP)**.

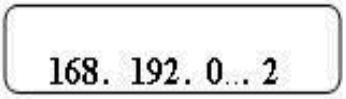
Fig.2.64 Propiedades de Protocolo Internet (TCP/IP)

5) Dentro de esta pantalla tendremos la dirección IP, La mascara de Subred y La puerta de Enlace predeterminada. Dentro de estas opciones haremos lo siguiente:

En la dirección IP aparecerá de esta forma……

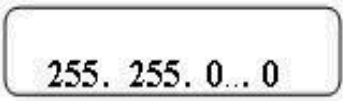


La rellenaremos de esta manera……

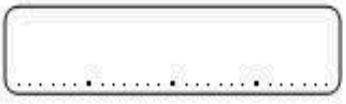


La Mascara de Subred aparecerá…….

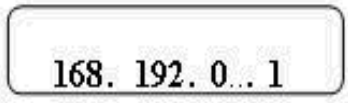
Quedará de esta forma…….



Puerta de Enlace predeterminada……..



Quedará así ……...



Nota: *La dirección IP cambiará un digito mas para cada estación.*

Ejemplo: *En la primera estación tendremos el IP.* ***168.192.0.2****, ya que el primer digito (1) pertenece al Servidor (HOST), a medida que vamos avanzando de Estaciones tendremos que agregar un digito mas. Si la primera Estación fue* ***168.192.0.2*** *la segunda Estación será* ***168.192.0.3*** *y así sucesivamente. Por otra parte la Mascara de Subred será siempre* ***255.255.0.0*** *para todas las Estaciones. Con respecto a la puerta de Enlace siempre será* ***168.192.0.1****, porque simplemente la puerta de enlace será siempre la misma ya que el Protocolo o el IP del Servidor es* ***168.192.0.1*** *es decir es el código que nos permite acceder a Internet mediante el Servidor.*

2.4.6.7 Comprobación de la Conexión

El primer pasó será encender todas las Estaciones de Trabajo (PC y cámaras IP) conectadas a la red, asegurándonos de que el Servidor este conectado a Internet y que el concentrador este encendido y funcionando.

Para constatar si las estaciones están conectadas con el Servidor abrimos el **Panel de Control**, damos doble clic sobre el icono de **Conexiones de Red,** ubicamos en el lado izquierdo una pequeña pantalla llamada **Otros Sitios**, se dará un clic sobre el nombre de nuestra red, aparecerá otra ventana en la parte superior izquierda de la pantalla, allí damos un clic en **Ver Equipos de Red.** Siguiendo estos sencillos pasos tendremos una vista completa de todos los equipos conectados a la red, de allí podremos monitorearlos y acceder a ellos.

2.4.6.8 Software de gestión de vídeo

El software de gestión de vídeo que funciona sobre un servidor Windows, establece la base para la grabación, análisis y monitorización de vídeo. Se encuentra disponible una amplia gama de software que se basa en las necesidades de los usuarios. Un navegador web estándar proporciona la visualización adecuada para muchas aplicaciones de vídeo IP, utilizando la interfaz web integrada en la cámara IP o el servidor de vídeo, especialmente en

aquellos casos en que una o unas pocas cámaras se visualizan simultáneamente. Existe una amplia gama de software de gestión de vídeo disponible, para el presente proyecto la mejor opción es Software IPView, sirve para monitorizar varias cámaras, detección de movimiento, captura de imágenes y grabación de video (sólo para Windows)

Fig.2.65 Monitoreo con IPView

El servidor de cámaras IPVIEW es el software perfecto para el monitoreo remoto y la transmisión en tiempo real de eventos a través de Internet o una red. El IPVIEW funciona con una o más cámaras de vídeo IP que le permite visualizar eventos en vivo con su navegador Web mediante Internet o Intranet. Se pueden gestionar remotamente hasta 16 cámaras con este software. El servidor de cámaras de Internet cuenta con transmisión de vídeo en tiempo real en calidad MPEG, captura automática de imagen y notificación de evento vía correo electrónico que hacen de ésta una solución ideal para aplicaciones de transmisiones de vídeo en Internet.

Nota: *Cada uno de los equipos que conformarán nuestro sistema, disponen de su propio software (cd de instalación) el cual es suministrado por los fabricantes y generalmente son fáciles de entender por el usuario, únicamente se debe tener en cuenta que sea compatible con los requerimientos de nuestro sistema (Protocolo, Sistema operativo, etc.).*

III. CAPITULO

RESULTADOS DEL SISTEMA

3.1 INTRODUCCIÓN

El presente proyecto esta basado en una alternativa tecnológica viable en lo que a sistemas de video vigilancia se refiere, para lo que se ha realizó la investigación de diversos productos y sistemas que brinden las condiciones adecuadas para que sean posteriormente instaladas en el HOSPITAL DE BRIGADA No. 11 “GALAPAGOS”.

Para el desarrollo del presente sistema se seleccionaron dispositivos de gran desempeño y funcionalidad. Dicha determinación se la realizó con el propósito de cumplir con una importante finalidad de nuestro proyecto el cual es el desarrollo de un sistema rápido, confiable y que otorgue las garantías necesarias al momento de ponerlo en funcionamiento.

Los equipos utilizados son de marcas reconocidas, que se acogen a protocolos y normas bajo las cuales se ha desarrollado el proyecto, dando aceptación al sistema en todos los parámetros de vigilancia por video.

Si bien es cierto los costos de algunos elementos se ven un poco elevados, esto se debe a que la tecnología utilizada para el proyecto es de última generación, que nos otorga grandes ventajas en comparación a otras que no lo pueden hacer, por otro lado creemos que si utilizamos este tipo de tecnología veremos ha futuro resultados positivos, sabiendo que la inseguridad es parte del diario vivir, es por eso que debemos estar siempre alertas y porque no dar utilidad a estos sistemas de video vigilancia con características de acorde a un mundo tecnificado.

3.2 ANÁLISIS EN BASE A SISTEMAS EXISTENTES

Es más fácil destacar las ventajas del vídeo IP si consideramos las desventajas del circuito cerrado de TV analógico. Los sistemas de vídeo basados en fibra o cable coaxial son limitados en muchos sentidos.

3.2.1 INSTALACIÓN

Sistema IP: No lleva asociada altos costes ni profundas modificaciones en el edificio, únicamente necesitamos cable de red o podemos utilizar el cableado de alguna red ya existente.

Sistema analógico: Suele ser más costoso, normalmente hay que llevar cableado de alimentación, otro de video y otro de toma a tierra.

3.2.2 ACCESIBILIDAD REMOTA

Sistema IP: El usuario puede acceder al vídeo en tiempo real en cualquier momento desde cualquier ordenador conectado a la red, esté donde esté. El vídeo puede almacenarse en ubicaciones remotas, por motivos de comodidad o seguridad, y la información puede transmitirse a través de la red LAN o de Internet.

Sistema analógico: La visualización únicamente se la puede realizar de manera centralizada desde el centro de monitoreo.

3.2.3 ESCALABILIDAD Y FLEXIBILIDAD

Sistema IP: Para ampliar una solución de vídeo IP basta con añadir las cámaras una a una. El proceso es rápido: normalmente sólo se tardan unos minutos en sacar el producto de la caja, conectarlo y empezar a enviar imágenes a través de la red.

Sistema analógico: La matriz analógica es el componente que proporciona flexibilidad al centro de control de los sistemas de circuito cerrado de TV analógicos. Sin embargo, ésta no puede ampliarse sin añadir hardware nuevo y depende de la situación. Por lo tanto, su capacidad total de ampliación, esto es, su costo de expansión, es bastante limitada.

.

3.2.4 ALMACENAMIENTO

Sistema IP: Almacena tanto tiempo y cantidad de imágenes como se desee (en función de la capacidad de los discos duros). El almacenamiento de las imágenes en el disco duro de un computador puede configurarse para minimizar la redundancia y es sencillo hacer una copia de seguridad de su contenido. Los grabadores de vídeo en red protegen las grabaciones incluso cuando un grabador deja de funcionar o se destruye.

Sistema analógico: A pesar de que el lanzamiento de los grabadores de vídeo digitales (DVR) ha mejorado la capacidad de grabación de los circuitos cerrados de TV, éstos también tienen limitaciones. Tienen que estar instalados cerca de la matriz analógica y a menudo se compromete la tasa de transmisión y la calidad de imagen.

3.2.5 CONTROL

Sistema IP: En caso de emergencia, la capacidad de control puede transferirse fácilmente a cualquier otro punto de la red, ya sea en el mismo lugar o en otro diferente. Las redes redundantes permiten que el sistema siga funcionando incluso cuando falla un enlace o un interruptor. El hecho de contar con un sistema basado en una red posibilita diagnósticos a través de todo el sistema para garantizar que todo funciona correctamente. Cada dispositivo se puede controlar continuamente y, si falla cualquier cosa se activa una alarma.

Sistema analógico: En un sistema analógico los dispositivos se tienen que controlar manualmente para garantizar una operación sin problemas y existe la posibilidad de que un fallo pase desapercibido durante un largo periodo de tiempo. Este problema existe especialmente en los DVR, ya que no siempre se señalan los fallos y se pueden perder durante mucho tiempo las grabaciones de todas las cámaras. Los sistemas analógicos pueden ejecutar diagnósticos limitados dependiendo de los diferentes componentes que se usen, pero esto no forma parte integral del sistema.

3.2.6 RENTABILIDAD

Sistema IP: El vídeo IP es muy rentable por muchos motivos, en una solución de vídeo IP, hay menos equipos que mantener que en un sistema analógico tradicional y, por tanto, menos componentes susceptibles de desgaste. Las imágenes se almacenan en discos duros informáticos, que son una solución más práctica y económica que las cintas de vídeo.

Sistema analógico: La opción de realizar una ampliación del sistema es prohibitiva, debido a la costosa inversión que se necesitaría para sustentar un cambio de infraestructura, por la gran cantidad de material que se emplearía.

3.2.7 DESVENTAJAS DEL SISTEMA IP

A pesar de ser un sistema con innumerables ventajas, existen ciertos aspectos negativos que parecen existir en torno a la videovigilancia IP:

- Escasa diversidad de cámaras para su elección y utilización en distintas aplicaciones así como adaptarlas al entorno.
- El costo por cámara es bastante más elevado que las cámaras analógicas CCTV (aunque reduce el coste en cableado y su instalación).

- Aunque con nuevas tecnologías de compresión se reduce el consumo de ancho de banda, la tasa de grabación de frames se limita mas y por tanto es inferior que en los sistemas Mixtos-IP.
- La seguridad de las transmisiones y las posibles intrusiones, al igual que ocurre con cualquier red de este tipo, los fabricantes han desarrollado una serie de barreras que ofrecen las máximas garantías: firewalls, redes privadas virtuales, protección con contraseña. En estos momentos las posibilidades de ataques dependen en buena parte de lo cuidadoso que sea el usuario.

La tecnología IP avanza de manera acelerada y segura, a pesar de estos aspectos negativos, que seguramente en base a estudios y experimentación serán solucionados en poco tiempo.

3.3 ANÁLISIS TÉCNICO

En la actualidad existen un sinnúmero de dispositivos en el mercado, pero, para una selección adecuada hemos tomado en cuenta aspectos como:

- La compatibilidad con normas y estándares de nuestro sistema.
- Procurar equipos que sean de marcas y empresas posicionadas en el mercado (3com, cisco, vivotek, etc.).
- Tomar como referencia equipos que ya están instalados y en operación.
- Lograr un equilibrio entre bondades técnicas y costo.
- Disponibilidad en el mercado.

3.3.1 CÁMARAS IP

Para realizar una comparación entre cámaras IP a continuación presentamos las principales características técnicas de cada una:

Tabla 3.1 Características técnicas cámaras IP

	AVI201 (AVTECH)	**DCS2120 (D-Link)**	**VI-IP7131 (VIVOTEK)**	**VI-PT7135 (VIVOTEK)**	**VI-PZ6112 (VIVOTEK)**
Puerto LAN	SI	SI	SI	SI	SI
Protocolos	DDNS, PPPoE, DHCP, NTP, SNTP, TCP/IP, ICMP, SMTP, FTP, HTTP, RTP, RTSP	TCP/IP,HTTP, SMTP,FTP, NTP,DNS, DHCP,PPPoE	TCP/IP.HTTP, SMTP,FTP,Telnet, NTP, DNS y DHCP Ethernet 10/100 Mbps Ethernet RJ-45	TCP/IP.HTTP, SMTP,FTP,Telnet, NTP, DNS y DHCP Ethernet 10 Base T o Fast 100 Base T	TCP/IP.HTTP, SMTP,FTP,Telnet, NTP, DNS, DDNS y DHCP Ethernet 10 Base T o Fast 100 Base T
RAM	32MB RAM	NE	32MB SDRAM	32MB SDRAM	16MB SDRAM
Sensor de Imagen	1/3.6" image sensor	CMOS	VGA CMOS	CMOS 1/4”	Sensor CCD 1/4” Color
Video	MPEG4 / MJPEG	MPEG-4	MPEG4	MPEG4. JPEG	MPEG4, MJPEG
Micrófono	NE	NE	SI	SI	SI
I/O	NO	NE	SI	NE	SI
Alimentación	DC12V, 0.5ª	5 V DC	12 Vdc, PoE 802.3af	100-240VAC 50/60Hz, 0.4 A	100-240VAC 50/60Hz, 0.4 A
Sistema Operativo	Windows XP, Windows 2000 Server, ME, 98, DirectX 9.0	NE	Windows: 2000, XP	Windows 98SE/ME/2000/ XP	Windows 98SE/ME/2000/ XP
PANTILT	80° / 55.6°	NO	NE	horizontal 350º; vertical 125º	horizontal 270º; vertical 135º
ZOOM	NE	NE	digital 4X	NE	x10 óptico x10 Dígital
Iluminación	1 lux	1.4 lux	1.5 lux	1 lux	1.5 lux
Seguridad	PASSWORD	NE	Clave de acceso	Clave de acceso	Clave de acceso
Temperatura	0—40 ºC	NE	0—40 ºC	0—40 ºC	0—40 ºC
Dimensiones	152.5mm (L) 115.2 mm(W) 40.2 mm(H)	11,43cm (L) 7,87cm (W) 4,06cm (H)	12.64cm (L) 9.62cm (W) 4.74cm (H)	NE	NE
Precio (USD)	**125.28**	**250**	**282.96**	**305.60**	**780.97**

***NE:** No Especifica

3.3.1.1 Cámara para interiores

En base al cuadro comparativo anterior, se ha determinado que la mejor opción para aplicarse en interiores es la cámara **VI-IP7131** de **VIVOTEK,** en vista de que es totalmente compatible con nuestro sistema sobre todo en lo que se refiere a conexión LAN, protocolos, compresión de video y sistema operativo.

Fig.3.1 cámara VI-IP7131 de VIVOTEK

Adicionalmente nos proporciona un buen nivel de seguridad (clave de acceso), a pesar de no poseer movimiento horizontal/vertical (PANTILT) tiene un Zoom digital 4x lo cual lo hace ideal para trabajar en los pasillos interiores del HB-11 “GALAPAGOS”.

Aunque es la de mayor precio de las cámaras fijas ofertadas, ve compensado su costo al evitar cableado adicional para alimentación ya que posee PoE.

La completa ilustración de sus características la podemos observar en el anexo F.

3.3.1.2 Cámaras para exteriores

Para esta aplicación la mejor opción es la **VI-PT7135** de **VIVOTEK**, al igual que en el caso anterior satisface nuestros requerimientos técnicos.

Fig.3.2 Cámara VI-PT7135 de VIVOTEK

Su movimiento horizontal (350º) y vertical (125º) así como su rango de temperatura de trabajo (0-40ºc) la hacen perfecta para cubrir las áreas exteriores del edificio del HB-11 “GALAPAGOS” y trabajar en las condiciones climáticas que presenta la zona, además el contar con una clave de acceso le proporciona un buen nivel de seguridad.

Las especificaciones para la alimentación (100-240VAC, 50/60Hz, 0.4 A) la hacen compatible con la red pública de alimentación sin necesidad de ningún dispositivo adicional. Su precio nos da un excelente nivel entre costo y bondades técnicas.

Un completo análisis de sus características técnicas se lo puede hacer en el anexo G.

3.3.2 SWITCH

Primeramente debemos realizar una comparación de los equipos más adecuados que el mercado nos presenta.

Tabla 3.2 Características técnicas de los Switch

	4210 PWR 18-Port (3com)	**FSH-1608PoE (Ovis-Link)**	**High Performance Network Switching (Advantek Networks)**
Puertos	18	16	16
Velocidad	10/100mbps	10/100mbps	10/100mbps
Interfaces	16 RJ-45 10BASE-T/100BASE-TX	RJ-45 10/100	Rj-45 x 16Nwqy switching ports Soporta Auto MDIX
Soporte	auto-negociación full-duplex half-duplex	Full/Half dúplex Por puerto	Full-Duplex, Half – Duplex
Plug-and-play	SI	SI	NE
PoE	Todos los puertos	8 puertos	8 puertos
Precio (USD)	660	357.50	156.45

Una vez expuestas las características técnicas de los diferentes equipos, el que más se ajusta a nuestras necesidades es el **4210 PWR 18-Port** de **3com**, ya que es un dispositivo potente pero fácil de utilizar, permite que los usuarios conecten un puerto de cualquier tipo a un nodo de 10Mbps ó 100Mbps para multiplicar el ancho de banda, mejorar los tiempos de respuesta y realizar pesadas cargas de trabajo.

Fig.3.3 Switch 4210 PWR 18-Port de 3com

Una de las características principales que nos lleva a elegir este equipo es que, sus 18 puertos tienen alimentación PoE, que lo hace compatible con la cámara **VI-IP7131**, lo que conlleva un ahorro en el cableado y por ende un ahorro en el costo.

Otra de las características es la marca 3com la misma que goza de alto prestigio en el mercado por la alta tecnología empleada en sus equipos y la eficiencia

demostrada en sus aplicaciones en varias instituciones de prestigio (la ESPEL entre ellas), esto hace que a pesar de ser la de mayor precio es la que mejor garantías nos ofrece.

El anexo H nos da una amplia visión de las características técnicas de este equipo.

3.3.3 ROUTER

A diferencia de los casos anteriores, esta vez seleccionaremos de manera directa un equipo que cubra nuestras necesidades y sea de una marca reconocida, ya que pesar de existir una gran variedad de productos en el mercado, la mayoría son de marcas desconocidas y sin respaldo, es por esta razón que nos hemos inclinado por el router **CISCO** de la serie **1700**, principalmente por tratarse de una marca de sólido prestigio, que incluso le ha permitido presentar sus equipos en aplicaciones de simulación.

Fig.3.4 Router CISCO1700

Los routers CISCO de la serie 1700 proporcionan un rápido, fiable y seguro acceso a Internet y a redes remotas a través de diferentes tecnologías de acceso WAN de alta velocidad.

3.3.4 PC (MONITOREO Y SERVIDOR/ALMACENAMIENTO)

Para el sistema de monitoreo con las cámaras IP, esta tienen un software propietario y se instalará en un computador Pentium IV el mismo que generará una pantalla con cada evento que sucediese.

De igual forma para el sistema de almacenamiento se utilizara un computador de igual características tomando en cuenta el diseño de este sistema de almacenamiento y para optimizar una alta capacidad de entrega, gran capacidad y tolerancia a fallas se pueden utilizar varios métodos de almacenamiento anteriormente expuestos en capítulo II.

Las principales características del computador las indicamos a continuación:

- Marca: XTRATECH
- Procesador: Pentium IV
- Velocidad: 3.2 GHz
- Memoria RAM: 512 Mbytes
- Espacio en disco: 120 Gbytes
- Sistema Operativo Windows XP

Para el computador de monitoreo se necesita de una pantalla de alta definición para lo cual se propone utilizar un monitor **LCD AOC 2230Fh** que tienen las siguientes características:

- Pantalla: LCD de 22”
- Tiempo de respuesta: 2 mseg
- Resolución: 1,680 x 1,050 pixeles o 720 x 1,080

Fig.3.5 Monitor LCD AOC 2230Fh

Adicionalmente posee una entrada por HDMI compatible HDCP, también integra lector de tarjetas 4 en 1 y un HUB USB, altavoces de bajo perfil integrados.

3.4 ANÁLISIS ECONÓMICO

Para el proyecto propuesto vamos realizar un estudio del costo, para lo cual se detallan los principales equipos a usarse en el sistema de videovigilancia IP y sus respectivos valores.

3.4.1 EQUIPOS

En este punto cabe destacar que en lo correspondiente a cámaras y switchs, después de un profundo análisis en sus características, desempeño, soporte, marca y disponibilidad en el mercado se ha llegado a la conclusión de utilizar los que brinden mejores resultados.

Esto no significa que hemos dejado de lado al resto de equipos, en estos casos al no existir mayores variantes en lo que a características técnicas se refiere se ha optado por las de marca de renombre y que ofrecen garantías.

En la tabla 3.3 se muestra el costo en equipos:

Tabla 3.3 Costo de equipos

DESCRIPCION	UNID.	P.U.(USD)	P. TOTAL(USD)
Cámaras interiores	4	282.96	1131.84
Cámaras exteriores	4	305.60	1222.40
Switch	1	660.00	660.00
Router	1	320.00	320.00
CPU	2	450.00	900,00
Monitor de 22”	1	380,00	380,00
Costo total para la adquisición de equipos			**4614.24**

Nota: *Los precios no incluyen IVA.*

3.4.2 EXTRAS Y COMPLEMENTARIOS

Otro rubro importante que generará la implantación de este sistema de videovigilancia IP, es la necesidad de una plataforma segura y confiable de cableado estructurado categoría 5, tomando en cuenta lo que corresponde a cableado y sus respectivos accesorios. A continuación se detallan los valores correspondientes a la implantación del cableado estructurado:

Tabla 3.4 Costos de Cableado

SUMINISTRO DE CABLEADO ESTRUCTURADO	UNID	P.U.(USD)	P.T.(USD)
Cable UTP unifilar CAT5	400m	0,15	60.00
Cable UTP multifilar CAT5	50m	0,20	10.00
Rosetas	20	1,50	30,00
Canaletas (2m)	110	1.70	187.00
Conectores RJ45 (macho)	20	0.30	280.00
Costo total para la adquisición de equipos			**567.00**

Nota: *precios no incluyen IVA.*

Hay que señalar que para este proyecto no se incurrirán en gastos por mano de obra, en vista de que en el caso de aprobarse el presente proyecto, estaría dentro de nuestras funciones y obligaciones la instalación del sistema (sin remuneración extra). En el caso de necesitar asesoría técnica sobre todo en lo que a equipos se refiere, esta será proporcionada por las empresas que nos suministrarán los mismos sin ningún recargo adicional.

Finalmente ponemos a consideración el monto total (sin IVA) que representaría la implantación del sistema:

COSTO DE EQUIPOS	4614.24
COSTO DE CABLEADO	567.00
COSTO TOTAL DEL SISTEMA	**5181.24 (USD)**

IV. CAPITULO

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- Mediante el presente trabajo se cumplió con uno de los principales objetivos de nuestro proyecto, el cual es el desarrollo de un sistema seguro y confiable, que otorgue las garantías necesarias tanto a los usuarios como al personal que labora en el HB-11 “GALAPAGOS”.

- Otro de los objetivos cumplidos es el poder ofrecer una alternativa tecnológicamente viable en lo que a sistemas de videovigilancia se refiere, para lo que se ha realizó la investigación de diversos productos y sistemas los que en conjunto permitieron convertir en realidad el mencionado principio.

- Para el desarrollo del diseño de este proyecto se escogieron dispositivos de gran aceptación en el mercado, al ser de marcas reconocidas, que se acogen a protocolos y normas bajo las cuales se ha desarrollado el proyecto, desde los pequeños conectores RJ45 hasta las sofisticadas cámaras IP.

- También se ha proporcionado un sistema que puede ser expandido, en el caso de un aumento de la infraestructura del edificio y por ende de sus servicios.

- En función de la accesibilidad remota se pone a disposición un sistema capaz de enlazarse desde cualquier parte del mundo, haciendo que el personal encargado de la seguridad pueda realizar el monitoreo desde otro lugar que se encuentre fuera del perímetro del edificio.

- La aplicación de la tecnología IP se la ha realizado basándose en los protocolos y normas de comunicación, interactuando con el lenguaje de los sistemas de seguridad, creando una plataforma capaz de recibir y poner en funcionamiento tecnologías y aplicaciones a futuro tales como sistemas 3G.

- La capacidad de crecimiento de este sistema de seguridad sobre una plataforma inalámbrica es otra de sus fortalezas, ya que permitirá llegar a lugares de difícil acceso, en el caso de no poder hacerlo con el cableado.

- La tecnología utilizada para el proyecto es una tecnología de última generación, que nos otorga capacidades que otras no nos pueden brindar.

- Finalmente podemos concluir que los análisis tanto técnicos como económicos demostraron que el proyecto es totalmente viable.

4.2 RECOMENDACIONES

En el aspecto técnico es recomendable explotar al máximo las bondades que este sistema nos ofrece, especialmente en lo que se refiere a entradas y salidas digitales, ya que mediante estas podemos configurar un sistema de seguridad integral, que incluya sensores (infrarrojos, magnéticos, etc.) y dispositivos de alarma.

También se debe tomar en cuenta que las empresas que proporcionen los equipos, den las respectivas garantías, así como también den las prestaciones necesarias sobre todo en lo que a mantenimiento y asesoría técnica se refiere.

Ya que el presente trabajo, está realizado en base a estudios técnicos y económicos, que lograron el diseño de un sistema con un alto nivel tecnológico con un costo moderado, es de vital importancia que sea tomado como base para la implementación física del mismo (en caso de aprobarse el proyecto).

Se hace necesario que se den el impulso y las facilidades necesarias, para que proyectos innovadores como este, sean aplicados en beneficio de la seguridad institucional. Creemos que el precio del sistema es mínimo en comparación con las bondades que presta, además debemos considerar que ningún precio es alto siempre y cuando nos dé la garantía de que bienes y sobre todo las personas estén bajo una total y absoluta **"seguridad"**.

BIBLIOGRAFÍA

Leon W.Couch II, SISTEMAS DE COMUNICACIÓN DIGITALES Y ANALÓGICOS, (5ta Edición, 1998).

Scott Keagy, INTEGRACION DE REDES DE VOZ Y DATOS, (Primera Edición, 2001).

Wayne Tomasi, SISTEMAS DE COMUNICACIONES ELECTRÓNICAS, (4ta Edición, 2003).

http://www.monografías.com

http://www.telefonica.com/whitepaper/imagenio.pdf

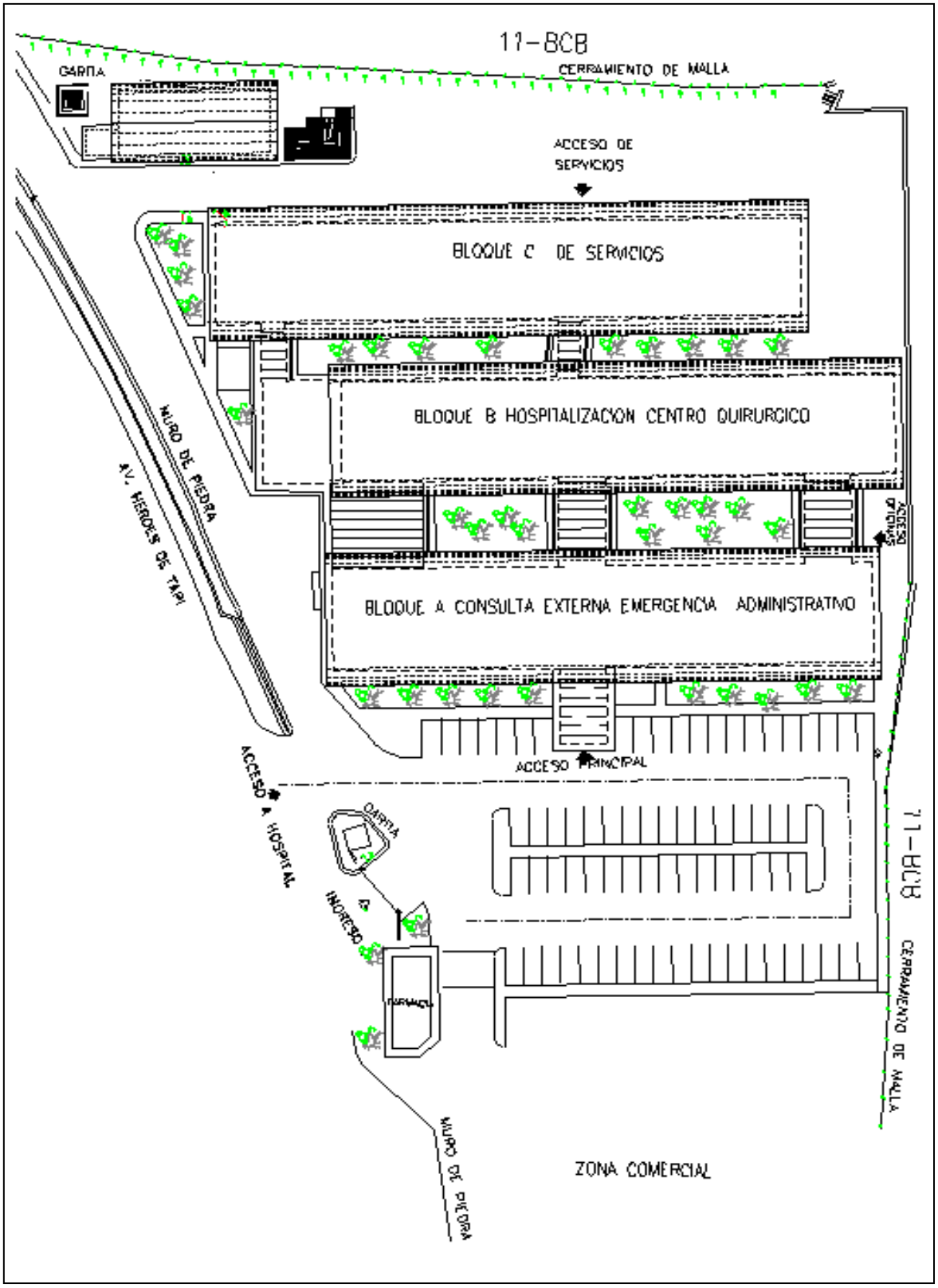
http://axis.com/whitepaper/video%vigilancia%IP.pdf

http://verint.com/videosolutions/whitepaper.asp

http://www.cisco.com/warp/public/146/pressroom/1999/oct04/15.html

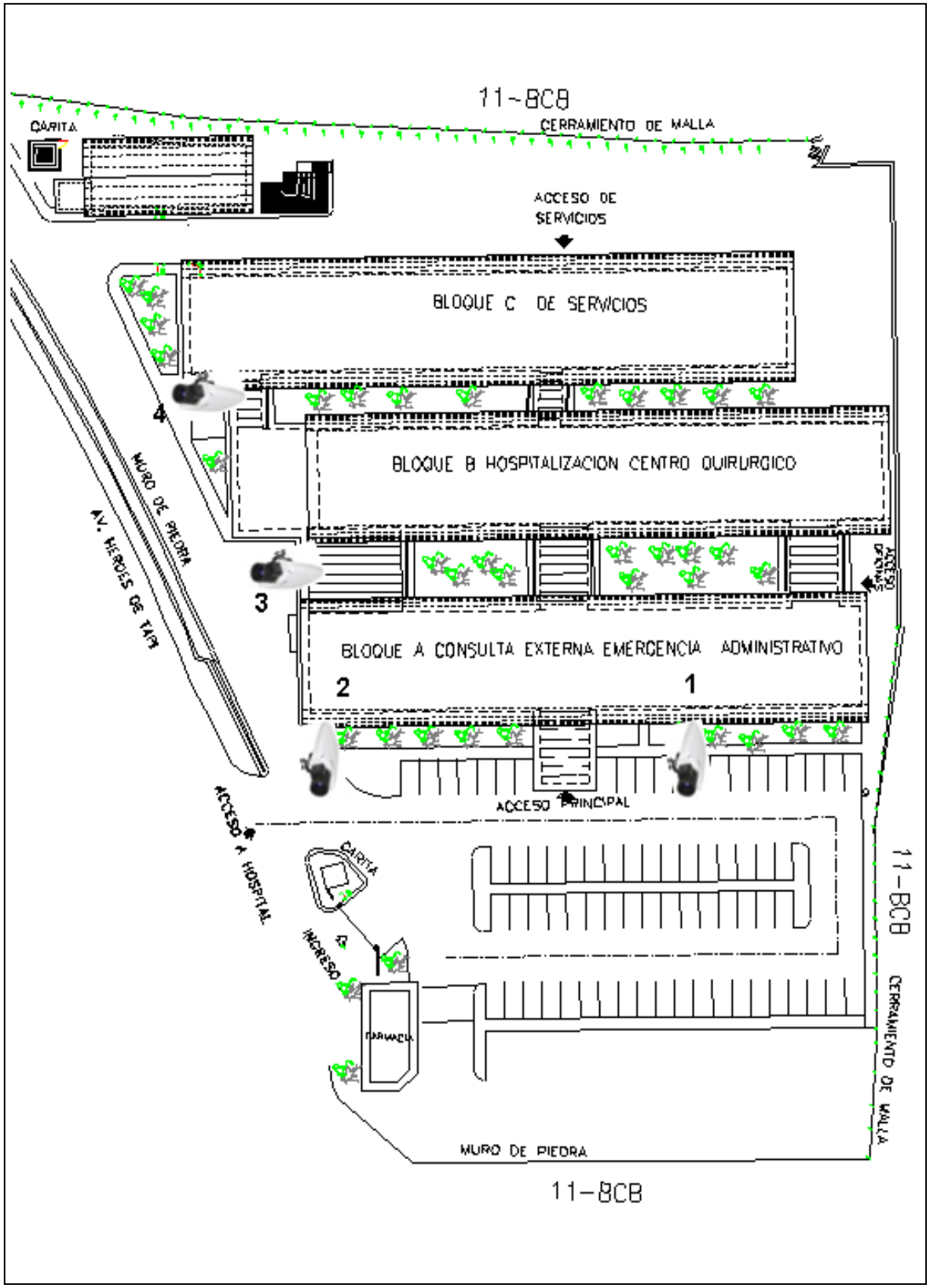
ANEXO A

HB-11 "GALÁPAGOS"

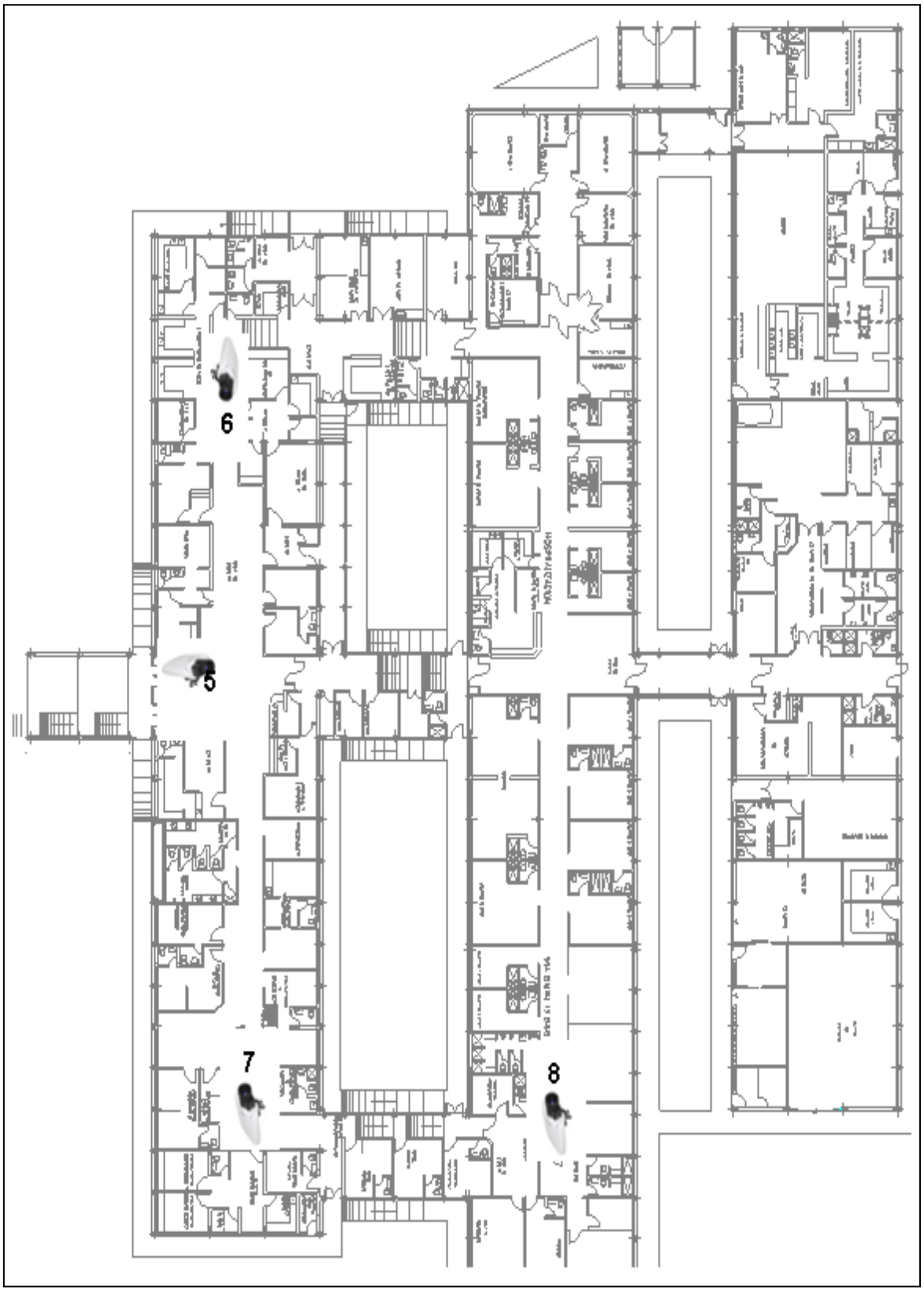


ANEXO B
ZONIFICACIÓN

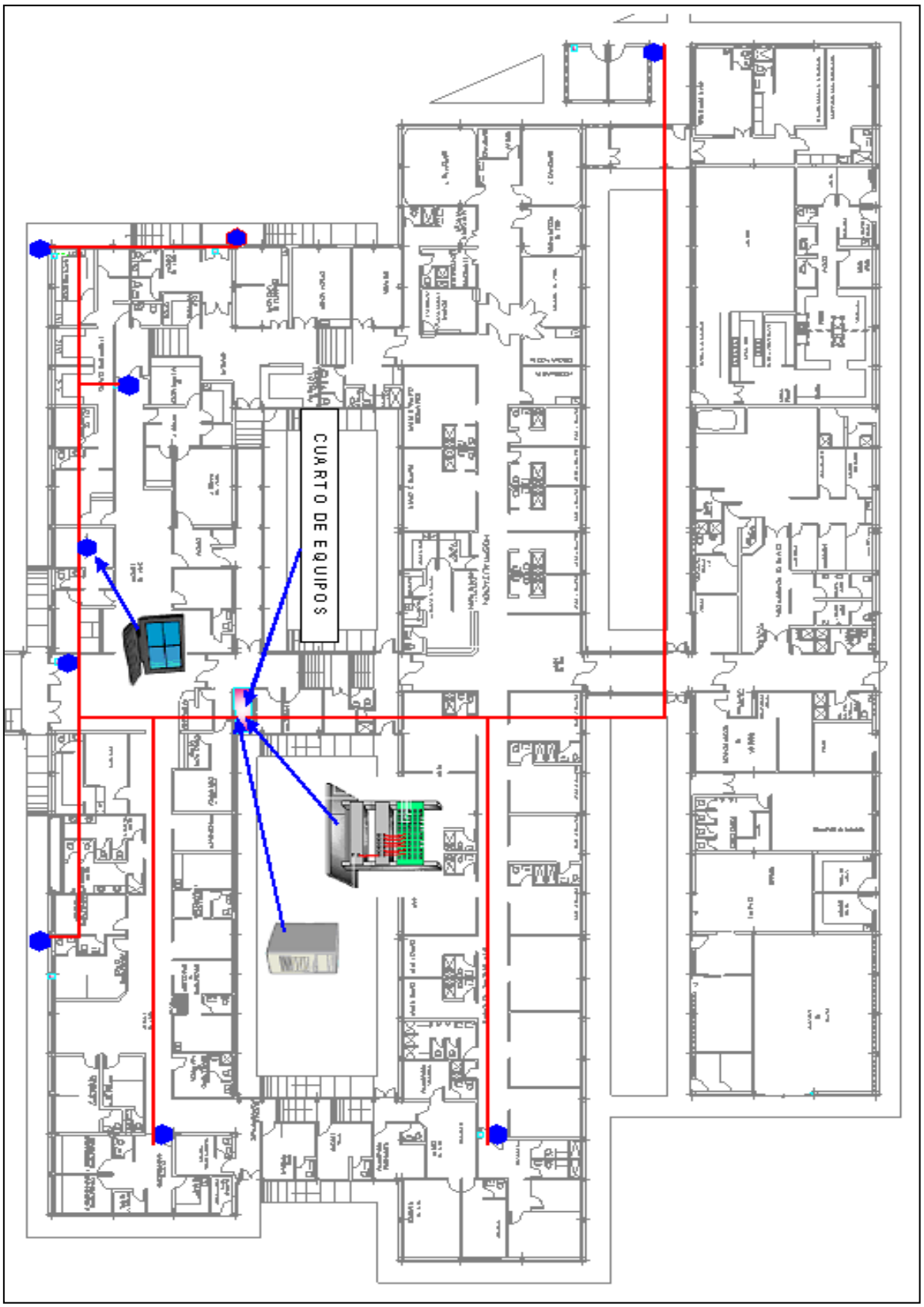
ANEXO C
CÁMARAS EXTERNAS



ANEXO D
CÁMARAS INTERIORES



ANEXO E
CABLEADO ESTRUCTURADO



ANEXO F

VIVOTEK Cámara IP COLOR VI-IP7131

Cámara a Color DIGITAL
Transmite vía TCP/IP
LAN – WAN – INTERNET

VIVOTEK

Sistema de vigilancia que transmite vía TCP/IP usando compresión MPEG4 30 fps

- *Cámara IP compatible 3GPP/ISMA, ofrece calidad de imagen superior con optimización del ancho de banda, permitiendo que los usuarios puedan acceder al video y audio transmitido desde sus PC's, celulares o adaptadores multimedia con TV en cualquier momento.*
- *Incluye software que permite visualizar hasta **16 cámaras en simultáneo** y **grabación en PC remota***
- *Compresión MPEG4 real 30 fps en resolución VGA*
- *Sistema PoE incorporado (Power over Ethernet)*
- *Soporta vigilancia móvil 3GGP*
- *Salida digital I/O para sensor externo y alarma*
- *Micrófono incorporado*
- *Clave de acceso (protección)*
- *Detección de movimiento inteligente*
- *Ancho de banda ajustable*
- *Zoom digital 4X - Soporta UPnP & IP dinámico - Fotos de pre y post alarma*

ESPECIFICACIONES TECNICAS

SISTEMA
CPU: VVTK-1000 SoC
RAM: 32MB SDRAM
ROM: 4MB FLASH ROM
Sensor de Imagen: VGA CMOS
Embedded OS: Linux 2.4

Networking: Protocolo: TCP/IP, HTTP, SMTP, FTP, Telnet, NTP, DNS y DHCP
Ethernet 10/100 Mbps Ethernet RJ-45

Video: MPEG4
Resolución: 30 frames hasta 640x480

Cámara: CMOS Sensor 1/4"
Resolución 640 x 480
Iluminación mínima 1.5 Lux / F2.0
AGC, AWB, AES
Iris Electrónico: 1/60—1/15,000 segundos
Lente fijo 4.0mm F2.0

Audio: Soporta GSM-AMR
Bit rate: GSM-AMR: 4.75k-12.2k
ACC: 16k a 128k

Dimensión: 12.64(L) x 9.62(W) x 4.74(H) cm
Peso: Neto 276 gramos

Alimentación: 12 Vdc, PoE 802.3af

Temperatura: 0—40 °C, humedad 20-80% RH

Aprobaciones: CE, FCC, PSE

Requerimientos para visualizar
OS: Windows: 2000, XP
Browser: Internet Explorer 5.x mínimo
Cellphone: 3GPP placer
Real Placer 10.5
Quick Time 6.5^Packed Video Placer 3.0

ANEXO G

VIVOTEK Cámara IP COLOR C/Pantilt VI-PT7135

Cámara a Color DIGITAL con Movimiento Horizontal 350° Tx TCP/IP:LAN –WAN– INTERNET

VIVOTEK

La Solución completa para GRABACION y TRANSMISION por internet de Audio y Video usando compresión MPEG4

- *Cámara IP compatible 3GPP/ISMA, ofrece calidad de imagen superior con optimización del ancho de banda, permitiendo que los usuarios puedan acceder al video y audio transmitido desde sus PC's, celulares o adaptadores multimedia con TV en cualquier momento.*
- *Incluye software que permite visualizar hasta 16cámaras en simultáneo y grabación en PC remota*
- *PANTILT incorporado: horizontal 350°; vertical 125°*
- *Micrófono incorporado*
- *Clave de acceso (protección)*
- *Optima sincronización de audio & video*
- *Alta preformase, totalmente configurable*
- *Detección de movimiento inteligente con 3 niveles*
- *Fotos de pre y post alarma*
- *Web Server incorporado.*

ESPECIFICACIONES TECNICAS

CPU: VVTK-1000 SoC
RAM: 32MB SDRAM
ROM: 4MB FLASH ROM

Networking: Protocolo: TCP/IP. HTTP, SMTP, FTP, Telnet, NTP, DNS y DHCP
Ethernet 10 Base T o Fast 100 Base T

Video: MPEG4. Imagen y calidad ajustables, JPEG
Resolución: 30 frames a 160x120 / 176x120 / 352x240 / 640x480

Cámara: Sensor CMOS 1/4"
Resolución 640(H) x 480(V)
Iluminación 1 Lux / F2.0, AGC, AWB.
Iris Electrónico: 1/60—1/15,000 segundos

Lente: tipo tarjeta 4.0 mm F2.0
Micrófono: Omni Direccional

Pan/Tilt : Pan +175° a –175°
Tilt +90° a –35°

Alimentación: 100-240VAC,50/60Hz, 0.4 A
Salida: 12VDC, 1.2A 6-15VDC min. 15W
Temperatura: 0—40 °C, humedad 95%RH

Aprobaciones: CE, FCC
Requerimientos para visualizar
Protocolo estándar TCP/IP
OS: Windows 98SE/ME/2000/XP
Browser: Internet Explorer 5.x mínimo
Cellphone: 3 GPP placer
Real Placer 10.5
Quick Time 6.5, Packet Video Placer 3.0

ANEXO H

− Conmutación 10/100 de Nivel 2 básica totalmente administrable y de clase empresarial a un precio asequible − Rendimiento wire-speed, sin bloqueo − Diseño de configuración fija y plug-and-play, de modo que el conmutador funciona de inmediato − Disponible en seis modelos: de 9, 18 y 26 puertos, con o sin PoE − El control de acceso a la red IEEE 802.1X ofrece seguridad basada en estándares, combinada con autenticación RADIUS − Apilamiento en cluster de hasta 32 dispositivos (Switch 4210, 4200G, 4500G, 5500 y 5500G) − Puertos SFP que soportan conexiones Gigabit y Fast Ethernet de fibra, facilitando así la migración de la red − El acceso a dispositivo autenticado mediante RADIUS (RADA) permite la autenticación de los dispositivos conectados mediante la dirección MAC, para un nivel adicional de seguridad de los puntos de entrada a la red − Los modelos Power over Ethernet proporcionan alimentación eléctrica y conectividad de datos sobre un mismo cable Ethernet − Sistema operativo común compartido por todos los conmutadores empresariales de 3Com, que simplifica la configuración y administración continua − Diseño sin ventilador, silencioso y de mayor eficiencia energética para los modelos sin PoE; resultan idóneos para su ubicación sobre una mesa o en un armario de cableado

Conmutación 10/100 de Nivel 2 totalmente administrable, con funcionalidades de clase empresarial

El 3Com® Switch 4210 es una familia de conmutadores de LAN 10/100 básicos de Nivel 2 con funcionalidades de QoS, seguridad y administración de clase empresarial, que proporciona un alto valor para los administradores de redes que necesitan un dispositivo económico de acceso a la red.

Los modelos Power over Ethernet (PoE) disponibles resultan idóneos para instalaciones de conectividad de red inalámbrica y de voz sobre IP; están también disponibles modelos sin PoE para una sencilla expansión de puertos. Todos los modelos incluyen enlaces ascendentes Gigabit y funcionalidad de apilamiento en cluster.