



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

**PROPUESTA DE UN DISEÑO DE INGENIERÍA PARA
UN SISTEMA DE VIDEO VIGILANCIA IP EN LA
FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN**

TESIS PROFESIONAL

**QUE PARA OBTENER EL TÍTULO DE INGENIERO
ELÉCTRICO ELECTRÓNICO**

P R E S E N T A

MOISÉS RAMÍREZ CUAUTLE

ASESOR DE TESIS

ING. JOSÉ LUIS PÉREZ BÁEZ



MÉXICO, D.F.

2014



Universidad Nacional
Autónoma de México

Dirección General de Bibliotecas de la UNAM

Biblioteca Central



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

DEDICATORIA

A mis padres Moisés Ramírez Monroy y Laura Cuautle Mosqueda, por el apoyo incondicional que siempre me han brindado durante toda la etapa de mi formación académica, así como, ser los pilares fundamentales en mi vida.

Con una especial dedicación a mis abuelos, que me acompañan desde donde quiera que estén y me ayudaron a formarme, estuvieron conmigo durante mi educación y son parte de ese motor que me impulsa a seguir.

AGRADECIMIENTOS

A la Universidad Nacional Autónoma de México, que gracias a esta gran y noble institución, me ha dado la oportunidad de incursionar en el hermoso mundo del saber, además, la oportunidad de llevar la imagen de la UNAM hacia el extranjero y demostrar que en México existe una Universidad, una Universidad donde existe la excelencia académica.

A mi hermana Laura Ramírez Cuautle, por su apoyo durante mi vida académica y ser un ejemplo a seguir.

A Nayelli García Delgado, por alentarme y brindarme su completo apoyo durante el desarrollo esta Tesis.

A mi asesor de Tesis y profesor José Luis Pérez Báez, por su conocimiento transmitido dentro y fuera de las aulas, así como su valioso apoyo durante el desarrollo de este trabajo de investigación.

A mis sinodales, por creer en mí y por ayudarme a concretar esta etapa académica durante la carrera profesional como docentes y en este momento como jurado.

Honor y Gloria a mis padres y a la Universidad.

INTRODUCCIÓN

El siguiente trabajo de investigación se recopila en un total de siete capítulos.

En el primer capítulo nombrado “Antecedentes” del presente trabajo de investigación, se abordan los antecedentes de la video vigilancia, la forma en cómo ha evolucionado desde su concepción hasta la actualidad y como estos sistemas pueden implementarse en la Facultad de Estudios Superiores Aragón para ayudar a que tenga más seguridad y de esta forma combatir diversos factores de riesgo.

En el capítulo número dos, se recopila información fundamental con el propósito de dar un marco teórico que derive a una correcta explicación lo más completa posible de los sistemas de video vigilancia IP, señales de video, topologías de red, redes IP, dispositivos de grabación, medios de enlace, alimentación, entre otros; todo esto para facilitar la comprensión del diseño que se realiza en esta propuesta.

En el tercer capítulo, se describe la necesidad por la cual se ha decidido realizar este trabajo de investigación. Se describe la zona geográfica donde está localizada la Facultad de Estudios Superiores Aragón, así como las zonas que se consideran conflictivas a los alrededores.

En el capítulo número cuatro, se dan a conocer las necesidades de seguridad de los alumnos, identificando las principales zonas a vigilar y de esta manera dar una propuesta técnica para la solución de la problemática. Se incluyen gráficas mostrando los resultados de las encuestas y un mapa indicando las zonas de bajo, medio y alto riesgo.

En el capítulo cinco, se encuentran las cámaras que se utilizan en el diseño de la propuesta del sistema, indicando sus características y la importancia de la instalación en cada una de las zonas de la Facultad. Así mismo se desarrolla la red IP para el sistema, indicando direccionamientos, máscaras de red y submáscaras. Se pueden visualizar diagramas de ubicación de cada cámara así como diagramas de conexión del sistema de video vigilancia.

En el capítulo seis, se indica el presupuesto total que se llevaría en la implementación de esta propuesta. Se ha dividido la Facultad en 4 zonas, en cada una de estas se desglosa el costo por componente arrojando un subtotal y finalmente se hace la sumatoria de las 4 zonas y de esta manera se obtiene el presupuesto total del sistema

Objetivo

Diseñar un Sistema de Video Vigilancia IP para ser instalado dentro de la Facultad de Estudios Superiores Aragón con el fin de aumentar la seguridad y prevenir situaciones de vandalismo; reduciendo de igual forma el costo de la seguridad.

Objetivos Específicos

- Diseñar una red de telecomunicaciones a prueba de fallas para implementar un sistema de video vigilancia que cubra el interior del campus.
- Diseñar un proceso de vigilancia más eficiente al tener control de puntos de riesgo en una misma ubicación y un proceso más fácil.
- Vigilar el interior del campus cubriendo las principales rutas de tránsito de los alumnos para disminuir los casos de vandalismo.
- Vigilar los puntos donde el alumnado tiende a dañar las instalaciones para evitar dichos desperfectos.
- Identificar los puntos eficaces de grabación considerando variables de visión y distancia para optimizar los recursos de video vigilancia.
- Diseñar e implantar un proceso de seguimiento de seguridad para tener indicadores de evaluación del proyecto.
- Mejorar el servicio de seguridad de la FES Aragón para crear un ambiente acorde a una multidisciplinaria universitaria.

Justificación

Reducir situaciones de vandalismo en la la FES Aragón.

Aumentar la seguridad en Universidades que se encuentran en el estado de México.

Casos registrados en el campus de acoso, vandalismo, etc (en base a los casos registrados hacia la población universitaria)

La mega tendencia hacia la tecnología IP en las redes de telecomunicaciones.

Gasto que hace la escuela en temas de seguridad.

Hipótesis

1.- La implantación de un Sistema de Video Vigilancia IP dentro de la Facultad de Estudios Superiores Aragón hará que esta aumente su seguridad, teniendo mayor control de las personas que entren y salgan de la entidad académica. Así mismo, se obtendrá una reducción referente a las situaciones vandalismo hacia las instalaciones.

2.- Se espera que la disminución del gasto en vigilancia dentro de la FES Aragón disminuya en un 30%.

ÍNDICE

| | |
|---|-----------|
| CAPÍTULO I ANTECEDENTES | 1 |
| CAPÍTULO II CONSIDERACIONES TEÓRICAS..... | 4 |
| 2.1 SEÑAL DE VIDEO..... | 5 |
| 2.1.1 SEÑAL DE VIDEO ANALÓGICA | 5 |
| 2.1.2 SEÑAL DE VIDEO DIGITAL..... | 10 |
| 2.2 TOPOLOGÍAS DE RED. | 18 |
| 2.2.1 MODELO OSI | 22 |
| 2.2.2 MODELO IP | 25 |
| 2.3 REDES IP..... | 27 |
| 2.3.1 DIRECCIONAMIENTOS..... | 28 |
| 2.3.2 REDES Y SUBREDES | 32 |
| 2.4 CÁMARAS DE VIDEO | 35 |
| 2.4.1 CÁMARAS DE VIDEO ANALÓGICAS | 40 |
| 2.4.2 CÁMARAS DE VIDEO DIGITAL..... | 41 |
| 2.5 DISPOSITIVOS ESPECIALES DE GRABACIÓN DE VIDEO..... | 45 |
| 2.5.1 GRABADOR DE VIDEO DIGITAL (DVR) | 46 |
| 2.5.2 GRABADOR DE VIDEO EN RED (NVR)..... | 52 |
| 2.6 CABLEADO Y MEDIOS DE ENLACE..... | 53 |
| 2.6.1 CABLE DE PAR TRENZADO..... | 54 |
| 2.6.2 FIBRA ÓPTICA..... | 58 |
| 2.6.3 WI –FI..... | 65 |
| 2.7 SISTEMAS DE ALIMENTACIÓN DE ENERGÍA..... | 68 |
| 2.7.1 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA..... | 68 |
| 2.7.2 POE | 70 |
| CAPÍTULO III DESCRIPCIÓN DE LA PROBLEMÁTICA..... | 73 |
| CAPÍTULO IV METODOLOGÍA DE ANÁLISIS Y PROPUESTA TÉCNICA..... | 77 |
| 4.1 METODOLOGÍA DE ANÁLISIS..... | 78 |
| 4.1.1 INTRODUCCIÓN | 78 |
| 4.1.2 ¿EN QUÉ CONSISTE EL DISEÑO DEL SISTEMA DE VIDEO VIGILANCIA IP PARA LA FES ARAGÓN? ... | 78 |
| 4.1.3 DESARROLLO DE LA METODOLOGÍA DE ANÁLISIS | 79 |
| 4.2 PROPUESTA TECNICA..... | 86 |
| 4.2.1 IDENTIFICACIÓN DE ZONAS DE RIESGO | 86 |
| CAPÍTULO V DESARROLLO DE LA PROPUESTA TÉCNICA..... | 87 |
| 5.1 DESARROLLO DE LA PROPUESTA TÉCNICA | 88 |
| 5.2 TIPOS DE CÁMARAS DE VIDEO VIGILANCIA..... | 88 |

| | |
|--|-------------------|
| 5.2.1 DESCRIPCIÓN DE LAS CÁMARAS | 89 |
| 5.3 UBICACIÓN DE LAS CÁMARAS..... | 90 |
| 5.3.1 UBICACIÓN POR ZONAS DE LAS CÁMARAS..... | 92 |
| 5.4 TIPO DE INSTALACIÓN | 97 |
| 5.4.1 CABLEADO..... | 98 |
| 5.5 SISTEMA ELÉCTRICO | 99 |
| 5.6 SISTEMA DE CONEXIÓN DE CÁMARAS..... | 101 |
| 5.7 DIRECCIONAMIENTO Y CREACIÓN DE SUBREDES | 104 |
| 5.8 DIAGRAMA LÓGICO..... | 108 |
| <i>CAPÍTULO VI COSTOS DE IMPLEMENTACIÓN</i> | <i>110</i> |
| 6.1 PRESUPUESTO POR ZONAS | 111 |
| 6.1.1 DESARROLLO PRESUPUESTO ZONA 1 | 112 |
| 6.1.2 DESARROLLO PRESUPUESTO ZONA 2 | 113 |
| 6.1.3 DESARROLLO PRESUPUESTO ZONA 3 | 115 |
| 6.1.4 DESARROLLO PRESUPUESTO ZONA 4 | 116 |
| 6.2 PRESUPUESTO CENTRO DE CONTROL..... | 117 |
| 6.3 PRESUPUESTO TOTAL | 118 |
| <i>CAPÍTULO VII CONCLUSIONES Y RECOMENDACIONES.....</i> | <i>119</i> |
| <i>BIBLIOGRAFÍA</i> | <i>122</i> |
| <i>REFERENCIAS WEB.....</i> | <i>123</i> |

CAPÍTULO I

ANTECEDENTES

Antecedentes de los Sistemas de Video Vigilancia

El presente trabajo de investigación ha adquirido en los recientes años una importancia fundamental como modo de seguridad, importancia que radica principalmente en proporcionar confianza, evidencia e infabilidad. La seguridad es una característica de cualquier sistema la cual nos indica que ese sistema está libre de todo peligro, daño o riesgo y que es en cierta manera confiable.

La historia de la video vigilancia se remonta a los años sesenta donde la policía de los Estados Unidos empieza a utilizar cámaras en Nueva York colocándolas en zonas estratégicas de la ciudad. Esto sentaría un precedente fuerte ya que no pasó mucho tiempo para que se extendiera a otras ciudades para que los policías pudieran vigilar las zonas claves con el uso de Circuitos Cerrados de Televisión. En los años setenta, Inglaterra comienza a utilizar la video vigilancia instalando cámaras en sus principales estaciones de tren subterráneo, así mismo empezó a supervisar el flujo del tráfico en sus carreteras principales. (CCTV y su Evolución, 2013)

Las cintas de cassette de vídeo son en gran parte responsable de popularizar la video vigilancia. La tecnología analógica utilizada en la grabación de cintas de vídeo dio una innovadora idea, la cual era, tener la posibilidad de preservar las pruebas en la cinta. Un problema de la tecnología analógica era que los usuarios tenían que cambiar las cintas cada día, afortunadamente esto se solucionó en la década de los noventa al introducir la tecnología digital lo que permitió la compresión de los videos lo que generaría un mayor tiempo de grabación por medio de la integración de un disco duro, la posibilidad de realizar grabaciones simultáneas de varias cámaras. Además las imágenes grabadas digitalmente tenían una mayor calidad y permitían una mejor manipulación. Todo esto serían las bases para que en un futuro se creara el grabador de video digital, actualmente llamado DVR.

Uno de los acontecimientos más importantes como fue el ataque terrorista a los Estados Unidos en septiembre de 2001, marcó una nueva etapa para la video vigilancia. Los desarrolladores de software e ingenieros empezaron a diseñar programas, los cuales hicieron de la video vigilancia un método de seguridad más eficaz, así como el hecho de aplicar nueva tecnología como lo fue el internet, ya que éste viene a complementar la video vigilancia como una parte fundamental al revolucionarla, eliminando todos los impedimentos para visualización y control, haciendo posible esto desde cualquier parte del mundo. Esto ha llevado al ser humano a realizar día con día sistemas de video vigilancia más potentes y más refinados.

El tema de asaltos, robos y agresiones en los alrededores de la FES Aragón también se ha extrapolado a las noticias y periódicos del Distrito Federal y Estado de México. Han existido diversos artículos a cargo de periodistas como Pulido (2013), Méndez (2013) y Fernández (2011) donde inclusive los alumnos y profesores han dado entrevistas; en estas se comenta que los alumnos acuden a la oficina jurídica de la Facultad, pero dado que no se cuenta con una seguridad o vigilancia interna, los casos quedan inconclusos ya que aunque el alumno pueda identificar al agresor no hay evidencia exacta.

Todo lo anterior da pauta para que los sistemas de video vigilancia sean implementados en lugares donde exista algún tipo de peligro o riesgo y se quiera prevenir o en su caso disminuir situaciones no deseadas. La tecnología ha permitido economizar el tema de vigilancia y facilitar al consumidor la manipulación de su sistema a través de cualquier dispositivo con acceso a internet en cualquier parte del mundo (SOS Seguridad, 2014).

El siguiente trabajo de investigación está basado en un diseño de cámaras de video vigilancia implementando tecnologías como el monitoreo vía remota mediante el uso de internet, esto con el fin de satisfacer las necesidades con las cuales cuenta hoy en día la Facultad de Estudios Superiores Aragón.

CAPÍTULO II
CONSIDERACIONES
TEÓRICAS

2.1 SEÑAL DE VIDEO

Video

El video es la tecnología de captación, grabación, procesamiento, almacenamiento, transmisión y reconstrucción por medios electrónicos digitales o analógicos de una secuencia de imágenes que representan escenas en movimiento. Por lo tanto la señal de vídeo analógica se produce tras convertir los cambios de la intensidad de la luz en señales eléctricas, estas señales son grabadas en materiales como las cintas magnéticas en formatos Betamax y VHS.

Inicialmente la señal de video está formada por un número de líneas agrupadas en varios cuadros y esto a la vez divididos en dos campos los cuales portan la información de luz y color de la imagen. El número de líneas de cuadros y la forma de portar la información de color depende del estándar de televisión del que hablemos (NTSC, PAL, SECAM). (Mtthewson, 1983, p 6-9)

2.1.1 SEÑAL DE VIDEO ANALÓGICA

Señal de video compuesto

Es una señal de vídeo analógica que se utiliza en la producción de televisión y en los equipos audiovisuales de uso comercial. Esta señal eléctrica es compleja ya que se codifica la imagen en sus diferentes componentes de luz y color introduciendo los sincronismos necesarios para su futura reconstrucción como se muestra en la *Fig. 2.1.1*. (Ramírez Tesis, 1979, p 11)

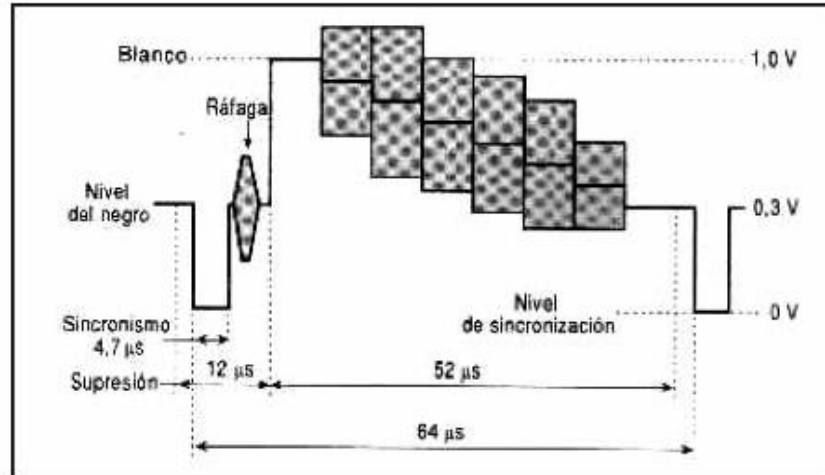


Fig.2.1.1 Señal de video compuesta

La señal de vídeo compuesto consta de las siguientes componentes:

- **Crominancia** - Porta la información del color de una imagen. (Ramírez Tesis, 190, p161) (*Fig. 2.1.2*)
- **Luminancia** - Porta la información de luz (imagen en blanco y negro). (Ramírez Tesis, 1990, p 161) (*Fig.2.1.3*)
- **Pulsos de Sincronismos** - Indican las características del barrido efectuado en la captación de la imagen. (Ramírez Tesis, 1990, p163) (*Fig. 2.1.4*)



Fig. 2.1.2 Crominancia



Fig. 2.1.3 Luminancia

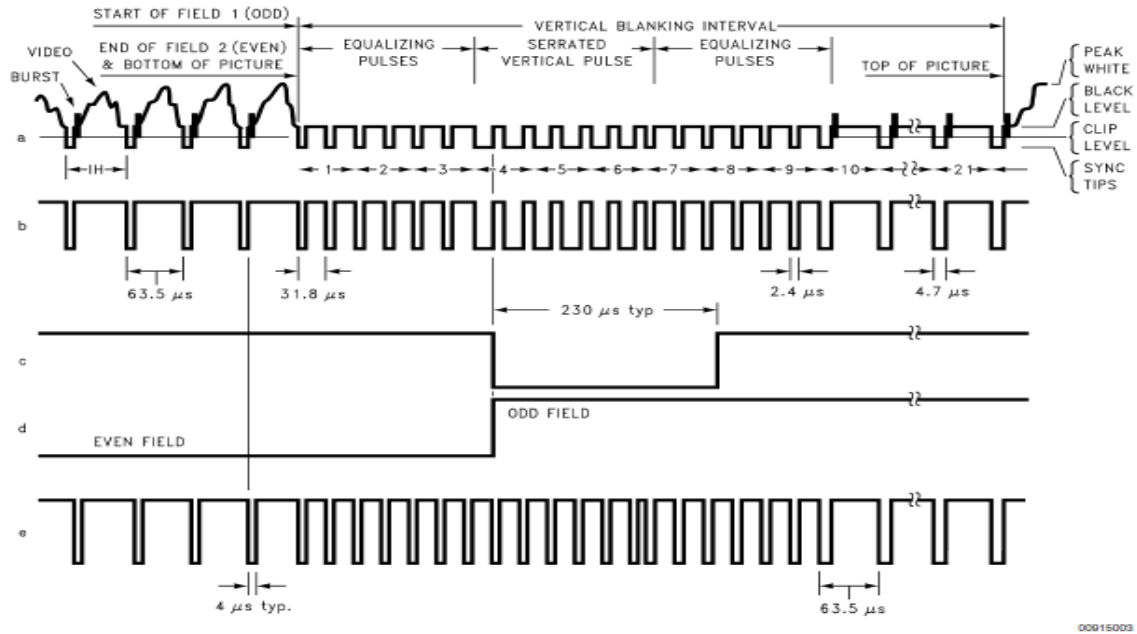


Fig. 2.1.4 Pulsos de sincronismo

El vídeo compuesto está codificado en formatos estándares como lo son NTSC, PAL y SECAM y es designado por las siglas CVBS, que significan Color, Video, Blanking, & Sync (Color, Vídeo, Borrado y Sincronismos).

Los siguientes conceptos están basados en los trabajos de investigación de Ramírez (1979 p 11-28) y Matthewson (1983 p 11-20).

Formatos Estándares de Televisión

El vídeo compuesto tiene diferentes estándares que difieren principalmente en las características utilizadas en el método de descomposición de la imagen y en la codificación del color.

La descomposición de la imagen para su captación se realiza mediante el barrido de diferentes fotogramas, llamados cuadros o frames (Fig.2.1.5), que se descomponen en líneas. El número de cuadros y de líneas marcan la característica del estándar, se agrupan en la utilización de 60 campos que generan 30 cuadros para América y Asia (Fig. 2.1.6) y 50 campos que generan 25 cuadros para Europa (estos datos estaban basados en la frecuencia fundamental de la red de distribución eléctrica).

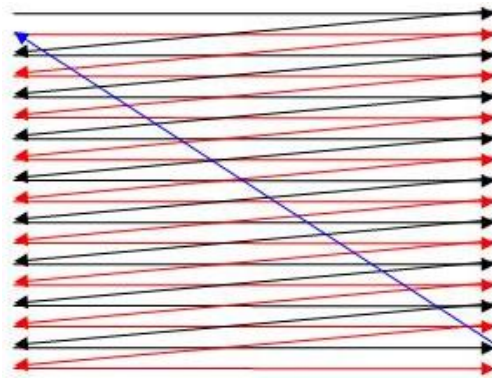


Fig. 2.1.5 Cuadro o frame

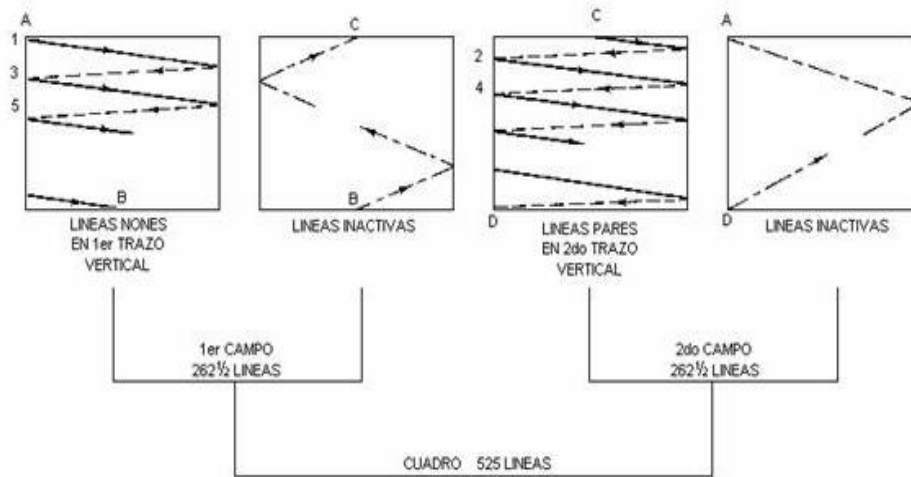


Fig.2.1.6 Campos

La codificación del color se realiza de diferentes formas, ello ha dado lugar a tres estándares diferenciados e incompatibles entre sí. Estos son NTSC, usado en América y Asia; PAL en Europa y SECAM en Francia y los países de la zona de influencia de la antigua URSS.

NTSC

NTSC (National Television System Committee, en español Comisión Nacional de Sistema de Televisión) es un sistema de codificación y transmisión de televisión en color analógico desarrollado en Estados Unidos en torno a 1940, y que se ha empleado en América del Norte, América Central, la mayor parte de América del Sur y Japón entre otros.

El NTSC seleccionó 525 líneas de barrido. La norma recomienda una velocidad de 30 fotogramas por segundo, que consta de dos campos entrelazados por cuadro en 262.5 líneas por campo y 60 campos por segundo. Otras normas en las recomendaciones finales fueron una relación de aspecto de 4:3, y la señal de sonido en frecuencia modulada (FM). El estándar NTSC ha sido adoptado por otros países, la mayoría de las Américas y Japón.

PAL

PAL (Phase Alternating Line, en español línea de fase alternada). Es el nombre con el que se designa al sistema de codificación utilizado en la transmisión de señales de televisión analógica en color en la mayor parte del mundo. Se utiliza en la mayoría de los países africanos, asiáticos y europeos, además de Australia y algunos países americanos.

El sistema de color PAL se usa habitualmente con un formato de vídeo de 625 líneas por cuadro y una tasa de refresco de pantalla de 25 cuadros por segundo, entrelazadas, como ocurre por ejemplo en las variantes PAL-B, G, H, I y N.

SECAM

SECAM (Séquentiel Couleur à Mémoire, en español Color Secuencial con Memoria). Es un sistema para la codificación de televisión en color analógica utilizado por primera vez en Francia y posteriormente en Japón.

La transmisión televisiva en SECAM, se forma escaneando la pantalla del televisor a 625 líneas y a una frecuencia de 25 frames por segundo. Este sistema es compatible con el sistema PAL, ya que utilizan los mismos formatos de escaneo y velocidades en los frames, la diferencia es la forma de cómo se codifica el color. Con esto queremos decir que podemos reproducir filmaciones en aparatos de sistema SECAM o a la inversa.

2.1.2 SEÑAL DE VIDEO DIGITAL

Principio del video digital

El video digital empezó a ser utilizado en 1983 por la empresa SONY el cual consistía en grabar una señal no comprimida de video de definición estándar en forma digital en vez de las formas analógicas de banda alta que se habían utilizado anteriormente.

En el video digital, la información se procesa en una serie de valores establecidos basados en ceros y unos (BIT) para que así sea entendible y la computadora pueda manejar la información. La tecnología de la digitalización ha contribuido al tratamiento de la imagen y el sonido para poder obtener un producto de calidad.

Existen grandes diferencias entre el video digital y el video analógico, las cuales son:

- En el sistema digital la calidad de la imagen se encuentra totalmente independiente, es decir, que solamente se ve afectada en el proceso de digitalización. En el sistema analógico se ve afectado por la cinta, reproductor, etc.
- En el sistema digital se puede editar fácilmente las imágenes ya que existe una mayor manipulación de ellas. En el video analógico la edición depende del soporte de cinta magnética que conlleva a seguir un orden en la filmación.
- En el video digital se utilizan los colores primarios, haciendo que la imagen se defina más exacta. El video analógico tiene una limitación en el uso de colores.
- En el sistema digital no se pierde calidad si se requiere sacar copias. En el sistema analógico la calidad va disminuyendo conforme al número de copias que se van sacando.

Para digitalizar un video es necesario partir de una señal analógica o bien una señal digital directa. Digitalizar quiere decir que convertirá el video en lenguaje máquina, capturarlo y transmitirlo a una computadora para que la señal de video sea procesada.

Señal de video digital

En el dominio digital, la información de video no está representada por la amplitud de las variables físicas, en este caso los voltajes de luminancia y crominancia, sino mediante dígitos que son el resultado de muestreo y codificación. Este conjunto de dígitos que representan la información recibe el nombre de señal digital. La señal digital puede digitalizarse tanto en forma compuesta como en componentes.

Codificación digital de la señal de video

Entre los principales motores para el manejo del video en forma digital estuvieron la conversión de estándares para la transmisión e intercambio internacional de programas, principalmente entre Europa y América y la grabación magnética. La conveniencia de emplear técnicas digitales, surge por las inevitables variaciones en la velocidad de transporte de la cinta que por pequeñas que sean necesitan ser compensadas para mantener la calidad de la señal. Una de las primeras aplicaciones desarrolladas en este sentido fue el corrector de base de tiempos en que la señal analógica captada se convierte en digital y se almacena para leerla posteriormente a una velocidad constante, eliminando así los errores de tiempo, es decir, en los periodos de línea y cuadro, así como los errores en la fase de la crominancia. Actualmente los correctores de tiempo son un elemento indispensable.

Los primeros experimentos para la digitalización de señales de video cromático siguieron dos enfoques separados, uno orientado a la señal compuesta y otro orientado a la señal en tres componentes distintas, bien sean las señales primarias R, G, B o la de luminancia y dos señales de diferencia de color que una vez transmitidas se combinan nuevamente para formar la señal compuesta. El manejo de la señal digital en forma compuesta presenta una serie de limitaciones importantes en el entorno del centro de producción, donde con frecuencia es necesario manejar la señal en componentes, lo que obliga a decodificar nuevamente la señal compuesta en sus componentes primarios contribuyendo al deterioro de la calidad de la imagen.

Mientras que la elección de la frecuencia de muestro para la señal en componentes ofrece un amplio grado de libertad, el muestreo de las señales compuestas debe hacerse a un múltiplo entero de la frecuencia de la subportadora, no tanto como un requisito desde el punto de vista teórico, sino práctico, ya que de esta forma se reduce la intermodulación entre la señal de muestreo y la subportadora, que es consecuencia del proceso no lineal de la conversión analógico-digital.

El muestreo referido a la subportadora es conveniente en el caso de la señal compuesta, ya que dependiendo del valor de la frecuencia de muestreo, el procesado de la señal puede ser más simple. Por ejemplo, si el muestreo de una señal de video con ancho de banda del orden de 5MHz se realiza a tres veces la frecuencia de la subportadora, el menor múltiplo de esta cuya frecuencia es mayor que la de Nyquist, y se puede excluir una de cada tres muestras de crominancia, alineando esta muestra con un eje adecuado a la fase de la subportadora, es decir, ajustando la fase de cada muestra. Esta técnica de excluir muestras es de gran importancia en el proceso de compresión para reducir el caudal binario de una señal de video digital y se designa submuestreo.

Desde el punto de vista de contenido de la información digital de video puede contemplarse en dos aspectos:

- Codificación digital para uso en centros de producción y con fines de distribución. En esa codificación la señal debe de manejarse en la máxima calidad posible.
- Codificación de fuente, orientada a la compresión de la señal, bien sea con fines de distribución o para su grabación en medios tales como discos compactos u otros similares. En esta codificación se pretende lograr la máxima calidad subjetiva.

En el primer caso, el punto de partida es la señal analógica o digital de video generada en una cámara, en el segundo, la señal puede ser también analógica o bien una señal digital previa.

Conversión Analógico-Digital

La conversión de una señal de video de analógica a digital obedece los mismos principios que se aplican a cualquier otra señal analógica y se basan en el principio de muestreo de Nyquist. La señal analógica debe limitarse en banda mediante un filtro de paso bajo y luego muestrearse a intervalos tales que la frecuencia de muestreo sea, por lo menos, el doble de la frecuencia máxima de la señal filtrada. El resultado del muestreo es una señal discreta de amplitud variable, a la que a continuación se somete al proceso de cuantificación a fin de traducir la amplitud de las muestras a un código generalmente binario, con pulsos de la misma amplitud y en que el número de los posibles niveles de cuantificación está determinado por el número de bits con que se codifican las muestras. La recomendación 601 del CCIR, en su forma original, define en 256 el número de niveles de cuantificación de la señal de video. De acuerdo a lo anterior, el proceso de conversión analógico-digital puede ilustrarse en la *Fig. 2.1.7*.

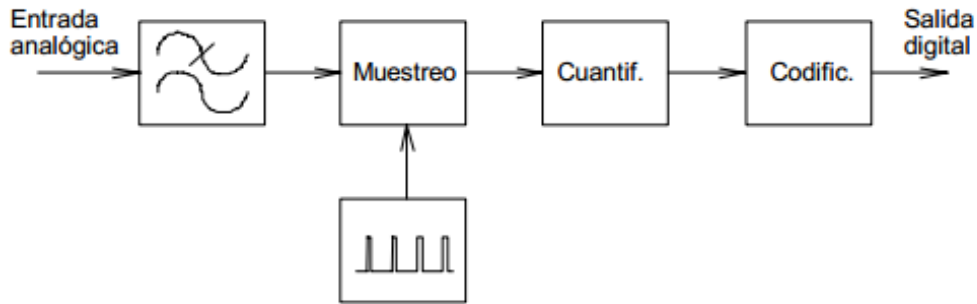


Fig. 2.1.7 Esquema conceptual de un conversor analógico-digital.

La digitalización de la señal analógica de video, se basa en los mismos principios de la modulación por codificación de pulsos (PCM) mediante la cual, una señal analógica limitada en banda, se convierte en una secuencia de señales binarias con un código específico y cuya teoría está tratada ampliamente en la literatura.

Muestreo - La frecuencia de muestreo es el número de muestras por unidad de tiempo que se toman de una señal continua para producir una señal discreta, durante el proceso necesario para convertirla de analógica en digital.

Cuantificación - En la cuantificación se asigna un determinado valor discreto a cada uno de los niveles de tensión obtenidos en el muestreo.

Codificación - En la codificación, a cada nivel de cuantificación se le asigna un código binario distinto, con lo cual ya tenemos la señal codificada y lista para ser transmitida.

Señal Digital - Finalmente se obtiene la señal digital.

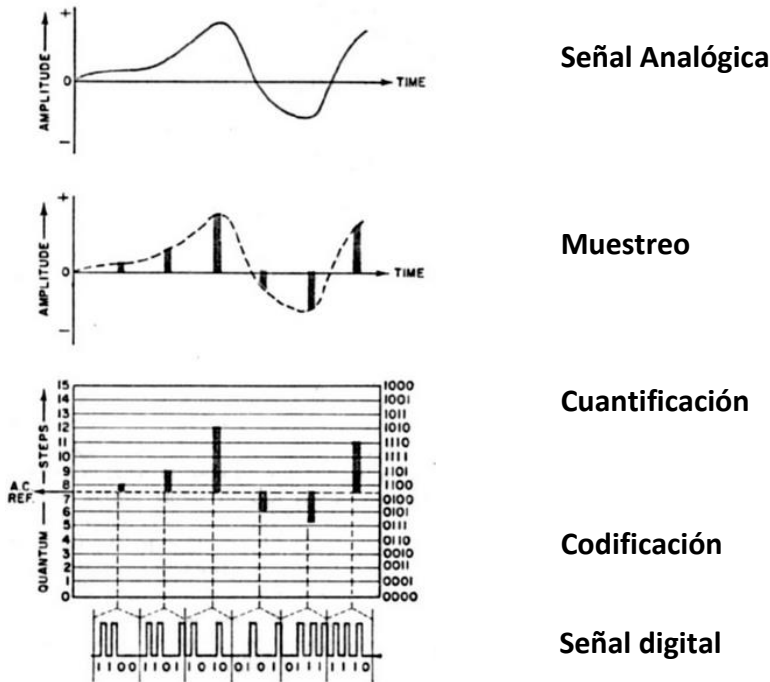


Fig. 2.1.8 Proceso del PCM

Compresión del video digital

La edición del video digital, solamente consiste en el tratamiento de este por medio de una computadora. Durante ese proceso se puede realizar corte a los fotogramas así como incorporar el sonido. Existen varios formatos de video que se pueden editar (AVI, MJPEG, MJPEG2, DVD, QUICK TIME, entre otros)

El último proceso que se realiza en el tratamiento del video digital es la difusión, publicación o grabación, ya sea en soporte de CD, DVD, o por la red. Los formatos de difusión que pueden existir son MPEG, MPEG-2, MPEG-4, con sus diferentes Codecs (función para comprimir un archivo) DivX, Xvid, etc.

Una vez digitalizado el video, implica un proceso de compresión ya que de lo contrario ocuparía mucho espacio en un espacio de almacenamiento. Normalmente cuando un video se edita, la digitalización se realiza a máxima claridad para evitar las pérdidas de calidad.

Existen dos tipos de compresión de video intra-frame (Fig. 2.1.9) o inter-frame (Fig. 2.1.10)

La intra-frame o compresión espacial comprime cada fotograma por separado, por lo tanto se utilizan las imágenes completas (Keyframes). Este método es de mayor calidad, lo que hace que ocupe más espacio.

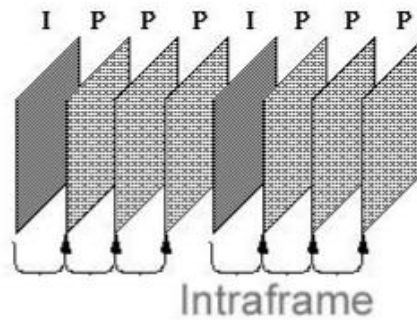


Fig.2. 1.9 Tipo de compresión por intra-frame.

El inter-frame es el método que comprime a partir de similitudes entre los fotogramas. Este método tiene menor calidad.

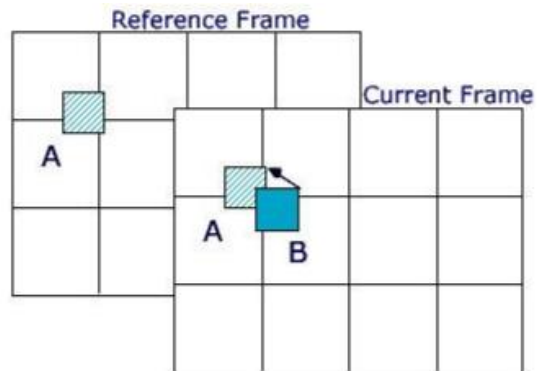


Fig. 2.1.10 Tipo de compresión por inter-frame.

En este último tipo de compresión se puede citar del tipo MPEG.

MPEG

Este estándar de compresión fue desarrollado por Moving Pictures Experts Group (en español, expertos en imágenes en movimiento). El método de compresión que utiliza es la similitud de contenidos, quiere decir que si percibe una parte común a todo, guarda un ejemplar y elimina el resto. De esta manera se consigue una reducción en el espacio de almacenamiento. Este formato se clasifica en MPEG-1, MPEG-2, MPEG—3 y MPEG-4.

MPEG1

Este formato de compresión surgió en el año de 1991, su calidad es parecida al del VHS. La finalidad de este formato era colocar el video digital en un soporte muy conocido como lo es el CD-ROM. Su tamaño es de 1.5 Mbps y se presenta a una resolución de 352x240 píxeles para NTSC y 352x288 en PAL. Actualmente este formato se utiliza bastante para visualizar vídeos por internet.

MPEG2

Este formato aparece en 1994, es uno de los formatos de compresión que ofrece mayor calidad de imagen, alcanza a su vez una velocidad en la transmisión de datos de 3 a 10 Mbits de ancho de banda, ofrece la transmisión de ficheros de vídeo digital a pantalla completa o broadcast, es el utilizado por la televisión digital y para la codificación del DVD de vídeo. Trabaja con resoluciones desde 352 x 480 y 1920 x 1080 píxeles o 720x576 (PAL) y 720x480 (NTSC).

MPEG3

Este formato se desarrolló para la televisión digital de alta calidad aunque el formato MPEG2 también cumplía perfectamente esta función. El formato MPEG3 tiene mayor ancho de banda que el MPEG2 y se optó por la utilización finalmente del formato MPEG2. Por este motivo el proyecto orientado en el MPEG3 se abandonó.

MPEG4

Uno de los Codecs utilizados en este formato son los famosos, DivX y XviD. Una de las grandes ventajas que ofrece este formato es una muy buena calidad, muy parecida al del formato DVD, a cambio de un factor de compresión mucho más elevado que otros formatos, dando como resultado archivos o ficheros más comprimidos que otros e ideales para poder transmitir los datos a través de Internet. Utiliza una resolución de 176 x 144 píxeles.

MPEG7

Este formato está en proyecto, cómo el estándar que más se utilizará en Internet y televisiones interactivas. Este formato codificará además de la imagen y sonido datos en lenguaje XML. MPEG7 servirá de gran ayuda para el avance de la nueva televisión interactiva con introducción de buscadores de contenidos, búsquedas de audiovisuales etc.

H.264

H.264 es un formato digital estandarizado para la compresión de vídeo de alta definición con una velocidad de bits elevada. El estándar de compresión de vídeo H.264 proporciona aproximadamente el doble de la compresión de la norma anterior MPEG-4 para la misma calidad de vídeo. Dentro del estándar H.264, define la calidad de vídeo más alta con la tasa de bits más baja, lo que es especialmente relevante para aplicaciones tales como los Circuitos Cerrados de Televisión (CCTV).

Las cámaras IP utilizan el protocolo de Internet (IP) para transmitir datos de audio y video, junto con las señales de control, sobre enlaces Ethernet en CCTV. Ofrecen numerosas ventajas con respecto a las cámaras de seguridad analógicas tradicionales, que normalmente transmiten una señal NTSC / PAL analógica a través de cable coaxial. A diferencia de las cámaras analógicas, las cámaras IP son compatibles con imágenes en alta definición (HD), análisis inteligente de vídeo, almacenamiento local y el mando a distancia. Los diseños de cámara de alimentación pueden ser alimentados a través de Ethernet (POE), sin fuentes de energía adicionales. Al utilizar el mismo cable para transmitir datos y alimentación, las instalaciones de POE pueden reducir sustancialmente los costos de cableado.

2.2 TOPOLOGÍAS DE RED.

Teoría de Redes

La teoría de las redes nace de la necesidad de compartir e intercambiar información a grandes distancias a través de un medio o una canal de comunicación por medio de diversas señales. La misión de las comunicaciones es transportar la mayor cantidad de información en el menor tiempo de una manera segura. Esto se logra gracias a diferentes técnicas tales como son la Modulación, Codificación, Multicanalización, etc. (Molina, 2004, p 5-7). Es necesario describir las siguientes definiciones:

Red - Una RED es un conjunto de computadoras o terminales conectados mediante una o más vías de transmisión y con determinadas reglas para comunicarse.

Host - Equipo el cual se conecta a una Red.

Protocolo - Conjunto de comandos establecido por convención que deben conocer tanto emisor como receptor para establecer una comunicación en un red de datos.

DTE - Data Terminal Equipment es el equipo terminal de datos, la computadora o terminal que es el extremo final de la red.

DCE - Data Communication Equipment es el equipo de comunicación. Generalmente un modem u algún otro dispositivo que establece el enlace físico y lógico con la red.

Internet - Una Internet es un conjunto de dos o más redes que se interconectan mediante los medios adecuados de transmisión para el intercambio de información.

Existen dos tipos de redes, la red orientada a conexión y la red no orientada a conexión.

Red Orientada a la Conexión

Es cuando se establece un único camino para la transferencia de la información. Los datos viajarán uno tras otro por dicho camino y no habrá más de un camino simultáneamente. Requiere obligatoriamente de tres fases las cuales son:

- Establecimiento
- Transferencia
- Desconexión

Algunos ejemplos son ATM o TCP.

Red no Orientada a la Conexión

Esta red no utiliza un único camino, sino que los datos se fraccionan y toman por distintas vías simultáneamente para llegar a destino. Se la conoce también como Servicio de Datagramas. Algunos ejemplos son IP y UDP.

Clasificación de las Redes

Tomando en cuenta lo que explica Molina (2004, p 22-27) acerca de redes y sus topologías; estas pueden clasificarse según la extensión que abarcan, cada uno de los tipos requiere de tecnologías y topologías específicas. Se distinguen en general tres categorías.

- **REDES LAN** (*Local Area Networks*): Son las que no exceden 1 km de extensión. Lo más habitual es que abarquen un edificio o varios dentro de una manzana o un área limitada.
- **REDES MAN** (*Metropolitan Area Network*): Hasta 10 Km, es decir, distintos puntos dentro de una misma ciudad.
- **REDES WAN** (*Wide Area Networks*): Más de 10 Km. Distintas ciudades dentro de un mismo país o distintos países.

Las redes pueden utilizar dos métodos de comunicación que las diferencia en:

REDES DE BROADCAST

Todas las máquinas comparten un único medio de transmisión. Es decir, que cuando una de ellas transmite, todas recibirán la información y solamente aquella a la cual va dirigida la utilizará.

REDES PUNTO A PUNTO

Existen conexiones individuales entre pares de máquinas.

Topologías de Red

La topología de red es la forma de comunicación usada por los dispositivos que conforman una red para intercambiar datos. Existen dos variantes en las topologías, las físicas y las lógicas. (Raya, J. & Raya, C; 1997, p 15 - 20)

Topología física: Es la conexión real del cableado entre los dispositivos.

- **ESTRELLA:** Los terminales se conectan todas directamente a un dispositivo central. (Fig. 2.2.1)
- **ANILLO:** El cable de interconexión recorre uno a uno las terminales cerrándose en un lazo. (Fig. 2.2.2)
- **BUS:** Un único cable recorre todas las terminales desde un extremo a otro. También se la conoce como topología horizontal. (Fig.2.2.3)
- **ÁRBOL:** Partiendo de un dispositivo central los equipos se van ramificando. También se la conoce como estructura jerárquica (Fig. 2.2.4)

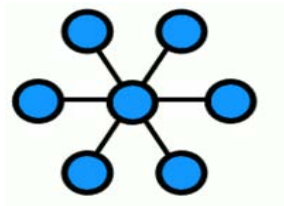


Fig. 2.2.1 ESTRELLA

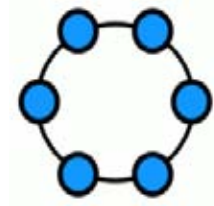


Fig. 2.2.2 ANILLO

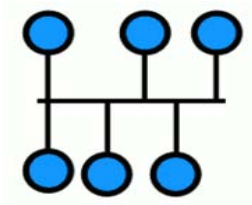


Fig. 2.2.3 BUS

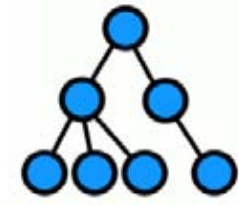


Fig. 2.2.4 ÁRBOL

Topologías lógicas: Se refieren al comportamiento de los datos en la red independientemente del conexionado físico. En las topologías lógicas solamente existe la de BUS y ANILLO.

Todas las anteriores físicas encuadran en alguna de las 2 topologías lógicas. Por ejemplo: Una red Ethernet que utiliza cable UTP y se conecta en estrella a un hub en realidad se comporta lógicamente como un bus.

2.2.1 MODELO OSI

Modelo OSI

En las obras de Molina (2004, p 57-61), Raya, J. & Raya, C. (1997, p 29-31) y Forouzan (2003 p 19-20). El modelo OSI (Open System Interconnection, en español Modelo de Interconexión de Sistemas Abiertos) es un modelo de Red descriptivo el cual fue creado por la ISO en 1980. Es un modelo de referencia para la definición de arquitecturas en la interconexión de los sistemas de comunicación. El modelo OSI se desarrolla implementando una normativa formada por siete capas que define las diferentes fases por las que deben pasar los datos para viajar de un dispositivo a otro sobre una red de comunicaciones (*Fig.2. 2.5*). Siguiendo este esquema se crearon una gran variedad de protocolos.



Fig. 2.2.5 Las 7 capas del Modelo OSI

Funciones principales de cada capa

Nivel Físico

- Transmisión de flujo de bits a través del medio.
- No existe estructura alguna.
- Maneja voltajes y pulsos eléctricos.
- Especifica cables, conectores y componentes de interfaz con el medio de transmisión.

Nivel de Enlace de Datos

- Estructura el flujo de bits bajo un formato predefinido llamado trama.
- Para formar una trama, el nivel de enlace agrega una secuencia especial de bits al principio y al final del flujo inicial de bits.
- Transfiere tramas de una forma confiable libre de errores (utiliza reconocimientos y retransmisión de tramas).
- Provee control de flujo.
- Utiliza la técnica de "piggybacking" (la cual es el acceso no autorizado de una LAN inalámbrica).

Nivel de Red (Nivel de paquetes)

- Divide los mensajes de la capa de transporte en paquetes y los ensambla al final.
- Utiliza el nivel de enlace para el envío de paquetes: un paquete es encapsulado en una trama.
- Enrutamiento de paquetes.
- Envío a los paquetes de nodo a nodo usando ya sea un circuito virtual o como datagramas.
- Control de Congestión.

Nivel de Transporte.

- Establece conexiones punto a punto sin errores para el envío de mensajes.
- Permite multiplexar una conexión punto a punto entre diferentes procesos del usuario (puntos extremos de una conexión).
- Provee la función de difusión de mensajes (broadcast) a múltiples destinos.
- Control de Flujo.

Nivel de Sesión

- Permite a usuarios en diferentes máquinas establecer una sesión.
- Una sesión puede ser usada para efectuar un login a un sistema de tiempo compartido remoto, para transferir un archivo entre 2 máquinas, etc.
- Controla el diálogo (quién habla, cuándo, cuánto tiempo, half duplex o full duplex).
- Función de sincronización.

Nivel de Presentación

- Establece una sintaxis y semántica de la información transmitida.
- Se define la estructura de los datos a transmitir (v.g. define los campos de un registro: nombre, dirección, teléfono, etc).
- Define el código a usar para representar una cadena de caracteres (ASCII, EBCDIC, etc).
- Compresión de datos.
- Criptografía.

Nivel de Aplicación

- Transferencia de archivos (ftp).
- Login remoto (rlogin, telnet).
- Correo electrónico (mail).
- Acceso a bases de datos, etc.
- Otras

2.2.2 MODELO IP

Modelo OSI

El modelo TCP/IP es un modelo de descripción de protocolos de red desarrollado en la década de los 70. El modelo TCP/IP se denomina a veces como Internet Model, Modelo DoD o Modelo DARPA. (Molina, 2004, p 62-64)

El modelo TCP/IP, describe un conjunto de reglas generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos. Para conseguir un intercambio fiable de datos entre dos equipos, se deben llevar a cabo muchos procedimientos separados.

TCP/IP tiene cuatro capas de abstracción según se define en el RFC 1122 (*Fig. 2.2.6*). Esta arquitectura de capas a menudo es comparada con el Modelo OSI de siete capas. Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados. (Forouzan, 2003, p 32-34)

Capa 4

También conocida como capa de aplicación, es asimilable a las capas 5 (sesión), 6 (presentación) y 7 (aplicación) del modelo OSI. La capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo.

Capa 3

También conocida como capa de transporte, es asimilable a la capa 4 (transporte) del modelo OSI.

Capa 2 o capa de internet: Internet.

También conocida como capa de Internet, es asimilable a la capa 3 (red) del modelo OSI.

Capa 1

También es conocida como capa de Acceso al Medio, es asimilable a la capa 2 (enlace de datos) y a la capa 1 (física) del modelo OSI.

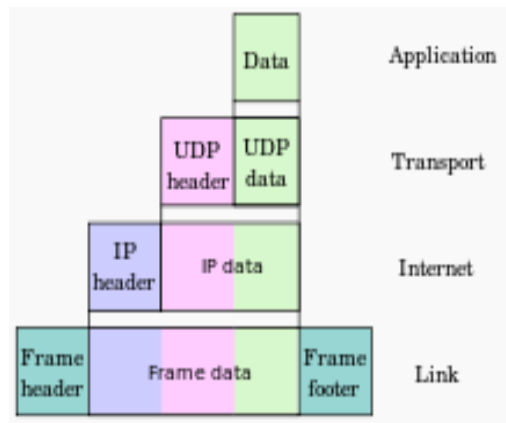


Fig. 2.2.6 Capas modelo TCP/IP

2.3 REDES IP

Protocolo IP

EL Protocolo IP (Internet Protocol, en español protocolo de internet) es un protocolo de comunicación de datos digitales clasificado funcionalmente en la Capa de Red según el modelo internacional OSI. Su función principal es el uso bidireccional en origen o destino de comunicación para transmitir datos mediante un protocolo no orientado a conexión que transfiere paquetes conmutados a través de distintas redes físicas previamente enlazadas según la norma OSI de enlace de datos.

Los aspectos más complejos de IP son el direccionamiento y el enrutamiento. El direccionamiento se refiere a la forma como se asigna una dirección IP y cómo se dividen y se agrupan subredes de equipos, mientras que el enrutamiento consiste en encontrar un camino que conecte una red con otra y, aunque es llevado a cabo por todos los equipos, es realizado principalmente por routers, que no son más que computadoras especializadas en recibir y enviar paquetes por diferentes interfaces de red, así como proporcionar opciones de seguridad, redundancia de caminos y eficiencia en la utilización de los recursos. (Forouzan, 2003, p 191-192)

Actualmente existen dos versiones de IP, las cuales son:

- **IPv4 32 bits de direcciones**

($2^{32} = 4,294,967,296$)

- **IPv6 128 bits de direcciones**

($2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$)

La principal diferencia entre las dos versiones son los bits de direcciones. (Forouzan, 2003, p 39-40)

2.3.1 DIRECCIONAMIENTOS

Direccionamientos

Una dirección IP es una etiqueta numérica que identifica de manera lógica y jerárquica a un dispositivo dentro de una red que utilice el protocolo IP (Internet Protocol). Este número no se debe confundir con la dirección MAC la cual es un identificador de 48bits para identificar de forma única los dispositivos de comunicación y no depende del protocolo de conexión utilizado ni de la red. Los dispositivos se conectan entre sí mediante sus respectivas direcciones IP. (Raya, J. & Raya, C; 1997, p 94)

Es muy común que la dirección IP cambie frecuentemente debido a los cambios en la red o porque el dispositivo encargado dentro de la red de asignar las direcciones IP decida asignar otra IP. A esta forma de asignación de dirección IP se denomina también dirección IP dinámica, normalmente se abrevia como IP dinámica. Los sitios de Internet que por su naturaleza necesitan estar permanentemente conectados tienen una dirección IP fija, comúnmente se abrevia IP fija o IP estática. Esta no cambia con el tiempo.

Las direcciones IPv4 se expresan con un número binario de 32 bits, permitiendo un espacio de direcciones de hasta 4.294.967.296 (2^{32}) direcciones posibles. Las direcciones IP se pueden expresar como números de notación decimal dividiendo los 32 bits de la dirección en cuatro octetos. El valor decimal de cada octeto está comprendido en el rango de 0 a 255, por lo tanto 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. (Forouzan, 2003, p 119-137)

En la expresión de direcciones IPv4 en decimal se separa cada octeto por un carácter único ".". 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:

10.128.001.255 ó 10.128.1.255

Clases de Redes IP

En esta arquitectura 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.

Clase A

En una red de clase A, se asigna el primer octeto para identificar la red, reservando los tres últimos octetos (24 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es $2^{24} - 2$ (se excluyen la dirección reservada para broadcast (últimos octetos en 255) y de red (últimos octetos en 0)), es decir, 16.777.214 hosts. (Tabla 2.3.1)

| | | | | |
|------------|----------------|---------------------------|-----------------|-----------------|
| 0 | Xxxxxxx | Xxxxxxxx | Xxxxxxxx | Xxxxxxxx |
| RED | | EQUIPOS TERMINALES | | |

Tabla.2.3.1 Dirección IP clase A en binario

Clase B

En una red de clase B, se asignan los dos primeros octetos para identificar la red, reservando los dos octetos finales (16 bits) para que sean asignados a los hosts, de modo que la cantidad máxima de hosts es $2^{16} - 2$, o 65.534 hosts. (Tabla 2.3.2)

| | | | | |
|------------|---------------|-----------------|---------------------------|-----------------|
| 10 | Xxxxxx | Xxxxxxxx | Xxxxxxxx | Xxxxxxxx |
| RED | | | EQUIPOS TERMINALES | |

Tabla 2.3.2 Dirección IP clase B en binario.

Clase C

En una red de clase C, se asignan los tres primeros octetos para identificar la red, reservando el octeto final (8 bits) para que sea asignado a los hosts, de modo que la cantidad máxima de hosts es $2^8 - 2$, ó 254 hosts. (Tabla 2.3.3)

| | | | | |
|------------|--------------|-----------------|-----------------|-------------------------------|
| 110 | Xxxxx | Xxxxxxxx | Xxxxxxxx | Xxxxxxxx |
| RED | | | | EQUIPOS TERMINALES |

Fig. Tabla 2.3.3 Dirección IP clase C en Binario.

A continuación se muestra una tabla con el tipo de clase de red, rango, número de redes, número de host por red, máscara de red y broadcast. (Tabla 2.3.4)

| Clase | Rango | No. De Redes | No. De Host por red | Máscara de Red | Broadcast |
|-------|---------------------------|--------------|---------------------|----------------|---------------|
| A | 1.0.0.0-126.255.255.255 | 126 | 16.777.214 | 255.0.0.0 | x.255.255.255 |
| B | 128.0.0.0-191.255.255.255 | 16.384 | 65.534 | 255.255.0.0 | x.x.255.255 |
| C | 192.0.0.0-223 | 2.097.252 | 254 | 255.255.255.0 | x.x.x.255 |
| D | 224.0.0.0-239.255.255.255 | Histórico | | | |
| E | 240.0.0.0-255.255.255.255 | Histórico | | | |

Tabla 2.3.4 Clases de red.

- La dirección 0.0.0.0 es reservada por la IANA para identificación local.
- La dirección que tiene los bits de host iguales a cero sirve para definir la red en la que se ubica. Se denomina dirección de red.
- La dirección que tiene los bits correspondientes a host iguales a 255, sirve para enviar paquetes a 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 designar la propia máquina. Se denomina dirección de bucle local o loopback.

Máscara de Subred

La máscara permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP. La necesitan los routers para determinar la dirección de red o subred a la que pertenece un determinado host. Dada la dirección de clase A 10.2.1.2 sabemos que pertenece a la red 10.0.0.0 y el host al que se refiere es el 2.1.2 dentro de la misma. La máscara se forma poniendo a 1 los bits que identifican la red y a 0 los bits que identifican el host. De esta forma una dirección de clase A tendrá como máscara 255.0.0.0, una de clase B 255.255.0.0 y una de clase C 255.255.255.0. Los dispositivos de red realizan un AND entre la dirección IP y la máscara para obtener la dirección de red a la que pertenece el host identificado por la dirección IP dada. Por ejemplo:

Máscaras de red por defecto:

Clase A 255.0.0.0

Clase B 255.255.0.0

Clase C 255.255.255.0

Ecuaciones con AND:

1 AND 1 = 1

1 AND 0 = 0

0 AND 1 = 0

0 AND 0 = 0

Ejemplo:

Dirección IP: 192.100.10.33

Clase: C

Parte de red: **192.100.10.33**

Parte de host: 192.100.10.**33**

Para obtener esta operación la computadora opera en modo binario utilizando una operación AND entre la dirección de red y máscara de subred.

| | RED | HOST |
|--------------------------|------------------------------------|---------------------------------|
| Dirección IP | 11000000.1100100.00001010. | 00100001 (192.100.10.33) |
| Máscara de SUBRED | <u>11111111.11111111.11111111.</u> | <u>00000000 (255.255.255.0)</u> |
| AND | 11000000.1100100.00001010. | 00100001 (192.100.10.33) |

2.3.2 REDES Y SUBREDES

Creación de Subredes

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas. Esto se realiza debido a la falta de organización dentro de la red o a que el tráfico broadcast puede llegar a disminuir la eficiencia de la red. Por lo tanto para solucionar este problema se puede subdividir la red en redes más pequeñas, esta técnica se conoce como, “subnetting”, “subneteo” o “división en subredes de longitud fija”. (Fig. 2.3.1)

En el interior la LAN se divide en LANs más pequeñas interconectadas por routers, sin embargo; desde afuera la LAN no ha cambiado.

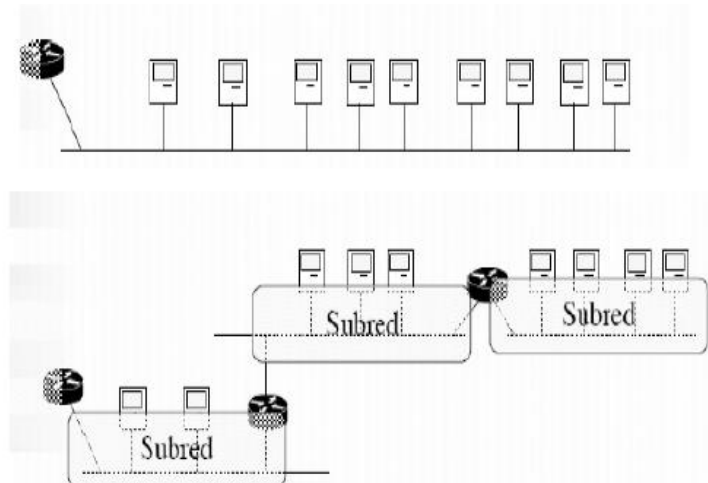


Fig. 2.3.1 División de LAN en LANs

Cada subred funciona como si fuera una red independiente, pero para realizar la división se necesita dividir la parte del hosts en dos partes.

| | | |
|----------------------|-------------------------|--------------------------|
| RED r bits | SUBRED n bits | HOSTS h-n bits |
|----------------------|-------------------------|--------------------------|

Para identificar la red se tiene en cuenta que la máscara pone a 1 todos los bits de red y además ahora pondrá a 1 los bits de subred.

| | | | |
|-----------|-------------------|----------------------|-------------|
| 10 | Network ID | SUBNETWORK ID | HOST |
|-----------|-------------------|----------------------|-------------|

| | |
|----------------------|---------------------|
| 1111.....1111 | 0000.....000 |
|----------------------|---------------------|

Pasos para dividir una red en subredes

1. Primero se debe de conocer el número de subredes que se requieren.
2. Se debe calcular cuántos bits se utilizarán para cada subred requerida.

Para determinar los dos pasos anteriores se utiliza la siguiente fórmula:

$$2^n - 2 \geq k$$

Donde "k" es el número de subredes.

Donde "n" es el número de bits que se necesitan.

Se restan "2" (la dirección de red y la dirección de broadcast)

Por ejemplo, si una organización quiere crear 5 subredes y dispone de la red 192.168.22.00

Datos

Sustituimos

Resultado

k=5

$$2^3 - 2 \geq 5$$

$$6 \geq 5$$

n=3

Por lo tanto se obtiene 6 subredes las cuales son suficientes para cubrir la necesidad de 5 subredes.

Nota:

Con 4 bits se obtiene 16 subredes (Son demasiadas subredes)

Con 3 bits se obtiene 8 subredes (Son suficientes subredes)

Con 2 bits se obtiene 4 subredes (Son insuficientes subredes)

1. Determinar la nueva máscara de subred.

Se tiene a 1 los bits correspondientes a la red y a la subred, por otro lado se tiene a 0 los bits correspondientes al host.

En el ejemplo anterior la dirección IP era 192.168.22.0 la cual corresponde a una dirección tipo clase C por lo tanto la parte de red tiene los 3 primeros bytes y los últimos 8 bits que corresponden al host, 5 serán de subred.

11111111.11111111.11111111.11100000
255 . 255 . 255 . 224

- 192.168.22.0 Era la IP de la red
- 255.255.255.248 Es la máscara de red
- 192.168.22.---00000 Se tiene 3 bits de subredes

Finalmente se tiene 6 direcciones de subred para utilizar.

| Binario | Decimal | |
|----------------------|----------------|--------------|
| 192.168.22.000 00000 | 192.168.22.0 | NO ASIGNABLE |
| 192.168.22.001 00000 | 192.168.22.32 | |
| 192.168.22.010 00000 | 192.168.22.64 | |
| 192.168.22.011 00000 | 192.168.22.96 | |
| 192.168.22.100 00000 | 192.168.128.0 | |
| 192.168.22.101 00000 | 192.168.22.160 | |
| 192.168.22.110 00000 | 192.168.22.192 | |
| 192.168.22.111 00000 | 192.168.22.224 | NO ASIGNABLE |

2.4 CÁMARAS DE VIDEO

Los autores Ruíz (1991, p 36-43) y Matthewson (1983, p 48-79) fueron de ayuda para desarrollar el punto 2.4 al tomar algunas de sus ideas que plasmaron en sus ejemplares.

Cámara de Video

La cámara de vídeo o videocámara es un dispositivo que captura imágenes convirtiéndolas en señales eléctricas, en la mayoría de los casos a señal de vídeo, también conocida como señal de televisión. En otras palabras, una cámara de vídeo es un transductor óptico.

Las primeras cámaras de video, propiamente dichas, utilizaron tubos electrónicos como captadores: un tipo de válvulas termoiónicas que realizaban, mediante el barrido por un haz de electrones del *target* donde se formaba la imagen procedente de un sistema de lentes, la transducción de la luz (que conformaba la imagen) en señales eléctricas. (Fig. 2.4.1)

Posteriormente se desarrollaron transductores de estado sólido llamados CCDs (Dispositivos de cargas acopladas). Ellos sustituyeron muy ventajosamente a los tubos electrónicos, propiciando una disminución en el tamaño y el peso de las cámaras de vídeo además de proporcionar una mayor calidad y fiabilidad.



Fig. 2.4.1 Cámara de televisión de estudio primitiva

Existen dos tipos básicos de cámaras de TV: las portátiles, también llamadas ENG, y las de estudio. Las cámaras de estudio van integradas en el sistema de producción correspondiente, mientras que las ENG trabajan independientes de cualquier instalación y suelen ir asociadas a un sistema de grabación de señales de TV; normalmente un VTR (Video Tape Recorder) portátil o asociado a la propia cámara.

Partes del sistema de una cámara

El sistema completo de una cámara de vídeo recibe el nombre de cadena de cámara y consta de la cabeza de cámara, que es la parte que está en el plató o en el lugar de la producción, y la estación base o base station que es la parte de la cámara que la une con el resto del sistema de producción.

La cabeza de cámara y la estación base se unen entre sí mediante una manguera de varios cables, por donde van las señales que se mandan del sistema a la cámara y de esta al sistema, así como las alimentaciones correspondientes. Este cable múltiple puede ser sustituido por un cable coaxial llamado Triaxial, por el que las señales se introducen mediante multiplexación en frecuencia. También hay sistemas de conexionado inalámbrico, pero sólo son utilizados en casos muy concretos y especiales.

Atendiendo a la cadena de cámara completa, se puede distinguir varias partes diferentes.

En la cabeza de cámara tenemos:

- **La óptica:** sistema de lentes que permiten encuadrar y enfocar la imagen en el target del captador.
- **El cuerpo de cámara:** Espacio donde reside la instrumentación electrónica encargada de la captación y la conversión de las imágenes.
- **El adaptador triaxial, o el adaptador al sistema de conexionado elegido con la estación base:** Comunica la cabeza de cámara con la estación base.

En la estación base tenemos:

- **El adaptador triaxial, o el adaptador al sistema de conexionado elegido:** Comunica la estación base con la cabeza de cámara.
- **Sistema electrónico:** Conjunto de circuitos necesarios para la conexión de la cadena de cámara al resto de la instalación.

Funcionamiento de una Cámara de Video

Primero, la luz que proviene de la óptica es descompuesta al pasar por un prisma de espejos dicróicos que descomponen la luz en las tres componentes básicas que se utilizan en televisión, donde el rojo -R o red, verde- G o green y azul -B o blue (*Fig. 2.4.2*). Justo en la otra cara de cada lado del prisma están los captadores, actualmente dispositivos CCDs y anteriormente tubos de cámara. El sistema óptico está ajustado para que en el target de cada captador se reconstruya la imagen nítidamente. Esta imagen es leída por los CCDs y su sistema de muestreo y conducida a los circuitos preamplificadores.

Los circuitos de muestreo y lectura de los CCD deben estar sincronizados con la señal de referencia de la estación. Para ello, todos los generadores de pulsos se enclavan con las señales procedentes del sistema de sincronismo de la cámara, que recibe la señal de genlock, normalmente negro de color, desde el sistema en el que se está trabajando. O bien, se trabaja sin referencia exterior, como suele hacerse al utilizar cámaras de ENG.

Ésta imagen leída por los CCD y su sistema de muestreo es conducida luego a los circuitos preamplificadores. En los preamplificadores se genera e inserta, cuando así se quiere, la señal de prueba llamada pulso de calibración, comúnmente llamada cal, la cual recorrerá toda la electrónica de la cámara y servirá para realizar un rápido diagnóstico y ajuste de la misma. De los preamplificadores las señales se enrutan a los procesadores, donde se realizan las correcciones de gamma, detalle, masking, pedestal, flare, ganancias, clipeos y limitadores.

Las señales ya están listas para salir al sistema de producción o para ser grabadas. Se envían entonces a los circuitos de visionado, los cuales muestran la imagen en el visor de la cámara y la transmiten mediante los correspondientes conectores de salida.

La salida básica, video compuesto VBS, sigue siendo la del sistema analógico de TV elegido: PAL, NTSC o SECAM, por lo que el codificador está presente en todas las cámaras. Estas señales son mandadas mediante el adaptador triax, fibra óptica o multicore (26pins) a la estación base, que se encargará de enrutarlas en el sistema de producción al que pertenece la cámara. Si la cámara está unida a un magnetoscopio es un camcorder o camiscopio y, entonces, las señales se suministran a los circuitos indicados para su grabación en cinta, en disco óptico, disco duro o tarjetas de memoria.

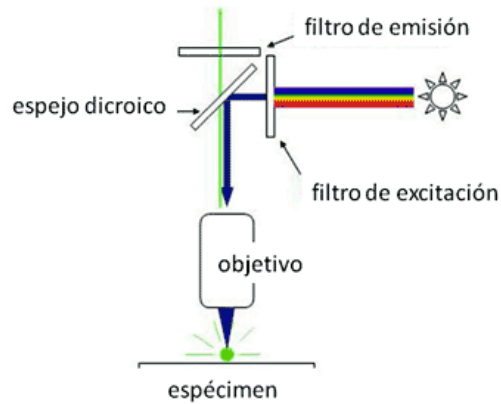


Fig. 2.4.2 Funcionamiento Espejo Dicroico

Clasificación de las cámaras

Cámara de vídeo semiprofesional.

- **Cámaras de estudio y de EFP:** estas cámaras están diseñadas para la obtención de la mejor calidad de imagen posible en función de la rapidez con que se obtiene. (Luminancia), colorimetría, detalle y demás ajustes para conseguir que todas las cámaras muestren imágenes semejantes.
- **Cámaras de ENG:** también conocidas como Camcorder, traen un grabador incorporado que almacena el vídeo y el audio generados por la cámara y su micrófono correspondiente.

Según su calidad

- **Cámaras domésticas:** Diseñadas completamente para uso doméstico, no aptas para transmisión
- **Cámaras semiprofesionales:** Son equipos relativamente asequibles en precio, su calidad es superior a las domésticas, y aunque son de calidad media en términos broadcast, se han vuelto populares en este ámbito como cámaras ENG, ya que su calidad de imagen sin ser profesional, es muy buena.

- **Cámaras profesionales:** Cámaras de gama alta, uso en productoras y canales de televisión, su costo no es asequible para el uso personal.
- **Cámaras broadcast:** Son equipos diseñados para la industria televisiva y emisión de la señal.
- **Cámaras de CCTV:** El principal objetivo de las cámaras para los Circuitos Cerrados de Televisión vigilar ciertas zonas. Según su calidad y características, existen una gran variedad de estas.

2.4.1 CÁMARAS DE VIDEO ANALÓGICAS

Cámara Analógica

En el pasado todas las cámaras de video eran analógicas. La señal de video analógica se puede conectar directamente a cualquier monitor, video grabador o frame grabber. El sensor CCD es también analógico y las primeras generaciones de cámaras CCD se pensaron para hacerlas compatibles con todos los sistemas analógicos existentes en el momento de su aparición. En las cámaras más modernas la salida puede ser analógica o digital dependiendo si la cámara incorpora un ADC y toda la electrónica asociada. En el caso de las cámaras analógicas, la salida es una señal analógica de video, que o puede venir acompañada o no, por otras señales de sincronización. La señal de video viene limitada por la anchura de banda y por el ruido análogo que puede proporcionar el cable. Además, pequeños errores de la señal entre la cámara y el ADC del frame grabber pueden causar pérdidas de fidelidad en la imagen.

Una señal de video compuesto analógico contiene toda la información de los píxeles con todas las señales de sincronismo en un mismo cable, lo que hace que la conexión sea simple y barata. Si la señal de video es de barrido variable, el cable es algo más complejo y debe llevar algunos hilos pero sigue siendo simple. El cable además puede tener algunas decenas de metros sin perder potencia la señal. Todas las cámaras estándar son analógicas, existen algunas cámaras de alta velocidad y de alta definición que también son analógicas.

2.4.2 CÁMARAS DE VIDEO DIGITAL

Cámara Digital

Las cámaras digitales utilizan la misma tecnología CCD que las analógicas, sin embargo; el ADC está dentro de la cámara y digitaliza el video directamente y proporciona una señal de salida digital que puede ser de distintos tipos. El hecho de que la señal se digitalice en la propia cámara hace que la calidad de la señal sea mejor, pero tiene el inconveniente de que los cables entre la cámara y el frame grabber no pueden ser muy largos y que, debido a que pasa cada una de las señales por cada cable, normalmente tienen un alto precio.

Sensor de Imagen Digital

Un sensor de imagen digital, actúa como la retina de los ojos, capta la luminosidad de las imágenes que son proyectadas sobre él continuamente y da inicio al proceso de captura de un ejemplar o de una secuencia de ejemplares de la imagen consecutivamente.

Se trata de un chip que puede contar con decenas de millones de transductores fotosensibles, cada uno de ellos capaz de convertir la energía luminosa de un punto de la imagen en carga eléctrica para ser leída o grabada posteriormente en la forma de imagen digitalizada en valores numéricos. Para la captación de la imagen a colores, es común que las cámaras de vídeo usen tres sensores (sistema 3CCD). (Steves Digicams, 2013)

Existen dos tipos de sensores, los CCD (*Fig. 2.4.3*) y los CMOS (*Fig.2. 4.4*).

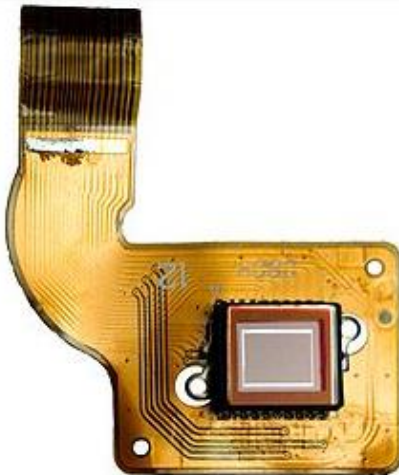


Fig. 2.4.3 Sensor de imagen CCD.

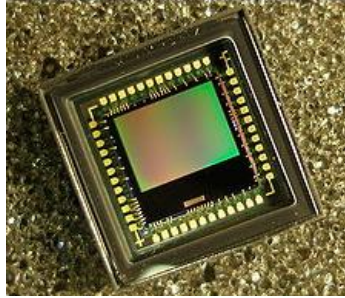


Fig. 2.4.4 Sensor de imagen CMOS.

Un CCD (charge-coupled device en español dispositivo de carga acoplada) es un circuito integrado que contiene un número determinado de condensadores enlazados o acoplados bajo el control de un circuito interno, cada condensador puede transferir su carga eléctrica a uno o a varios de los condensadores que estén a su lado en el circuito impreso. (TELEDYNE, 2013) La alternativa digital a los CCD son los dispositivos CMOS (complementary metal oxide semiconductor) utilizados en algunas cámaras digitales y en numerosas cámaras web. En la actualidad los CCD son mucho más populares en aplicaciones profesionales y en cámaras digitales.

El CCD es un sensor con diminutas células fotoeléctricas que registran la imagen. Desde allí la imagen es procesada por la cámara y registrada en la tarjeta de memoria. La capacidad de resolución o detalle de la imagen depende del número de células fotoeléctricas del CCD. Este número se expresa en píxeles. A mayor número de píxeles, mayor resolución. Actualmente las cámaras fotográficas digitales incorporan CCD con capacidades de hasta ciento sesenta millones de píxeles (160 megapíxeles).

Los píxeles del CCD registran gradaciones de los tres colores básicos: rojo, verde y azul (RGB), por lo cual tres píxeles, uno para cada color, forman un conjunto de células fotoeléctricas capaz de captar cualquier color en la imagen. Para conseguir esta separación de colores la mayoría de cámaras CCD utilizan un filtro Bayer (Fig. 2.4.5) que proporciona una trama para cada conjunto de cuatro píxeles de forma que un pixel registra luz roja, otro luz azul y dos píxeles se reservan para la luz verde. El resultado final incluye información sobre la luminosidad en cada píxel pero con una resolución en color menor que la resolución de iluminación. Se puede conseguir una mejor separación de colores utilizando dispositivos con tres CCD acoplados y un dispositivo de separación de luz como un prisma dicróico que separa la luz incidente en sus componentes rojo, verde y azul. Estos sistemas son mucho más caros que los basados en máscaras de color sobre un único CCD. Algunas cámaras profesionales de alta gama utilizan un filtro de color rotante para registrar imágenes de alta resolución de color y luminosidad pero son productos caros y tan solo pueden fotografiar objetos estáticos.

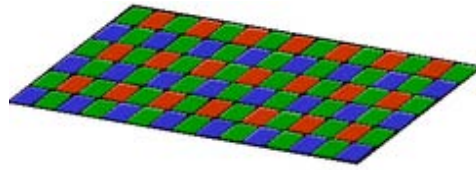


Fig. 2.4.5 Filtro Bayer utilizando numerosas cámaras digitales.

Los detectores CCD, al igual que las células fotovoltaicas, se basan en el efecto fotoeléctrico, la conversión espontánea de luz recibida en corriente eléctrica que ocurre en algunos materiales. La sensibilidad del detector CCD depende de la eficiencia cuántica del chip, la cantidad de fotones que deben incidir sobre cada detector para producir una corriente eléctrica. El número de electrones producido es proporcional a la cantidad de luz recibida (a diferencia de la fotografía convencional sobre negativo fotoquímico). Al final de la exposición los electrones producidos son transferidos de cada detector individual (fotosite) por una variación cíclica de un potencial eléctrico aplicada sobre bandas de semiconductores horizontales y aislados entre sí. De este modo, el CCD se lee línea a línea, aunque existen numerosos diseños diferentes de detectores.

Las imágenes obtenidas por una cámara CCD son sometidas a un proceso de corrección que consiste en restar de la imagen obtenida la señal producida espontáneamente por el chip por excitación térmica (campo oscuro) y dividir por una imagen de un campo homogéneo (campo plano o flat field) que permite corregir las diferencias de sensibilidad en diferentes regiones del CCD y corregir parcialmente defectos ópticos en la cámara o las lentes del instrumento utilizado.

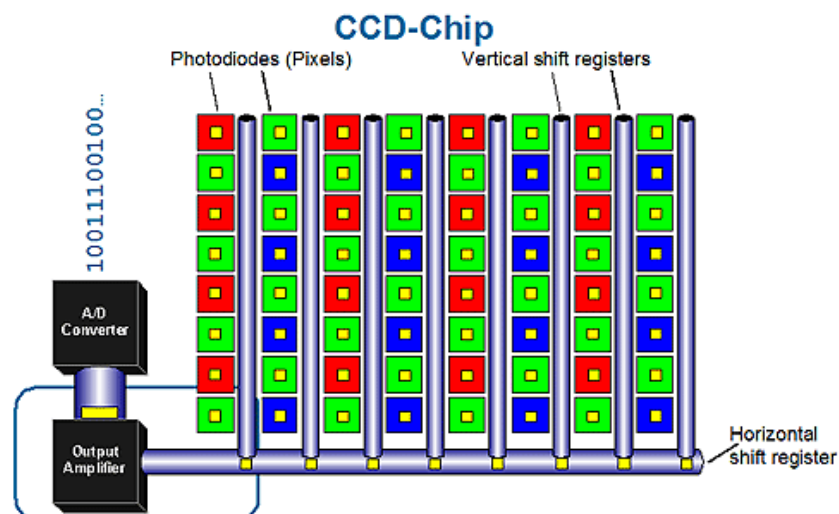


Fig. 2.4.6 CCD

Cámara IP

Lo que comúnmente se conoce como una cámara IP es una cámara que digitaliza y procesa las imágenes analógicas, las codifica internamente, y luego transmite la información de vídeo digital a través de una conexión Ethernet a un ordenador o dispositivo similar. (TTCS.SL, 2014) Una cámara IP puede tener un CMOS o en un sensor CCD, y está disponible en los mismos estilos que las cámaras de vigilancia tradicionales como Pan / Tilt / Zoom, cúpulas, balas, cajas, infrarrojos, encubiertas y sin hilos.

Cámaras IP están típicamente equipadas con un servidor web incorporado y se puede acceder y controlar a través de cualquier red IP como una red WAN, LAN, Intranet o Internet. Mediante la utilización de un navegador web estándar o los usuarios de software cliente puede ver la salida de una cámara IP de vídeo desde cualquier ubicación local o remota. Una cámara IP es un "dispositivo de red". Tiene su propia dirección IP, se conecta directamente a una red cableada o inalámbrica y no requiere mantenimiento.

Diferencia entre una cámara analógica y una IP

La principal diferencia entre las cámaras analógicas y IP es el método por el cual se transmite la señal de vídeo y, en última instancia, donde el vídeo se comprime, o "codificado".

Las cámaras analógicas no tienen incorporado los servidores web o los codificadores y no requieren mantenimiento técnico. Estas funciones se implementan en la grabación y / o equipos de control.

2.5 DISPOSITIVOS ESPECIALES DE GRABACIÓN DE VIDEO

Grabación analógica de video

Los métodos análogos de grabación recurren a una cinta magnética a la cual barren completamente dejando a su paso una huella electromagnética que puede traducirse luego en sonidos. Los impulsos electrónicos de las imágenes (señal de vídeo) y del sonido (señal de audio) se graban y almacenan en la cinta de vídeo (que es un soporte de plástico recubierto de óxido de hierro que queda magnetizado). Durante la reproducción, la información almacenada se vuelve a convertir en señales de audio y vídeo y son traducidas por el aparato de TV.

La cantidad de información electrónica es mucho mayor para la grabación de vídeo que para la de audio. El magnetoscopio es un aparato utilizado para grabar imágenes en movimiento en cinta magnética. También se le conoce como VTR (acrónimo del inglés video tape recorder) cinta abierta y VCR (*Fig.2.5.1*) Video Cassette Recorder, cuando la cinta viene en una cassette, como las cintas de uso doméstico. Muchas veces se le denomina según el formato de grabación o como vídeo.



Fig. 2.5.1 VCR

Actualmente existen grabadoras de vídeo digital (DVR) basadas en disco duro, esto significa un cambio de época o generacional ya que tradicionalmente se usaba el VCR como medio de almacenamiento. El DVR es mucho más cómodo, y también permite realizar diversas funciones, como pausar TV en vivo, repetición de escenas, persiguiendo la reproducción en una grabación se puede ver antes de que se ha completado, y omisión de publicidad. La mayoría de los DVR usan el MPEG formato para la compresión de las señales de vídeo digitalizadas.

Las capacidades de grabación de vídeo se han convertido en una parte esencial del decodificador, como espectadores de televisión han querido tomar el control de su experiencia de visualización. Dado que los consumidores han podido converger cantidades cada vez mayores de contenido de vídeo en sus decodificadores, entregados por transmisión tradicional de cable, satélite y terrestre, así como IP de redes, la capacidad de capturar la programación y verla cuando lo deseen se ha convertido en una función que actualmente tienen muchos consumidores.

2.5.1 GRABADOR DE VIDEO DIGITAL (DVR)

DVR

Un grabador de vídeo digital (*Fig. 2.5.2*) DVR, Digital Video Recorder es un dispositivo interactivo de grabación de video en formato digital. Se compone por hardware y software, donde el hardware consiste en un disco duro de gran capacidad, un microprocesador y los buses de comunicación, por otra parte el software proporciona diversas funcionalidades para el tratamiento de las secuencias de video recibidas, acceso a guías de programación y búsqueda avanzada de contenidos.

El DVR nace gracias al nuevo formato digital de la televisión, este hecho permite almacenar la información y manipularla posteriormente con un procesador. De modo que se podría calificar al DVR como una computadora especializada en el tratamiento de imágenes digitales. El DVR se ha diferenciado de su predecesor analógico la videograbadora en la cual tan solo se podían almacenar imágenes de forma pasiva, con la posibilidad de rebobinarlas hacia delante o hacia atrás, y por supuesto pausarlas.



Fig. 2.5.2 DVR

Fuente de Video

Televisión y vídeo son términos que a veces se utilizan indistintamente, pero difieren en su significado técnico. El video es la parte visual de la televisión, mientras que la televisión es la combinación de vídeo y de audio modulada en una frecuencia portadora (es decir, un canal de televisión) para la entrega.

Introducción a las fuentes analógicas

Los primeros grabadores de vídeo digitales se han diseñado para grabar la televisión analógica en los formatos NTSC , PAL o SECAM.

Para grabar una señal analógica se requieren unos pocos pasos. Tarjeta sintonizadora de TV sintoniza en una frecuencia particular y luego funciona como un capturador de fotogramas , rompiendo las líneas en píxeles individuales y cuantificación en un formato que un ordenador puede comprender. Entonces la serie de fotogramas junto con el audio (también muestreada y cuantificada) se comprimen en un formato manejable, como MPEG-2, por lo general en el software.

Introducción a las fuentes digitales

Grabación de señales digitales es generalmente una captura directa de los binarios MPEG datos que están siendo recibidos. No se requiere hardware caro para cuantificar y comprimir la señal (como la cadena de televisión ya lo ha hecho en el estudio).

PVR DVD basados en el mercado a partir de 2006 no son capaces de capturar el rango completo de la señal visual disponible con la televisión de alta definición (HDTV). Esto es así porque las normas HDTV se finalizaron en un momento posterior que los estándares para DVDs. Sin embargo, PVR DVD-basados se pueden utilizar (aunque a menor calidad visual) con la televisión de alta definición HDTV, ya disponible en la actualidad conjuntos también tienen conexiones de A / V estándar.

Cámaras de vídeo digital

Una cámara de video digital combina una cámara y una grabadora de vídeo digital.

Algunos DVR basados en DVD incorporan conectores que se pueden utilizar para capturar video digital desde una cámara de vídeo. Alguna edición del DVD resultante suele ser posible, por ejemplo, agregar puntos de capítulo.

Algunas grabadoras de vídeo digitales ahora pueden grabar en estado sólido tarjetas de memoria flash (llamadas cámaras de video en flash). Generalmente usan Secure Digital tarjetas, puede incluir conexiones inalámbricas (Bluetooth y Wi-Fi), y puede reproducir SWF archivos. Hay algunas grabadoras de vídeo digitales que combinan vídeo y gráficos en tiempo real a la tarjeta de memoria flash, llamado DTE o "directos para editar". Estos se utilizan para acelerar el flujo de trabajo de edición en la producción de video y televisión, desde cintas de vídeo no lineal entonces necesitan ser trasladados a la estación de trabajo de edición.

Aplicaciones del DVR

Grabación de TV

TV DVR utiliza generalmente la guía de programación electrónica (EPG).

Seguridad

Las grabadoras de vídeo digital están configuradas para aplicaciones de seguridad física, como grabar señales de vídeo de circuito cerrado de televisión para fines de documentación y detección. Muchos están diseñados para grabar audio. El DVR se han convertido en los dispositivos que son versátiles y ofrecen servicios que exceden el simple registro de imágenes de video que se hizo anteriormente a través de reproductores de vídeo. Un sistema de CCTV DVR ofrece una multitud de funciones avanzadas en tecnología de vídeo, incluyendo búsquedas de video por evento, fecha, hora y cámara. También hay mucho más control sobre la calidad y velocidad de cuadro que permite optimizar el uso de espacio en disco y el DVR puede configurarse para sobrescribir las imágenes más antiguas de seguridad si el disco se llena. En algunos sistemas de DVR de seguridad de acceso remoto de imágenes de seguridad utilizando una PC también se puede lograr mediante la conexión del DVR a una red LAN o Internet. Algunas de las últimas grabadoras de vídeo digital profesional de vídeo incluyen el firmware de análisis, para habilitar la funcionalidad como la "virtual Tripwire" o incluso la detección de objetos abandonados en la escena.

DVR de seguridad se pueden clasificar como sea basado en PC o incrustado . La arquitectura de un DVR basado en PC es un ordenador clásico personales con tarjetas de captura de vídeo diseñado para capturar imágenes de vídeo. Un tipo DVR incorporado está diseñado específicamente como un grabador de vídeo digital con su sistema operativo y software de aplicación que figura en el firmware o memoria de sólo lectura .

Características del hardware

Las características del Hardware en los DVRs de seguridad varían entre los fabricantes y pueden incluir, pero no están necesariamente limitados a:

- Diseñado para rack de montaje o configuraciones de escritorio.
- Entradas de vídeo únicas o múltiples con los tipos de conectores compatibles con el vídeo analógico o digital proporcionada como cable coaxial, par trenzado o de fibra óptica por cable. El número más común de las entradas son 1, 2, 4, 8, 16 y 32. Los sistemas pueden ser configurados con un gran número de entradas de la creación de redes obuses DVRs individuales juntas.
- Salidas controladas a los monitores de vídeo externos.
- Interruptores del panel frontal y los indicadores que permiten a las diversas características de la máquina a controlar.
- Conexiones en consonancia con el tipo de red y se utilizan para controlar las funciones de la grabadora y para enviar y / o recibir señales de vídeo en red.
- Las conexiones a los dispositivos de control externos como teclados .
- La conexión a las unidades de pan-tilt-zoom externos que las cámaras de posición.
- CD interno, DVD, dispositivos VCR normalmente para archivar video.
- Conexiones externas a los medios de almacenamiento .
- Entradas de evento de alarma de los dispositivos de detección de seguridad externa, por lo general una entrada por video.
- Alarma salidas de eventos de características de detección de internos, como la detección de movimiento o pérdida de vídeo.

Características del software

Las características del software pueden variar entre los fabricantes y pueden incluir, pero no están necesariamente limitados a:

- Seleccionables tasas de captura de imágenes de los usuarios, ya sea en régimen de todo o entrada de base de entrada. La característica de velocidad de captura puede ser programada para ajustar automáticamente la velocidad de captura de la ocurrencia de una alarma externa o un evento interno
- Seleccionable resolución de imagen ya sea en régimen de todo o entrada de base de entrada. La característica de resolución de la imagen puede ser programado para ajustar automáticamente la resolución de la imagen en la ocurrencia de una alarma externa o un respiradero e interna.
- Los métodos de compresión para determinar la calidad de la reproducción. Compresión de hardware H.264 ofrece altas velocidades de transferencia a través de Internet con el vídeo de alta calidad.
- Detección de movimiento : Siempre en una entrada de base de entrada, esta función detecta el movimiento en la imagen, total o una porción definida por el usuario de la imagen y por lo general proporciona ajustes de sensibilidad. Detección provoca un evento interno que puede ser la salida a un equipo externo y / o ser utilizados para provocar cambios en otras características internas.
- La falta de detección de movimiento. Siempre en una entrada de base de entrada, esta función detecta el movimiento de un objeto en el campo de visión y permanece inmóvil por un tiempo definido por el usuario. Detección provoca un evento interno que puede ser de salida al equipo externo y / o se utiliza para desencadenar cambios en otras características internas.
- Dirección de detección de movimiento. Siempre en una entrada de base de entrada, esta función detecta la dirección del movimiento en la imagen que se ha determinado por el usuario como un hecho inaceptable. Detección provoca un evento interno que puede ser la salida a un equipo externo y / o utilizarse para desencadenar cambios en otras características internas.
- Enrutamiento de entrada de vídeo a los monitores de vídeo basado en las entradas de usuario o automáticamente en alarmas o eventos.
- De entrada, fecha y hora de estampación .
- Alarma y registro de eventos en las entradas de vídeo correspondientes.
- Alarma y búsqueda de eventos.
- Uno o más canales de grabación de sonido.

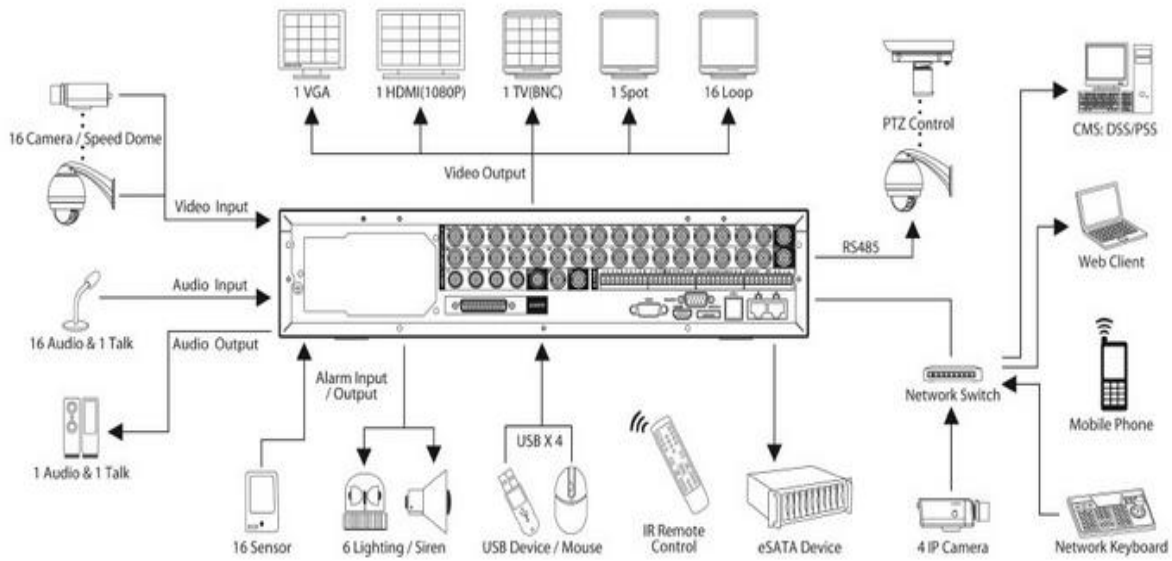


Fig. 2.5.3 Diagrama de conexión.

Formatos de archivo, resoluciones y sistemas de archivo.

Los DVR generalmente pueden grabar y reproducir H.264 , MPEG-4 Parte 2 , MPEG-2 . mpg , MPEG-2 . TS , VOB y las imágenes ISO de vídeo, con MP3 y AC3 pistas de audio. También pueden mostrar imágenes (JPEG y PNG) y reproducir archivos de música (MP3 y Ogg). Algunos dispositivos se pueden actualizar para reproducir y grabar en los nuevos formatos.

Las grabaciones de televisión de definición estándar suelen tener 480p/i/576p/i mientras que HDTV es por lo general en 720p/1080i.

Así mismo, suelen registrar en la propiedad de sistemas de archivos para la protección de copia, aunque puedan utilizar FAT sistemas de archivos.

2.5.2 GRABADOR DE VIDEO EN RED (NVR)

Un grabador de vídeo en red (NVR) es un programa de software el cual graba vídeo en formato digital a una unidad de almacenamiento como: disco duro, USB, Tarjeta SD, entre otros. Un NVR no contiene hardware de captura de vídeo dedicada. Sin embargo; el software se ejecuta normalmente en un dispositivo específico, por lo general utiliza un sistema operativo embebido. Para ayudar a mantener una mayor funcionalidad, los sistemas operativos estándar como Linux y Windows se utilizan con procesadores estándar de Intel y el software de gestión de vídeo. Un NVR normalmente se despliega en un vídeo IP de un sistema de video vigilancia.

Los grabadores de vídeo en red son diferentes de los grabadores de vídeo digital (DVR), ya que su entrada es a partir de una red en lugar de una conexión directa a una captura de video o tarjeta de sintonizador . El video en un DVR se codifica y se procesa en el DVR, mientras que el vídeo en un NVR se codifica y se procesa en la cámara, luego es transmitido al NVR para su almacenamiento o visualización remota.

Existen sistemas de seguridad NVR / DVR híbridos que incorporan funciones de ambos NVR y DVR; estos son considerados una forma de NVR.

Los sistemas de seguridad NVR son generalmente inalámbricos, tienden a ser más fáciles de instalar, se puede acceder a través de un navegador web, y permitir que el usuario será notificado por correo electrónico si se dispara una alarma.

2.6 CABLEADO Y MEDIOS DE ENLACE

Cableados y Medios de Enlace

Los medios de transmisión se pueden clasificar en dos grandes grupos, esto dependerá de la forma de conducir la señal a través del medio. Existen medios de transmisión guiados y medios de transmisión no guiados. Según el sentido de la transmisión podemos encontrarnos con tres tipos diferentes: simplex (Sólo permiten la transmisión en un sentido), half-duplex (una conexión en la que los datos fluyen en una u otra dirección, pero no las dos al mismo tiempo) y full-duplex (permitiendo canales de envío y recepción simultáneos).

Medios de transmisión guiados

Los medios de transmisión guiados están conformados por un cable que se encarga de la conducción de las señales desde un extremo al otro. Las principales características de los medios guiados son el tipo de conductor utilizado, la velocidad máxima de transmisión, las distancias máximas que puede ofrecer entre repetidores, la inmunidad frente a interferencias electromagnéticas, la facilidad de instalación y la capacidad de soportar diferentes tecnologías de nivel de enlace.

La velocidad de transmisión depende directamente de la distancia entre los terminales, y de si el medio se utiliza para realizar un enlace punto a punto o un enlace multipunto. Debido a esto los diferentes medios de transmisión tendrán diferentes velocidades de conexión que se adaptarán a utilizaciones dispares.

Dentro de los medios de transmisión guiados, los más utilizados en el campo de las comunicaciones son:

2.6.1 CABLE DE PAR TRENZADO

Cable de par trenzado

Consiste en un par de hilos de cobre conductores cruzados entre sí, con el objetivo de reducir el ruido de diafonía. Existen dos tipos de par trenzado:

- **Protegido:** Shielded Twisted Pair (STP)
- **No protegido:** Unshielded Twisted Pair (UTP): es un cable de pares trenzado y sin recubrimiento metálico externo, de modo que es sensible a las interferencias. Es importante guardar la numeración de los pares, ya que de lo contrario el efecto del trenzado no será eficaz, disminuyendo sensiblemente o incluso impidiendo la capacidad de transmisión. Es un cable barato, flexible y sencillo de instalar

Las aplicaciones principales en las que se hace uso de cables de par trenzado son:

- **Bucle de abonado:** es el último tramo de cable existente entre el teléfono de un abonado y la central a la que se encuentra conectado. Este cable suele ser UTP Cat.3 y en la actualidad es uno de los medios más utilizados para transporte de banda ancha, debido a que es una infraestructura que está implantada en el 100% de las ciudades.
- **Redes LAN:** en este caso se emplea UTP Cat.5 o Cat.6 para transmisión de datos, consiguiendo velocidades de varios centenares de Mbps. Un ejemplo de este uso lo constituyen las redes 10/100/1000BASE-T.

Categoría 6 (Cable UTP)

Cable de categoría 6, o Cat 6 (ANSI/TIA/EIA-568-B.2-1) es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retrocompatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para la diafonía (o crosstalk) y ruido. El estándar de cable es utilizable para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 Mbits en cada par.

Composición del cable

El cable contiene 4 pares de cable de cobre trenzado. La especificación ANSI/TIA-568-B.2-1 aclara que el cable puede estar hecho con calibres de cable entre 22 y 24 AWG, mientras que el cable cumpla todos los estándares de testeo indicados. Cuando es usado como un patch cable, Cat-6 es normalmente terminado con conectores RJ-45, a pesar de que algunos cables Cat-6 son incómodos para ser terminados de tal manera sin piezas modulares especiales y esta práctica no cumple con el estándar.

Si los componentes de los varios estándares de cables son mezclados entre sí, el rendimiento de la señal quedará limitada a la categoría que todas las partes cumplan. Como todos los cables definidos por TIA/EIA-568-B, el máximo de un cable Cat-6 horizontal es de 90 metros (295 pies). Un canal completo (cable horizontal más cada final) está permitido a llegar a los 100 metros en extensión.

Los cables UTP Cat-6 comerciales para redes LAN, son eléctricamente construidos para exceder la recomendación del grupo de tareas de la IEEE, que está trabajando desde antes de 1997. (Molina 2004, p 110 -111)

En la categoría 6 (*Tabla 2.6.1*), el cableado para trabajar en redes sobre 250 MHz, los valores propuestos que se deben cumplir son:

| frecuencia (MHz) | PS Atenuación (dB) | pr-pr NEXT (dB) | PS NEXT (dB) | pr-pr ELFEXT (dB) | PS ELFEXT (dB) | Pérdida retorno (dB) | Retraso Fase (ns) | Retraso Torc. (ns) |
|------------------|--------------------|-----------------|--------------|-------------------|----------------|----------------------|-------------------|--------------------|
| 1 | 2,2 | 72,7 | 70,3 | 63,2 | 60,2 | 19,0 | 580,0 | 50,0 |
| 4 | 4,2 | 63,0 | 60,5 | 51,2 | 48,2 | 19,0 | 563,0 | 50,0 |
| 10 | 6,5 | 56,6 | 54,0 | 43,2 | 40,2 | 19,0 | 556,8 | 50,0 |
| 16 | 8,3 | 53,2 | 50,6 | 39,1 | 36,1 | 19,0 | 554,5 | 50,0 |
| 20 | 9,3 | 51,6 | 49,0 | 37,2 | 34,2 | 19,0 | 553,6 | 50,0 |
| 31,25 | 11,7 | 48,4 | 45,7 | 33,3 | 30,3 | 17,1 | 552,1 | 50,0 |
| 62,5 | 16,9 | 43,4 | 40,6 | 27,3 | 24,3 | 14,1 | 550,3 | 50,0 |
| 100 | 21,7 | 39,9 | 37,1 | 23,2 | 20,2 | 12,0 | 549,4 | 50,0 |
| 125 | 24,5 | 38,3 | 35,4 | 21,3 | 18,3 | 11,0 | 549,0 | 50,0 |
| 155,52 | 27,6 | 36,7 | 33,8 | 19,4 | 16,4 | 10,1 | 548,7 | 50,0 |
| 175 | 29,5 | 35,8 | 32,9 | 18,4 | 15,4 | 9,6 | 548,6 | 50,0 |
| 200 | 31,7 | 34,8 | 31,9 | 18,4 | 15,4 | 9,0 | 548,4 | 50,0 |
| 250 | 36,0 | 33,1 | 30,2 | 17,2 | 14,2 | 8,0 | 548,2 | 50,0 |

Tabla 2.6.1 Especificaciones ISO Cat. 6



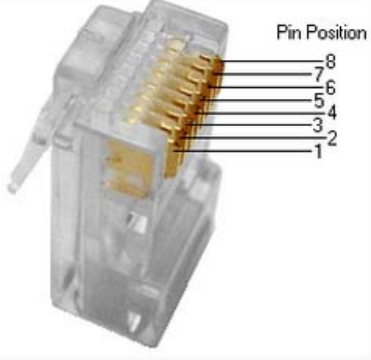






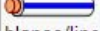
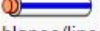


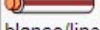
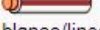


| Pin | T568A Par | T568B Par | Cable | T568A Color | T568B Color | Pins en la cara del enchufe (el socket se invierte) |
|-----|-----------|-----------|-------|--|--|--|
| 1 | 3 | 2 | tip |  blanco/linea verde |  blanco/linea naranja |  |
| 2 | 3 | 2 | ring |  verde |  naranja | |
| 3 | 2 | 3 | tip |  blanco/linea naranja |  blanco/linea verde | |
| 4 | 1 | 1 | ring |  azul |  azul | |
| 5 | 1 | 1 | tip |  blanco/linea azul |  blanco/linea azul | |
| 6 | 2 | 3 | ring |  naranja |  verde | |
| 7 | 4 | 4 | tip |  blanco/linea marron |  blanco/linea marron | |
| 8 | 4 | 4 | ring |  marron |  marron | |

Fig. 2.6.1 Composición del cable para usarlo con RJ-45

Categoría 6ª

La TIA (Telecommunications Industry Association) aprobó una nueva especificación estándar de rendimiento mejorados para sistemas con cables trenzados no blindado (unshielded) y cables trenzados blindado (Foiled). La especificación ANSI/TIA/EIA-568-B.2-10 indica sistemas de cables llamados Categoría 6 Aumentada o más frecuentemente "Categoría 6A", que operan a frecuencias de hasta 550 MHz (tanto para cables no blindados como cables blindados) y proveen transferencias de hasta 10 Gbit/s (10GBASE-T). La nueva especificación mitiga los efectos de la diafonía o crosstalk. Soporta una distancia máxima de 100 metros. En el cable blindado la diafonía externa (crosstalk) es virtualmente cero.

Longitud máxima

Cuando se utiliza para 10/100/1000 BASE-T, la longitud máxima permitida de un cable Cat 6 es de 100 metros o 328 pies. Consiste en 90 metros (295.275591 pies) de sólido "horizontal" cableado entre el panel de conexiones y la toma de pared, además de 10 metros (32.808399 pies) de cable de conexión trenzado entre cada gato y el dispositivo conectado.

Cuando se usa para 10GBASE-T, Cat 6 longitud máxima del cable es 55 metros en un entorno de alien crosstalk favorable, pero sólo 37 metros en un entorno hostil con diafonía extraña, como por ejemplo cuando se instalan varios cables juntos. Sin embargo, debido a que los efectos de los ámbitos de alien crosstalk en los cables son difíciles de determinar antes de la instalación, se recomienda que todos los cables Cat 6 se utilizan para 10GBASE-T están eléctricamente probados una vez instalados. Con sus especificaciones mejoradas, Cat 6A no tiene esta limitación y se puede ejecutar 10GBASE-T en 100 metros sin la prueba electrónica.

Advertencias de instalación

Los cables categoría 6 y 6a deben estar correctamente instalados y terminados para cumplir con las especificaciones. El cable no debe estar retorcido o doblado demasiado fuerte (el radio de curvatura debe ser de al menos cuatro veces el diámetro exterior del cable. Los pares de cables deben estar sin torsión y la cubierta exterior no debe ser despojada de más de 1/2 pulgada (1,27 cm).

Todos los cables blindados deben estar conectados a tierra para garantizar seguridad y eficacia y una conexión de blindaje continuo mantiene de principio a fin se desarrollan cuando hay más de una conexión a tierra y la diferencia de potencial de voltaje en modo común a estas conexiones a tierra introducir ruido en el cableado.

2.6.2 FIBRA ÓPTICA

La fibra óptica

La fibra óptica es un medio de transmisión empleado habitualmente en redes de datos. Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio y superiores a las de cable convencional. Son el medio de transmisión por excelencia al ser inmune a las interferencias electromagnéticas, también se utilizan para redes locales, en donde se necesite aprovechar las ventajas de la fibra óptica sobre otros medios de transmisión.

Cable de fibra por su composición hay tres tipos disponibles actualmente:

- Núcleo de plástico y cubierta plástica
- Núcleo de vidrio con cubierta de plástico (frecuentemente llamada fibra PCS, El núcleo silicio cubierta de plástico)
- Núcleo de vidrio y cubierta de vidrio (frecuentemente llamadas SCS, silicio cubierta de silicio)

Las fibras de plástico tienen ventajas sobre las fibras de vidrio por ser más flexibles y más fuertes, fáciles de instalar, pueden resistir mejor la presión, son menos costosas y pesan aproximadamente 60% menos que el vidrio. La desventaja es su característica de atenuación alta: no propagan la luz tan eficientemente como el vidrio. Por tanto las de plástico se limitan a distancias relativamente cortas, como puede ser dentro de un solo edificio.

Las fibras con núcleos de vidrio tienen baja atenuación. Sin embargo, las fibras PCS son un poco mejores que las fibras SCS. Además, las fibras PCS son menos afectadas por la radiación y, por lo tanto, más atractivas a las aplicaciones militares. Desafortunadamente, los cables SCS son menos fuertes, y más sensibles al aumento en atenuación cuando se exponen a la radiación. (Bartnikas & Srivastava, 2010, p 53-54)

Cable de fibra óptica disponible en construcciones básicas:

- Cable de estructura holgada.
- Cable de estructura ajustada.

Para explicar los distintos tipos de fibra se ha tomado la explicación de los autores Bartikas, Srivastava (2010, p 55-70), Jardón y Linares. (1995, p 30-46)

Cable de estructura holgada

Consta de varios tubos de fibra rodeando un miembro central de refuerzo, y rodeado de una cubierta protectora. El rasgo distintivo de este tipo de cable son los tubos de fibra. Cada tubo, de dos a tres milímetros de diámetro, lleva varias fibras ópticas que descansan holgadamente en él. Los tubos pueden ser huecos o, más comúnmente estar llenos de un gel resistente al agua que impide que ésta entre en la fibra. El tubo holgado aísla la fibra de las fuerzas mecánicas exteriores que se ejerzan sobre el cable. (Fig.2.6.2)

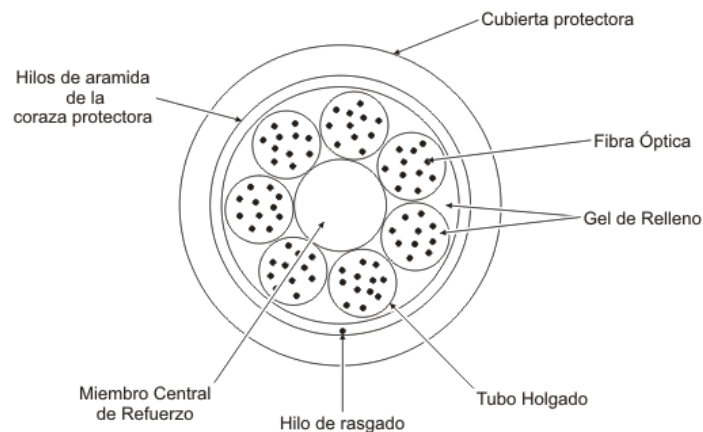


Fig. 2.6.2 Cable de tubo holgado.

El centro del cable contiene un elemento de refuerzo, que puede ser acero, Kevlar o un material similar. Este miembro proporciona al cable refuerzo y soporte durante las operaciones de tendido, así como en las posiciones de instalación permanente. Debería amarrarse siempre con seguridad a la polea de tendido durante las operaciones de tendido del cable, y a los anclajes apropiados que hay en cajas de empalmes o paneles de conexión.

La cubierta o protección exterior del cable se puede hacer, entre otros materiales, de polietileno, de armadura o coraza de acero, goma o hilo de aramida, y para aplicaciones tanto exteriores como interiores. Con objeto de localizar los fallos con el OTDR de una manera más fácil y precisa, la cubierta está secuencialmente numerada cada metro (o cada pie) por el fabricante. (Fig. 2.6.3)

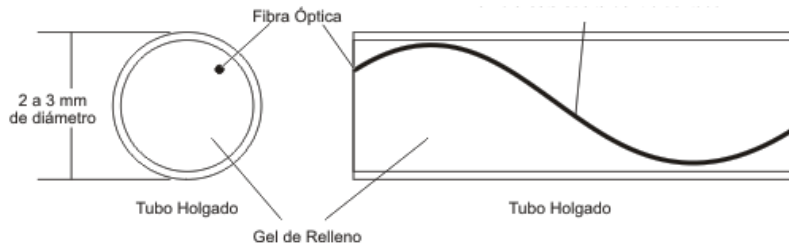


Fig. 2.6.3 Tubo holgado de cable de fibra óptica.

Cable de estructura ajustada

Contiene varias fibras con protección secundaria que rodean un miembro central de tracción, y todo ello cubierto de una protección exterior. La protección secundaria de la fibra consiste en una cubierta plástica de $900 \mu\text{m}$ de diámetro que rodea al recubrimiento de $250 \mu\text{m}$ de la fibra óptica. (Fig. 2.6.4)

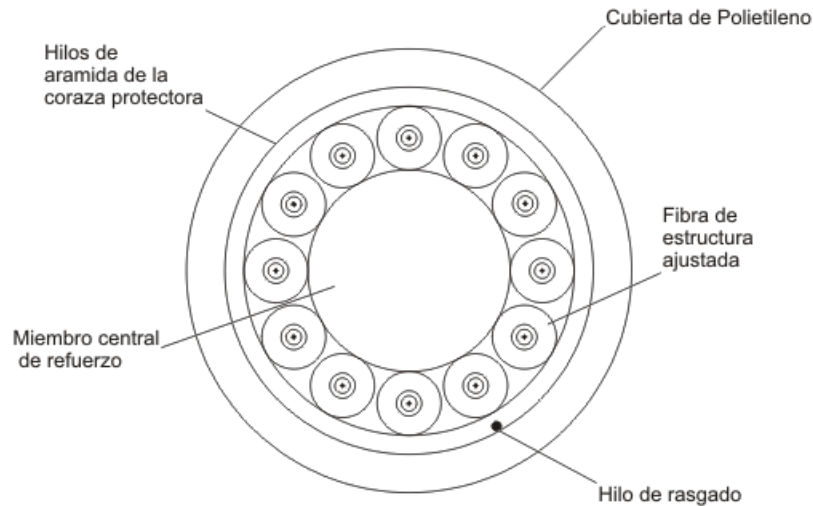


Fig. 2.6.4 Cable de estructura ajustada.

Cable blindado

Tienen una coraza protectora o armadura de acero debajo de la cubierta de polietileno. Esto proporciona al cable una resistencia excelente al aplastamiento y propiedades de protección frente a roedores. Se usa frecuentemente en aplicaciones de enterramiento directo o para instalaciones en entornos de industrias pesadas. El cable se encuentra disponible generalmente en estructura holgada aunque también hay cables de estructura ajustada. (Fig. 2.6.5)

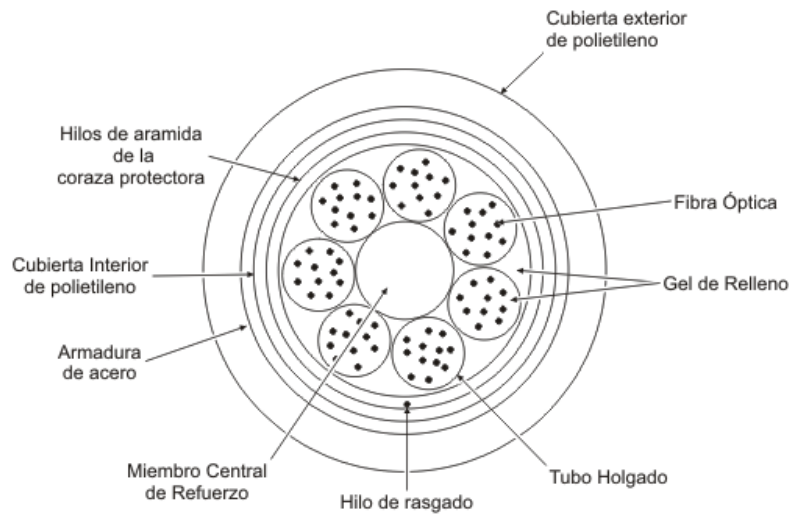


Fig. 2.6.5 Cable de fibra óptica con armadura.

Clasificación de las fibras ópticas

Las fibras ópticas utilizadas actualmente en el área de las telecomunicaciones se clasifican fundamentalmente en dos grupos según el modo de propagación: Fibras Multimodo y Fibras Monomodo.

Fibras ópticas Multimodo

Son aquellas que pueden guiar y transmitir varios rayos de luz por sucesivas reflexiones, (modos de propagación). Los modos son formas de ondas admisibles, la palabra *modo* significa trayectoria. (Fig. 2.6.6)

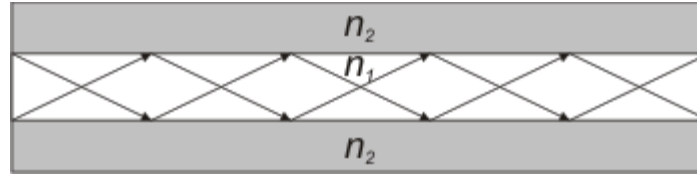


Fig. 2.6.6 Fibra Multimodo

Fibras ópticas Monomodo

Son aquellas que por su especial diseño pueden guiar y transmitir un solo rayo de luz (un modo de propagación) y tiene la particularidad de poseer un ancho de banda elevadísimo. (Fig. 2.6.7)

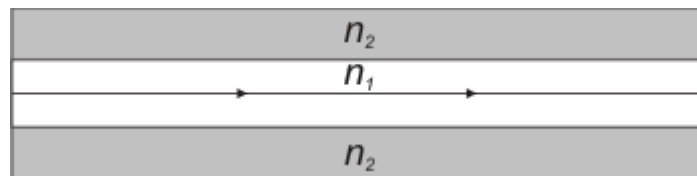


Fig. 2.6.7 Fibra Monomodo

En estas fibras monomodo cuando se aplica el emisor de luz, el aprovechamiento es mínimo, también el costo es más elevado, la fabricación difícil y los acoples deben ser perfectos.

| Medio de Transmisión | Razón de datos total | Ancho de Banda | Separación entre repetidores |
|----------------------|----------------------|----------------|------------------------------|
| Par Trenzado | 4 Mbps | 3 Mhz | 2 a 10 km |
| Cable Coaxial | 500 Mbps | 350MHz | 1 a 10 km |
| Fibra Óptica | 2Gbps | 2GHz | 10 a 100 km |

Tabla 2.6.2 Tabla de comparación entre los medios de transmisión guiados.

Medios de transmisión no guiados

En este tipo de medios tanto la transmisión como la recepción de información se lleva a cabo mediante antenas. A la hora de transmitir, la antena irradia energía electromagnética en el medio. Por el contrario, en la recepción la antena capta las ondas electromagnéticas del medio que la rodea.

La configuración para las transmisiones no guiadas puede ser direccional y omnidireccional.

- Direccional, la antena transmisora emite la energía electromagnética concentrándola en un haz, por lo que las antenas emisora y receptora deben estar alineadas.
- Omnidireccional, la radiación se hace de manera dispersa, emitiendo en todas direcciones, pudiendo la señal ser recibida por varias antenas.

Generalmente, cuanto mayor es la frecuencia de la señal transmitida es más factible confinar la energía en un haz direccional.

La transmisión de datos a través de medios no guiados añade problemas adicionales, provocados por la reflexión que sufre la señal en los distintos obstáculos existentes en el medio. Resultando más importante el espectro de frecuencias de la señal transmitida que el propio medio de transmisión en sí mismo.

Según el rango de frecuencias de trabajo, las transmisiones no guiadas se pueden clasificar en tres tipos: radio, microondas y luz (infrarrojos/láser).

| Banda de Frecuencia | Nombre | Modulación | Razón de Datos | Aplicaciones Principales |
|---------------------|--------------------------------|---------------|----------------|---|
| 30-300 kHz | LF (low frequency) | ASK, FSK, MSK | 0,1-100 bps | Navegación |
| 300-3000 kHz | MF (medium frequency) | ASK, FSK, MSK | 10-1000 bps | Radio AM Comercial |
| 3-30 MHz | HF (high frequency) | ASK, FSK, MSK | 10-3000 bps | Radio de onda corta |
| 30-300 MHz | VHF (very high frequency) | FSK, PSK | Hasta 100 kbps | Television VHF, Radio FM |
| 300-3000 MHz | UHF (ultra high frequency) | PSK | Hasta 10 Mbps | Television UHF, Microondas Terrestres |
| 3-30 GHz | SHF (super high frequency) | PSK | Hasta 100Mbps | Microondas terrestres y por satélite |
| 30-300 GHz | EHF (extremely high frequency) | PSK | Hasta 750 Mbps | Enlaces cercanos con punto a punto experimentales |

Tabla 2.6.3 Tabla de comparación de rangos de frecuencias.

2.6.3 WI –FI

Wi-Fi

El trabajo que realizó Molina (2004, p 119-127) ayuda a explicar la comunicación inalámbrica, se han tomado algunas ideas para la redacción de los siguientes párrafos. La forma de comunicación Wi – Fi (Wireless Fidelity en español fidelidad inalámbrica) es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica. Los dispositivos habilitados con Wi-Fi, tales como: una computadora personal, una consola de videojuegos, un smartphone o un reproductor de audio digital, pueden conectarse a Internet a través de un punto de acceso de red inalámbrica. Dicho punto de acceso (hotspot) tiene un alcance de unos 20 metros en interiores y al aire libre una distancia mayor. Pueden cubrir grandes áreas la superposición de múltiples puntos de acceso.



Fig. 2.6.8 Comportamiento Wi-Fi.

Dispositivos

Existen varios dispositivos Wi-Fi, los cuales se pueden dividir en dos grupos: Dispositivos de Distribución o Red, entre los que destacan los routers, puntos de acceso y Repetidores; y Dispositivos Terminales que en general son las tarjetas receptoras para conectar a la computadora personal, ya sean internas (tarjetas PCI) o bien USB.

Dispositivos de Distribución o Red:

- Los puntos de acceso son dispositivos que generan un "set de servicio", que podría definirse como una "Red Wi-Fi" a la que se pueden conectar otros dispositivos. Los puntos de acceso permiten, en resumen, conectar dispositivos en forma inalámbrica a una red existente. Pueden agregarse más puntos de acceso a una red para generar redes de cobertura más amplia, o conectar antenas más grandes que amplifiquen la señal.
- Los repetidores inalámbricos son equipos que se utilizan para extender la cobertura de una red inalámbrica, éstos se conectan a una red existente que tiene señal más débil y crean una señal limpia a la que se pueden conectar los equipos dentro de su alcance. Algunos de ellos funcionan también como punto de acceso.³
- Los router inalámbricos son dispositivos compuestos, especialmente diseñados para redes pequeñas (hogar o pequeña oficina). Estos dispositivos incluyen, un Router (encargado de interconectar redes, por ejemplo, nuestra red del hogar con internet), un punto de acceso (explicado más arriba) y generalmente un switch que permite conectar algunos equipos vía cable (Ethernet yUSB). Su tarea es tomar la conexión a internet, y brindar a través de ella acceso a todos los equipos que conectemos, sea por cable o en forma inalámbrica.

Ventajas

- Al ser redes inalámbricas, la comodidad que ofrecen es muy superior a las redes cableadas porque cualquiera que tenga acceso a la red puede conectarse desde distintos puntos dentro de un rango suficientemente amplio de espacio.
- Una vez configuradas, las redes Wi-Fi permiten el acceso de múltiples ordenadores sin ningún problema ni gasto en infraestructura, ni gran cantidad de cables.
- La Wi-Fi Alliance asegura que la compatibilidad entre dispositivos con la marca *Wi-Fi* es total, con lo que en cualquier parte del mundo podremos utilizar la tecnología Wi-Fi con una compatibilidad total.
-

Desventajas

- Una de las desventajas que tiene el sistema Wi-Fi es una menor velocidad en comparación a una conexión cableada, debido a las interferencias y pérdidas de señal que el ambiente puede acarrear.
- La desventaja fundamental de estas redes existe en el campo de la seguridad. Existen algunos programas capaces de capturar paquetes, trabajando con su tarjeta Wi-Fi en modo promiscuo, de forma que puedan calcular la contraseña de la red y de esta forma acceder a ella. Las claves de tipo WEP son relativamente *fáciles de conseguir* con este sistema. La alianza Wi-Fi arregló estos problemas sacando el estándar WPA y posteriormente WPA2, basados en el grupo de trabajo 802.11i. Las redes protegidas con WPA2 se consideran robustas dado que proporcionan muy buena seguridad. De todos modos muchas compañías no permiten a sus empleados tener una red inalámbrica. Este problema se agrava si consideramos que no se puede controlar el área de cobertura de una conexión, de manera que un receptor se puede conectar desde fuera de la zona de recepción prevista (e.g. desde fuera de una oficina, desde una vivienda colindante).
- Hay que señalar que esta tecnología no es compatible con otros tipos de conexiones sin cables como Bluetooth, GPRS, UMTS, etc.

2.7 SISTEMAS DE ALIMENTACIÓN DE ENERGÍA

2.7.1 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA

Un sistema de alimentación ininterrumpida, SAI, también conocido como UPS (del inglés uninterruptible power supply), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante la ausencia de energía eléctrica a todos los dispositivos que tenga conectados. Otras de las funciones que se pueden adicionar a estos equipos es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Los SAI dan energía eléctrica a equipos llamados cargas críticas, como pueden ser aparatos médicos, industriales o informáticos que, como se ha mencionado anteriormente, requieren tener siempre alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión). (Rojas, 2008)

Como consulta para los tipos de SAI se recurrió a: APC y Mitsubishi (2014)

Tipos de SAI

SAI de continua

Las cargas conectadas a los SAI requieren una alimentación de corriente continua, por lo tanto éstos transformarán la corriente alterna de la red comercial a corriente continua y la usarán para alimentar la carga y almacenarla en sus baterías. Por lo tanto no requieren convertidores entre las baterías y las cargas.

SAI de corriente alterna

Estos SAI obtienen a su salida una señal alterna, por lo que necesitan un inversor para transformar la señal continua que proviene de las baterías en una señal alterna.

SAI en estado de espera (Stand-by Power Systems)

Es llamado sistema en "stand-by", o en espera, debido a que el circuito de alimentación alternativo, el inversor, está "fuera de línea", o inactivo, en espera de entrar en funcionamiento cuando se produzca un fallo en la alimentación de red. Posee un elemento conmutador que conecta y desconecta uno u otro circuito alternativamente.

SAI en línea (on-line)

En cambio, en el SAI "en línea" (on-line), la batería y el Inversor están permanentemente siendo utilizados, lo que garantiza una máxima respuesta en tiempo y forma ante el evento de falla de red. Además, también pueden corregir los desplazamientos de frecuencia, ya que re-generan la onda alterna permanentemente (entrada alterna, rectificado a continua, inversor vuelve a generar tensión alterna).

SAI con volante inercial

En este caso la energía para mantener el suministro de alimentación eléctrica se conserva a través del denominado Almacenamiento cinético. De esta manera, no se requiere el uso de baterías y con ello se evita la necesidad de mantenerlas o reemplazarlas.

Aplicación del SAI

El papel del SAI es suministrar potencia eléctrica en ocasiones de fallo de suministro, en un intervalo de tiempo "corto". Algunas fallas comunes son:

Corte de energía: pérdida total de tensión de entrada.

- **Sobretensión:** tiene lugar cuando la tensión supera el 110% del valor nominal.
- **Caída de tensión:** cuando la tensión es inferior al 85-80% de la nominal.
- **Picos de tensión.**
- **Ruido eléctrico o electromagnético.**
- **Inestabilidad en la frecuencia.**
- **Distorsión armónica:** cuando la onda sinusoidal suministrada no tiene esa forma.

2.7.2 POE

Power Over Ethernet (PoE)

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 a un dispositivo de red (switch, punto de acceso, router, teléfono o cámara IP, etc.) usando el mismo cable que se utiliza para la conexión de red. Elimina la necesidad de utilizar tomas de corriente en las ubicaciones del dispositivo alimentado 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. *(Fig 2.7.1)*

Ventajas

- PoE es una fuente de alimentación inteligente: Los dispositivos se pueden apagar o reiniciar desde un lugar remoto usando los protocolos existentes, como el Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol).
- PoE simplifica y abarata la creación de un suministro eléctrico altamente robusto para los sistemas: La centralización de la alimentación a través de concentradores (hubs) PoE significa que los sistemas basados en PoE se pueden enchufar al Sistema de alimentación ininterrumpida (SAI) central.
- Los dispositivos se instalan fácilmente allí donde pueda colocarse un cable LAN, y no existen las limitaciones debidas a la proximidad de una base de alimentación.
- Un único juego de cables para conectar el dispositivo Ethernet y suministrarle alimentación, lo que simplifica la instalación y ahorra espacio.
- La instalación no supone gasto de tiempo ni de dinero ya que no es necesario realizar un nuevo cableado.
- PoE dificulta enormemente cortar o destrozarse el cableado: Generalmente el cableado se encuentra unido a bandejas en los huecos del techo o detrás de conductos de plástico de muy difícil acceso.

Desventajas

- Ausencia de estándares tecnológicos para la interoperabilidad de equipos.
- Para poder usar PoE, todos los dispositivos de Red (Hub/Switch, Cámaras IP, Puntos de Acceso) deben ser compatibles con la norma (IEEE 802.3af).

Funcionamiento PoE

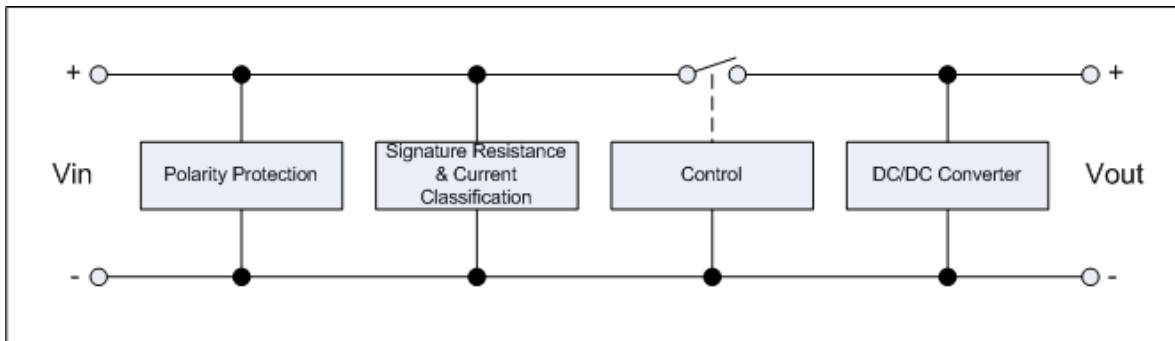


Fig.2. 7.1 Fases de PoE

La figura muestra las fases que debe realizar un PoE para poder alimentar usando un cable. Estas fases son 4, y cada una se corresponde con un bloque:

- **Primer bloque:** “Polarity Protection” o “Auto-polarity Circuit”. Como indica la norma, la tensión introducida puede venir de dos formas: una de las formas consiste en usar el par de datos del cable de Ethernet como fuente de alimentación. Dicha forma permite transmitir datos y alimentar a la vez por el mismo par. La segunda forma usa otros pares alternativos para enviar la tensión.
- **Segundo bloque:** “Signature and Class circuitry”. Para asegurarse que el dispositivo no aplica una tensión a un dispositivo que no implementa PoE, el dispositivo empezará a dar unos determinados niveles de tensión. Estos niveles de tensión se dividen en 4 etapas. Al principio el dispositivo aplicará una tensión baja (2.7V a 10.1V) buscando una resistencia de 25K Ω . Si es demasiado alta o demasiado baja, no hará nada. Esta fase permite proteger un dispositivo que no es PoE de uno que sí que lo es. En caso de que resulte ser PoE, buscará que clase de alimentación requiere. Para ello, elevará la alimentación a 14,5-20,5 V y medirá la corriente que circula a través de él.

- **Tercer bloque:** “Control Stage”. Es importante que el convertidor Dc/Dc no funcione mientras el dispositivo está realizando la fase de clasificación del bloque dos. El controlador deberá estar encendido cuando $V = 35\text{ V}$
- **Cuarto bloque:** “Convertidor DC/DC”. Generalmente la tensión nominal usada es de 48V y no suele ser práctica en muchas aplicaciones, dónde se requiere un voltaje menor (3.3V, 5V o 12V). Una manera muy efectiva de lograr este objetivo es usar un convertidor Buck DC/DC. Este convertidor es capaz de trabajar en un amplio rango de tensiones (36V a 57V), en condiciones de mínima y máxima carga.

Después de explicar esto, se tiene que hablar brevemente de cuál es la máxima potencia que puede entregar. Aunque ya se mencionó algo en la fase 2, es recomendable explicar lo siguiente: La máxima potencia que puede dar la fuente de alimentación es de 15.4W (400mA @ 48V o 350mA @ 44V) [La norma IEEE 802.3af no deja muy clara estas últimas medidas]. Si se cuenta las pérdidas, entonces la potencia máxima será de 12.95W (350mA @ 37V). En muchos casos esta cifra también se queda algo corta, pues, supone que el convertidor DC/DC tiene eficiencia máxima. Al final, la potencia será un valor comprendido entre 12.95 – 10.36 W (el último valor será el peor caso posible).

CAPÍTULO III
DESCRIPCIÓN DE
LA PROBLEMÁTICA

DESCRIPCIÓN DE LA PROBLEMÁTICA DENTRO Y EN LOS ALREDEDORES DE LA FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

La Facultad de Estudios Superiores Aragón es una entidad académica, la cual pertenece a la Universidad Nacional Autónoma de México. Fue fundada en el año de 1976 con el objetivo de satisfacer la demanda que tenía Ciudad Universitaria. Desde esa época la Facultad se ha consolidado como una de las más importantes entidades académicas de nivel superior en el norte del Área Metropolitana y en el Estado de México, ofreciendo catorce licenciaturas de las áreas Físico Matemáticas y de las Ingenierías, Ciencias Sociales y Artes y Humanidades, atendiendo aproximadamente a 17,027 alumnos hasta el año 2012. (FES Aragón Historia, 2014)

La multidisciplinaria cuenta con una amplia población, todas las personas realizan labores académicas día con día dentro de la Facultad, utilizando las instalaciones que esta ofrece para la comunidad universitaria; sin embargo, debido a que es una gran cantidad de universitarios no se puede tener un control eficaz, por lo tanto esto causa que en ocasiones los alumnos dañen las instalaciones provocando una mala imagen de la Facultad.

La propuesta de colocar un sistema de video vigilancia surge de la necesidad de contar con mayor seguridad planteada por los alumnos y por los daños físicos que sufre la Facultad. El vandalismo es uno de los principales problemas con los que se encuentra día a día las instalaciones y los alumnos. El vandalismo se ha definido en este trabajo de investigación como robos de accesorios en aulas, baños y demás, daño de aulas que no permiten tener un mobiliario adecuados para el uso académico.

La FES Aragón cuenta con diferentes áreas donde los universitarios desarrollan actividades académicas, culturales y deportivas diariamente. Algunas de éstas son: CIMA, Centro Tecnológico, Biblioteca, Laboratorios, Aulas, Estacionamiento, Centro de Extensión Universitaria y Área Deportiva, entre otras. Cabe mencionar que el Área Deportiva cuenta con una gran extensión territorial, la cual no se utiliza en su totalidad, quedando sola y sin vigilancia en ciertos horarios y épocas del año. Por lo tanto el Área Deportiva, queda vulnerable y es muy fácil que puedan ingresar saltándose la reja que existe para delimitar la Institución y la vía pública.

Debido a que la Facultad está ubicada en la Avenida Rancho Seco, sin número, en el municipio de Nezahualcóyotl, Estado de México colindando con las colonias Impulsora, Plazas de Aragón, Prados y Bosques de Aragón (*Fig 3.1.1*), entre los metros Nezahualcóyotl e Impulsora, los estudiantes deben trasladarse a ésta, pasando por colonias con alto índice de criminalidad, lo que conlleva que los delincuentes tengan como principal objetivo los transportes públicos y las calles cercanas para llegar a la Facultad, afectando a los alumnos y académicos de la Institución.

Fernández desde el año 2011 comenta la situación de agravios tras entrevistar a varios estudiantes y corroborando la investigación con las encuestas realizadas en el 2014, los robos y daños ocurren con frecuencia dentro de la entidad académica. La necesidad detectada es la falta de seguridad dentro y en los alrededores de la Facultad, ya que las poblaciones sensibles afectadas son: alumnos, académicos, administrativos y personal de trabajo.

Por otro lado, existen diferentes formas de acceso a la Facultad por las cuales toda la comunidad universitaria ingresa. La primera forma es por avenida Rancho Seco, donde se puede encontrar la entrada peatonal y la entrada vehicular, esta última para ingresar al estacionamiento de estudiantes, la segunda forma es por avenida Bosques de África, donde se puede ingresar de la misma manera, solamente que la entrada vehicular es para el estacionamiento de profesores. La salida se lleva a cabo de la misma forma por la que se entra a la Facultad.

Finalmente, otra problemática que surge es en los accesos, debido a que en la Institución no se tiene el suficiente control de las personas y vehículos que ingresan, por lo que es muy fácil que sujetos ajenos a la entidad académica puedan entrar sin ningún problema pudiendo realizar actos vandálicos ya sea a las instalaciones o a las personas que estudian y laboran dentro de la Institución.



Fig. 3.1.1 Colonias que rodean la FES Aragón.

CAPÍTULO IV
METODOLOGÍA DE
ANÁLISIS Y
PROPUESTA
TÉCNICA

4.1 METODOLOGÍA DE ANÁLISIS

4.1.1 INTRODUCCIÓN

Para contrarrestar la problemática, se ha tomado la decisión de proponer un diseño de ingeniería basado en un sistema de video vigilancia IP, con el propósito de tener un mayor control en los accesos a la Facultad y disminuir el daño a las instalaciones. Así mismo se hace el uso de las nuevas tendencias en tecnología y telecomunicaciones para que la Facultad pueda ser monitoreada vía remota, sin necesidad de trasladarse a ésta, a cualquier hora y época del año, por lo tanto esto genera una vigilancia cómoda y a la vez más eficaz.

4.1.2 ¿EN QUÉ CONSISTE EL DISEÑO DEL SISTEMA DE VIDEO VIGILANCIA IP PARA LA FES ARAGÓN?

El diseño del sistema de video vigilancia consiste en la instalación de cámaras de video vigilancia en las entradas y salidas de la Facultad, así como dentro de la misma. Éstas cámaras serán monitoreadas por el personal de seguridad desde una central de video vigilancia que estará dentro de la Institución, sin embargo; también podrán ser monitoreadas sin la necesidad de estar en la central, esto quiere decir que las imágenes captadas por las cámaras podrán ser visualizadas en equipos terminales en cualquier parte de la Facultad o en el exterior. Algunos de estos equipos son: Computadoras de escritorio, Computadoras personales, Tabletas, celulares, entre otros.

La comunicación vía remota entre la central de video vigilancia y los equipos terminales se logra realizar gracias al internet que se implementa en el sistema. Así mismo el tipo de redes que se pretende utilizar en el diseño del sistema son las siguientes:

LAN - Local Area Network por sus iniciales en inglés o Red de Área Local en español, esta será útil para que se lleve a cabo la interconexión y comunicación entre la central y los equipos terminales dentro de la Facultad.

WAN - World Area Network por sus iniciales en inglés o Red de Área Global en español, ésta será útil para que se lleve a cabo la interconexión y comunicación entre la central y los equipos terminales en cualquier parte del mundo.

Por otra parte, el sistema no solamente se encarga de captar imágenes y visualizarlas en los monitores de los dispositivos electrónicos, también tiene la función de grabar estas imágenes en dispositivos de almacenamiento masivo llamados DVR, Digital Video Recorder por sus iniciales en inglés o Grabador de Video Digital en español, para que en el caso de que ocurra un evento no deseado, como por ejemplo: Asaltos dentro de la Facultad, Choque en el estacionamiento, Mal uso de las instalaciones, por nombrar algunos, se pueda acudir a la central de video vigilancia y revisar el DVR para ver las imágenes que ha grabado y con esto saber quién es el responsable.

4.1.3 DESARROLLO DE LA METODOLOGÍA DE ANÁLISIS

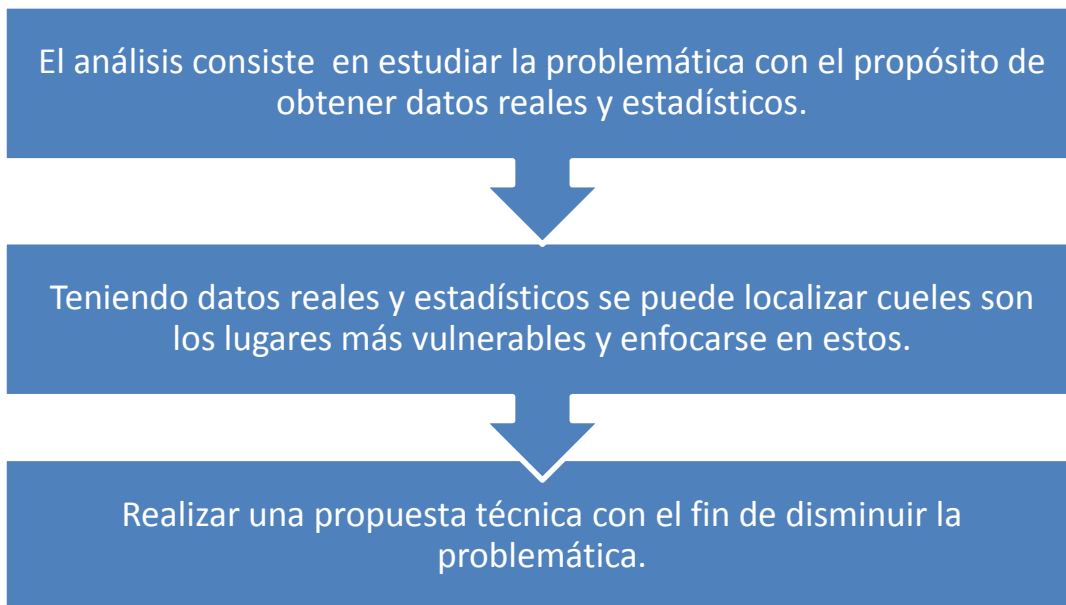


Fig. 4.1.1 Metodología de análisis

En la *Fig. 4.1.1* se muestra los pasos a seguir dentro de la metodología para llegar al objetivo de éste trabajo de investigación que es realizar una propuesta de un diseño de video vigilancia IP para la FES Aragón.

Datos Estadísticos

Los datos estadísticos se obtuvieron principalmente de una fuente interna la cual fueron los alumnos. Se aplicó un cuestionario piloto, el cual se realizó para este trabajo de investigación en el año 2014. Éste cuestionario piloto se realizó a 210 estudiantes de la FES Aragón con el propósito de recaudar datos tanto de seguridad como de acontecimientos que los universitarios han vivido y visto durante la estancia en la Facultad.

Fuente interna

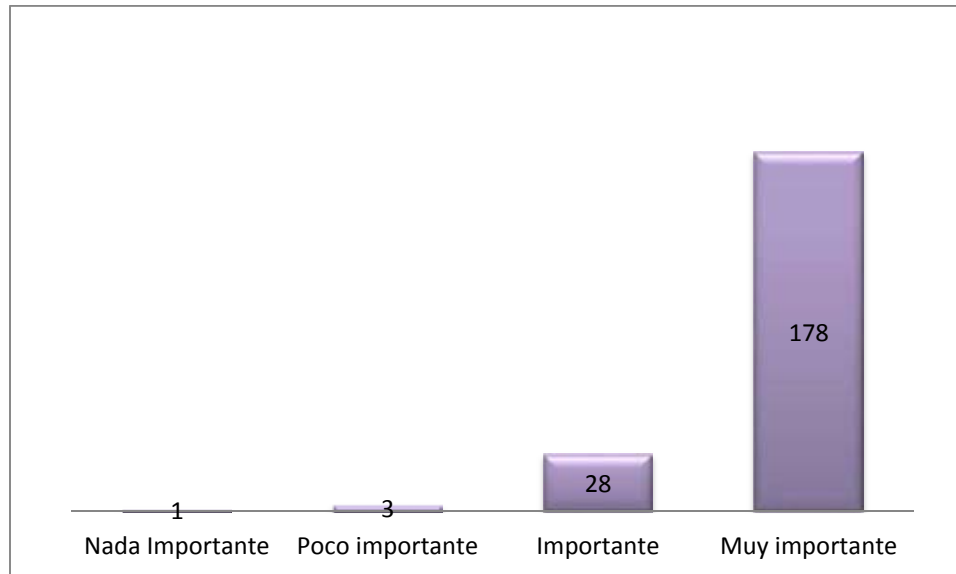
Durante este trabajo de investigación se ha realizado un cuestionario piloto, el cual se aplicó a 210 estudiantes de distintas carreras de la FES Aragón. Éste cuestionario tuvo como finalidad recaudar datos estadísticos, los cuales fueron:

- Saber que tan importante es la seguridad en la Facultad para los estudiantes.
- Saber el nivel de seguridad con el que se cuenta actualmente.
- ¿Qué tan bueno sería tener un sistema de cámaras de video vigilancia?
- Saber si han presenciado daño a las instalaciones o algún robo dentro o fuera de la Facultad.
- ¿Qué zonas consideran ser vigiladas?
- ¿Qué horario y que temporada consideran apropiado para que el sistema esté en funcionamiento y pueda estar la Facultad vigilada?
- ¿Qué tanto impacto tendría la instalación del sistema de video vigilancia?
- Sexo y Edad.

La recaudación de estos datos estadísticos arrojó los siguientes resultados los cuales se visualizan en las siguientes gráficas:

1. ¿Qué tan importante es para el estudiante la seguridad dentro y fuera de la Facultad?

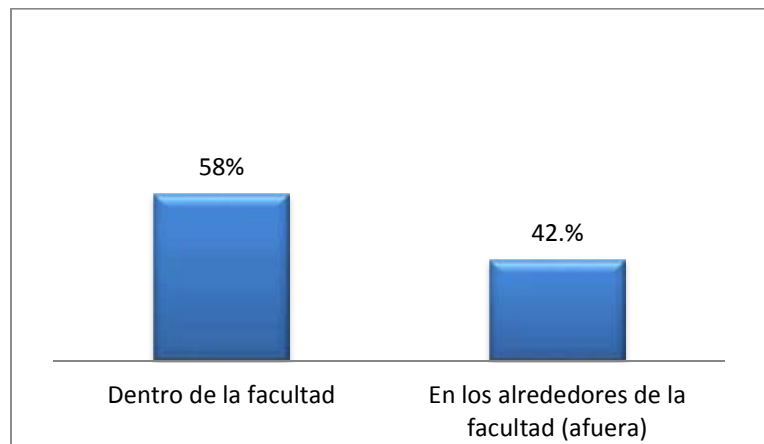
Teniendo como opciones: Nada importante, Poco importante, Importante y Muy importante. 178 alumnos respondieron que es Muy importante, como se muestra en la *Gráfica 4.1.1*.



Gráfica 4.1.1 Importancia de la seguridad dentro y fuera de la Facultad.

2. Calificación del 1 al 10 según el nivel de seguridad con el que cuenta la FES Aragón dentro y fuera actualmente.

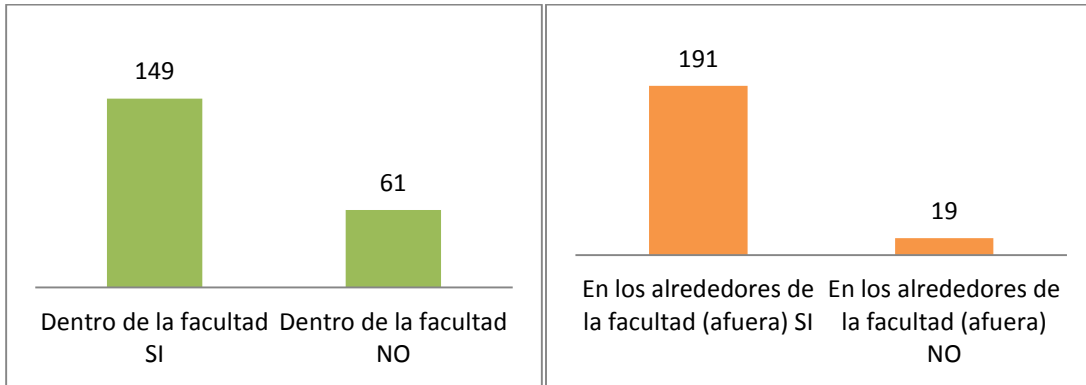
El 58% de los alumnos encuestados han reflejado que se sienten seguros dentro de la Facultad y el 42% se sienten seguros fuera, lo que refleja que la mayoría de los alumnos sienten más seguridad dentro de la Facultad.



Gráfica 4.1.2 Seguridad dentro y fuera de la Facultad.

- ¿Ayudaría a la FES Aragón contar con un sistema de cámaras de video vigilancia dentro y en los alrededores de ésta?

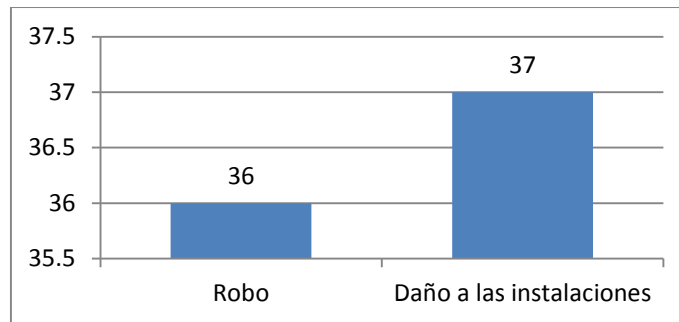
Los resultados fueron positivos para la implementación del sistema de video vigilancia, *Gráfica 4.1.3.*



Gráfica 4.1.3 ¿Ayudaría tener un sistema de cámaras de video vigilancia?

- ¿Les ha tocado presenciar daño a las instalaciones o robo?

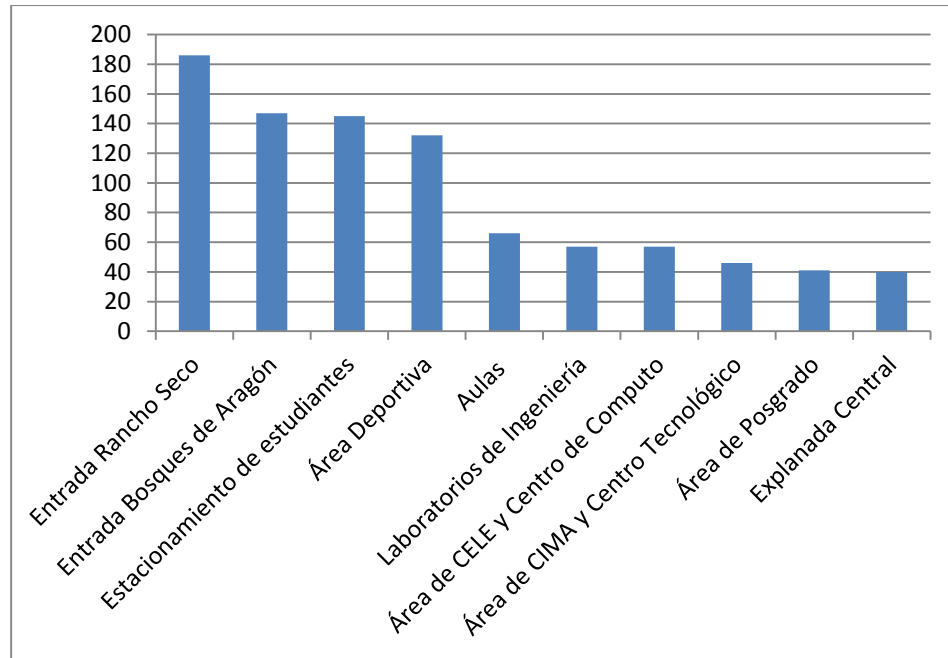
De los 210 alumnos que realizaron la encuesta, 73 respondieron que si han presenciado daño a las instalaciones o algún robo dentro de ésta. *Gráfica 4.1.4.*



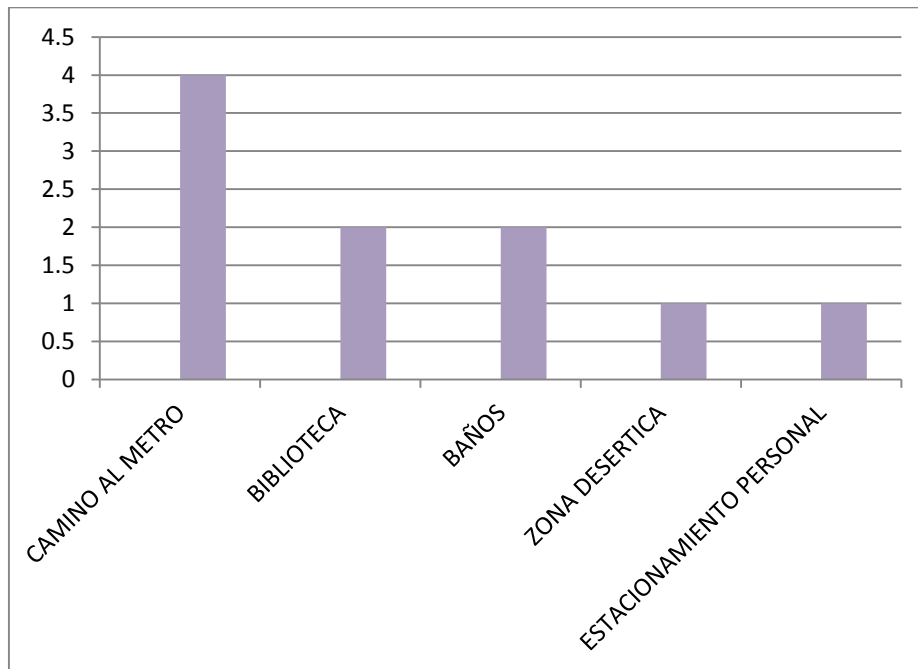
Gráfica 4.1.4 Daño a las instalaciones o robo.

5. ¿Qué Zonas consideran los estudiantes ser vigiladas?

En la *Gráfica 4.1.5* se muestra las opciones que venían dentro del cuestionario, en la *Gráfica 4.1.6* se muestra otras zonas que ellos consideran ser vigiladas.



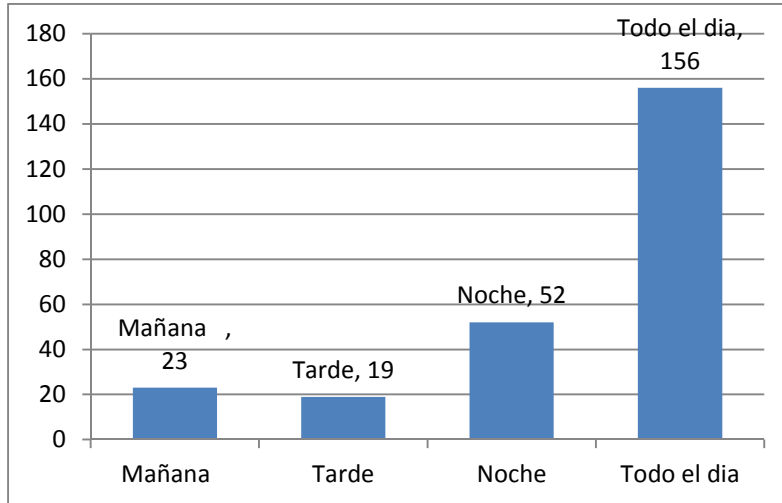
Gráfica 4.1.5 Zonas consideradas a ser vigiladas.



Gráfica 4.1.6 Otras Zonas.

6. Horario el cual se considera tener en funcionamiento el sistema de video vigilancia.

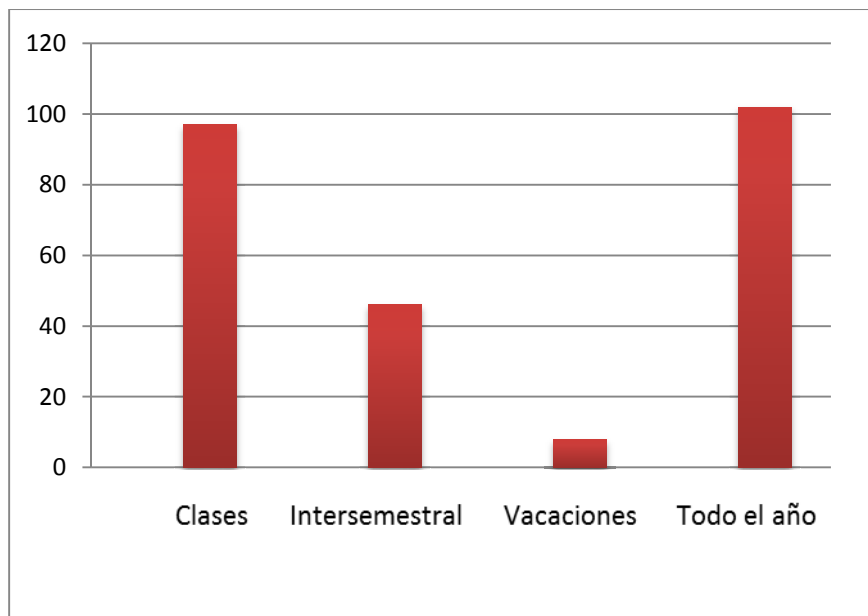
Los alumnos seleccionaron una o más de una opción entre: Mañana, Tarde, Noche y Todo el día. *Gráfica 4.1.7.*



Gráfica 4.1.7 Horario de Vigilancia.

7. Temporadas que son consideradas para que el sistema de video vigilancia esté operando.

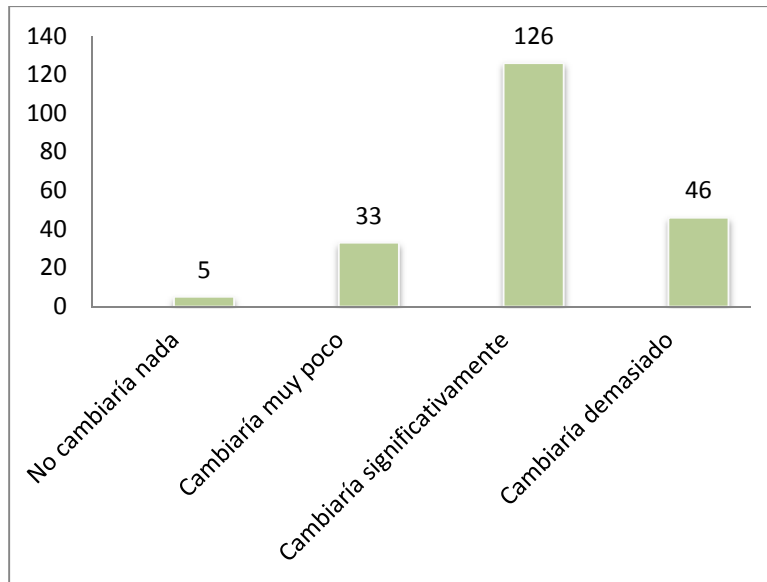
Los alumnos seleccionaron una o más de una opción entre: Día de clases, Periodo Intersemestral, Vacaciones o Todo el año. *Gráfica 4.1.8.*



Gráfica 4.1.8 Temporada de vigilancia.

8. ¿Qué tanto mejoraría el buen uso de las instalaciones y la seguridad en la FES Aragón con la implementación del sistema de video vigilancia?

Finalmente el cuestionario termina con esta pregunta arrojando un resultado positivo para la implementación de un sistema de video vigilancia, ver *Gráfica 1.9*. Los alumnos tenían las siguientes opciones: No cambiaría nada, Cambiaría muy poco, Cambiaría significativamente o Cambiaría demasiado.



Gráfica 4.1.9 Implementación del Sistema de Video Vigilancia.

Una vez aplicando éste cuestionario, se puede observar las necesidades que tienen los alumnos de la Facultad en materia de seguridad. Así mismo los resultados mostrados indican las zonas requeridas para ser vigiladas así como el horario y la temporada del año. Una vez teniendo estos datos se puede plantear una propuesta técnica para atacar estas necesidades y así cubrirlas.

4.2 PROPUESTA TÉCNICA

4.2.1 IDENTIFICACIÓN DE ZONAS DE RIESGO

Debido a los resultados arrojados en la aplicación de un cuestionario piloto que se realizó a la población de alumnos de la Facultad de Estudios Superiores Aragón, se pudo obtener las zonas más demandadas para ser vigiladas *Fig. 4.2.1*, las cuales son las siguientes:

- **Zona de Riesgo Alto:** Estacionamiento de Alumnos, Área Deportiva y las entradas de Bosques de Aragón y Rancho Seco.
- **Zona de Riesgo Medio:** Aulas, Laboratorios de Ingeniería, Área de CELE y Centro de Computo.
- **Zona de Riesgo Bajo:** Área de CIMA y Centro Tecnológico, Área de Posgrado y Explanada Central.

Se propone la instalación de un sistema de cámaras de video vigilancia en las zonas demandadas por la comunidad universitaria las cuales serán monitoreadas por el personal de vigilancia ya sea en los centros de control o vía remota.

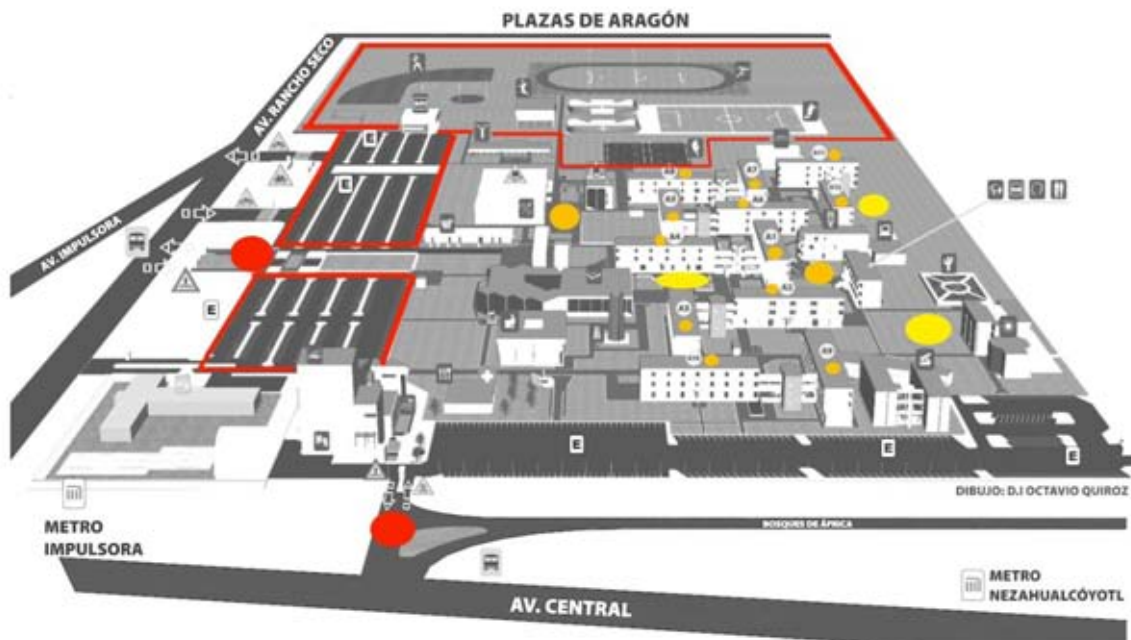


Fig. 4.2.1 Mapa FES Aragón indicando zonas de riesgo.

CAPÍTULO V
DESARROLLO DE LA
PROPUESTA
TÉCNICA

5.1 DESARROLLO DE LA PROPUESTA TÉCNICA

La propuesta para la implementación del sistema de cámaras de video vigilancia se basa en los datos estadísticos que resultaron del cuestionario aplicado a la comunidad universitaria. Estos datos indican las principales zonas que deben ser vigiladas según las necesidades de los alumnos, sin embargo; se debe de tomar en cuenta diversos factores para la implementación de ésta propuesta los cuales se desarrollan en éste capítulo.

5.2 TIPOS DE CÁMARAS DE VIDEO VIGILANCIA

| ZONA | TIPO DE CÁMARA |
|-----------------------------------|----------------|
| Entradas-Salidas Peatonales | Mini Domo |
| Entradas-Salidas Vehiculares | Bala HLC |
| Estacionamientos y Área Deportiva | PTZ y Bala |
| Laboratorios | Bala |
| Explanada Central | Bala |
| CIMA Y Centro Tecnológico | Bala |
| CELE y Centro de Computo | Bala |

Tabla 5.2.1 Tipos de cámaras.

Se instalarán cámaras dentro del campus las cuales tendrán diferentes características según la Zona que se vigilará, todo esto con el fin de obtener una captura de imágenes más eficiente. *Tabla 5.2.1*

5.2.1 DESCRIPCIÓN DE LAS CÁMARAS

Cámara PTZ: El significado de las siglas PTZ es: Pan Tilt Zoom. Estas cámaras tienen como característica principal un movimiento sobre dos ejes, ya sea horizontal o vertical así como tener la capacidad de hacer acercamientos. Debido a las características que ofrece ésta cámara, se planea para ser instaladas en zonas abiertas como son el Estacionamiento y el Área Deportiva. *Ver Fig. 5.2.1.*



Fig. 5.2.1 Cámara PTZ

Cámara Bala: Estas cámaras serán instaladas en entradas y salidas vehiculares así como en los edificios dentro de la Facultad con la finalidad de dar un seguimiento al tránsito de los alumnos. Existen dos tipos de cámara tipo Bala, los cuales son:

- Cámara con lente Vari focal: Este tipo está especialmente diseñada para funcionar a diferentes distancias focales por lo cual nos permite ajustar el ángulo de apertura dependiendo la distancia que se quiere enfocar. Estas cámaras pretenden ser instaladas en estacionamientos y en los edificios de las facultad para vigilar el transito del alumnado. *Ver Fig. 5.2.2.*



Fig. 5.2.2 Cámara Bala

- **Cámara HLC:** Cámaras High Low Contrast que en español quiere decir cámaras de alto y bajo contraste, este tipo de cámaras están diseñadas para ajustar el contraste debido a la luz que le es emitida al objetivo. Por lo anterior cumplen las características para ser instaladas en las entradas y salidas vehiculares. *Ver Fig. 5.2.3.*



Fig. 5.2.3 Cámara Bala HLC

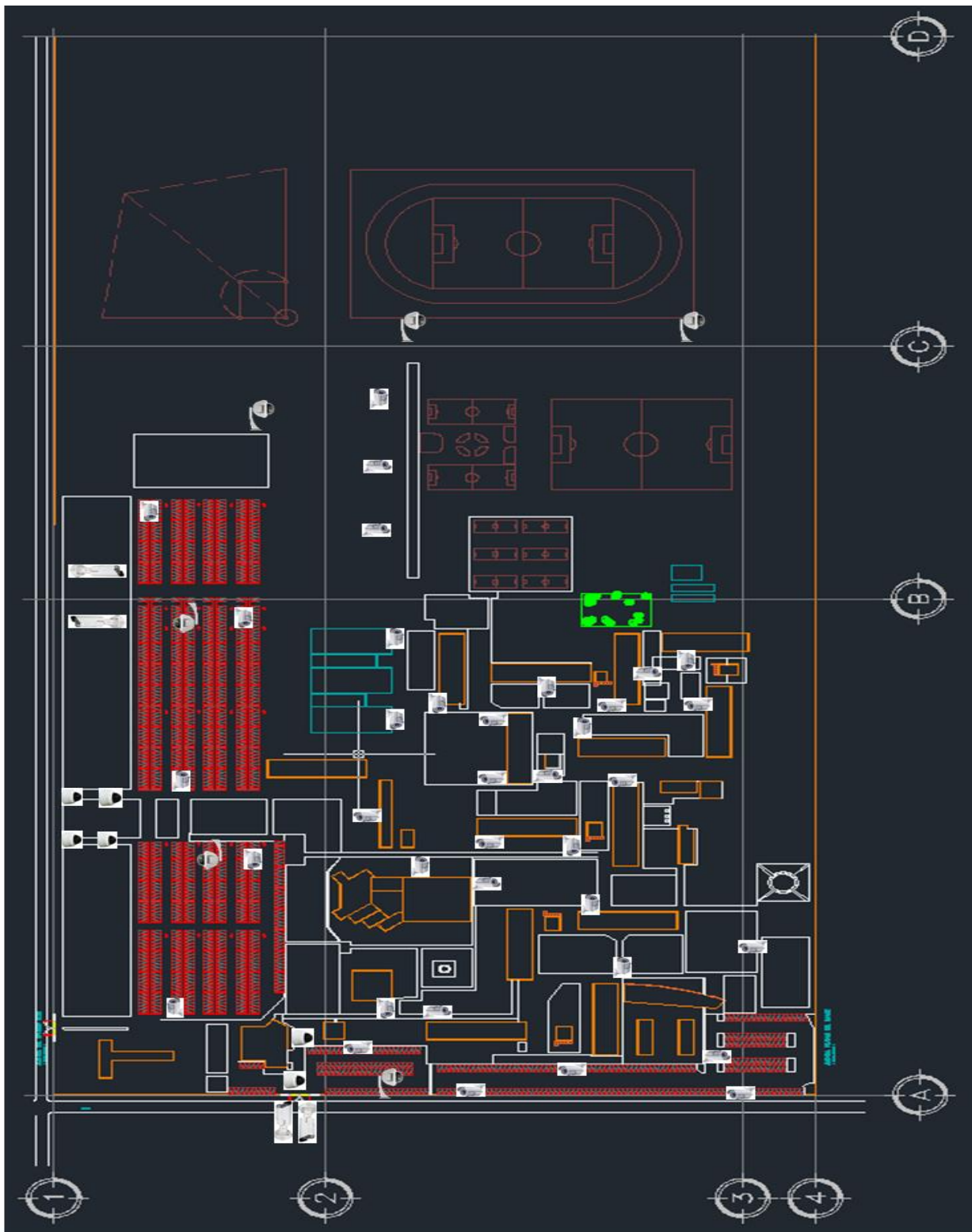
Cámara Mini Domo: Este tipo de cámaras serán instaladas en las entradas y salidas peatonales así como en la zona de cajas. Cuentan con un pequeño domo el cual las cubre de diversas situaciones ambientales y así mismo no deja que se vea a que dirección está vigilando lo que provoca el fenómeno de disuasión en las personas que la llegan a ver. *Ver Fig. 5.2.4.*



Fig. 5.2.4 Cámara Mini Domo

5.3 UBICACIÓN DE LAS CÁMARAS

Un punto importante en la elaboración de la propuesta es la ubicación de las cámaras. Las cámaras de video vigilancia se instalarán en base a los resultados obtenidos en la aplicación del cuestionario. En el *Plano 5.3.1*, se observan el tipo y la ubicación general de las cámaras.



Plano 5.3.1 Ubicación general de las cámaras.

5.3.1 UBICACIÓN POR ZONAS DE LAS CÁMARAS

- ZONA 1: Estacionamiento de alumnos.
- ZONA 2: Estacionamiento profesores.
- ZONA 3: Área deportiva.
- ZONA 4: Edificios, Pasillos y Explanadas.

ZONA 1: Estacionamiento de Alumnos

El estacionamiento de alumnos está integrado por tres secciones de cajones para autos, también está integrado por la entrada y salida vehicular y finalmente por la entrada y salida peatonal, todos estos accesos y salidas colindan con la avenida rancho seco. En el *Plano 5.3.2* se muestra la ubicación de cada cámara en esta zona.

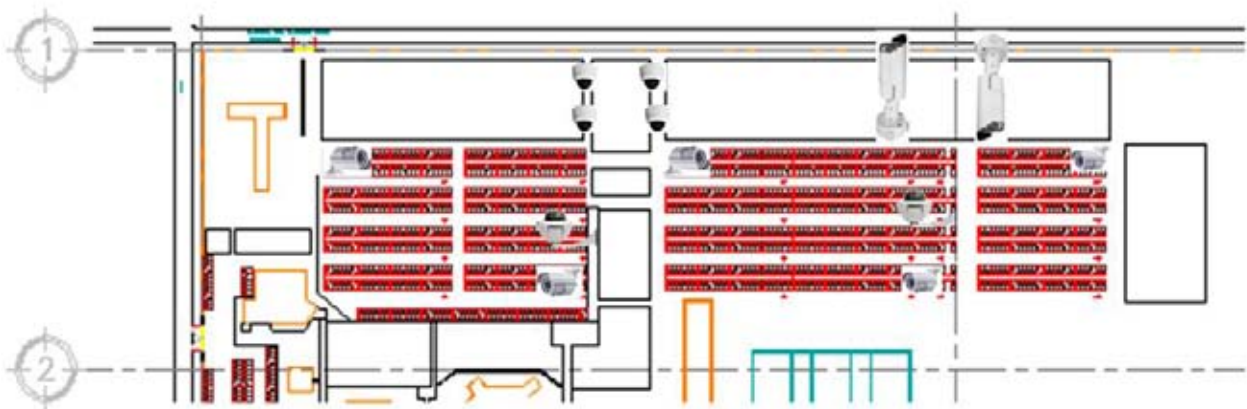
La cantidad y el tipo cámaras que se instalarán en esta zona son:

5 Tipo Bala – Para vigilar los cajones de estacionamiento.

12 Tipo Bala HLC – Existen 6 plumas en la entrada y 6 en la salida vehicular, por lo tanto se instalará 1 cámara por cada pluma.

2 Tipo PTZ – Para reforzar la vigilancia en el estacionamiento teniendo la posibilidad de mover la cámara y hacer acercamientos.

4 Mini Domo – 2 para la entrada y 2 para la salida peatonal.



Plano 5.3.2 ZONA 1

ZONA 2: Estacionamiento de Profesores

El estacionamiento de profesores por los cajones para autos, por la entrada y salida tanto peatonal como vehicular que colindan con la colonia Bosques de Aragón y finalmente por las cajas de la FES Aragón. En el *Plano 5.3.3* se muestra la ubicación de cada cámara en esta zona.

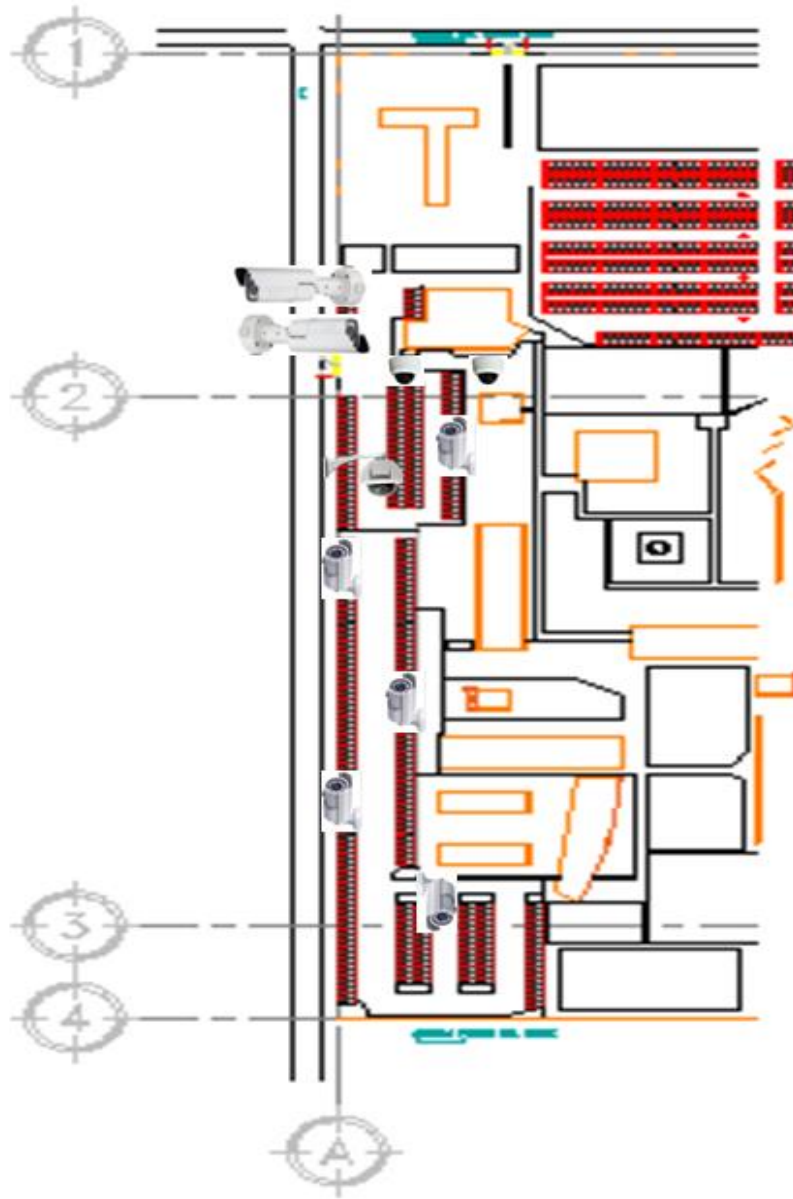
La cantidad y el tipo cámaras que se instalaran en esta zona son:

5 Tipo Bala – Para vigilar cajones del estacionamiento.

4 Tipo Bala HLC - Existen 2 plumas en la entrada y 2 en la salida vehicular, por lo tanto se instalara 1 cámara por cada pluma.

1 Tipo PTZ - Para reforzar la vigilancia en el estacionamiento y el pasillo que conecta directamente con el edificio de gobierno de la Facultad, teniendo la posibilidad de mover la cámara y hacer acercamientos.

5 Mini Domo – 2 cámaras para la entrada y salida peatonal y 3 cámaras para la zona de cajas.



Plano. 5.3.3 ZONA 2

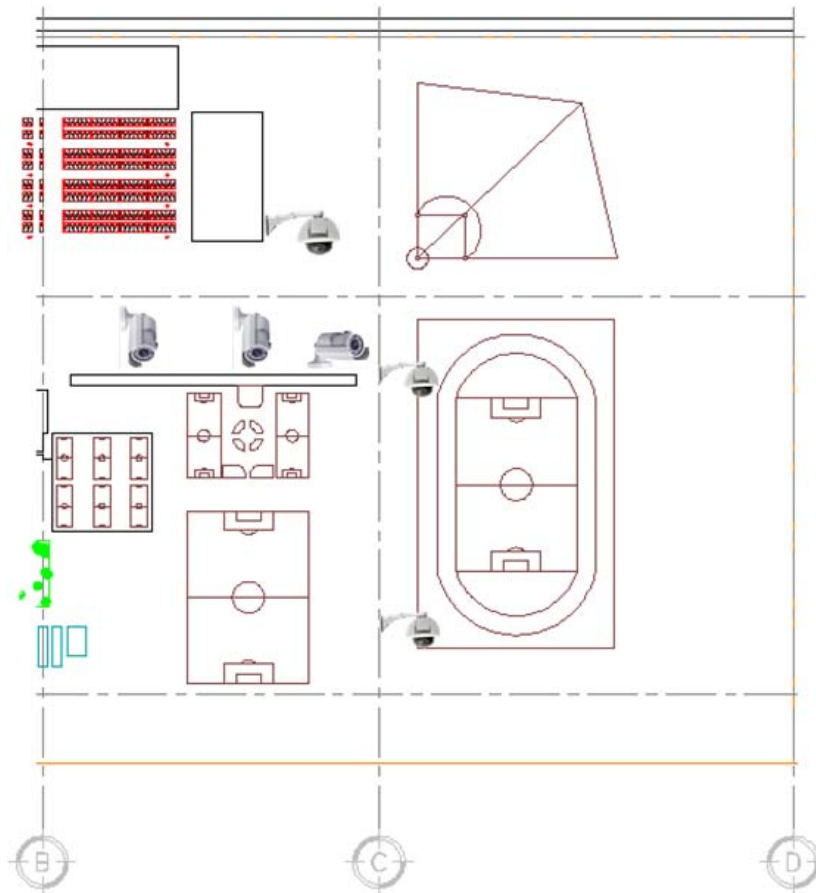
ZONA 3: Área deportiva

El Área deportiva está integrada por los campos deportivos de la Facultad, así como los espacios para jugar fútbol 7 y basquetbol. En el *Plano 5.3.4* se muestra la ubicación de cada cámara en esta zona.

La cantidad y el tipo cámaras que se instalarán en esta zona son:

3 Tipo Bala – 2 Para vigilar las canchas de basquetbol y de fútbol 7 y 1 cámara para vigilar el campo de fútbol soccer.

3 Tipo PTZ – Este tipo de cámaras son ideales para zonas abiertas, por lo tanto vigilarán los campos deportivos de la Facultad teniendo un gran campo de visión.

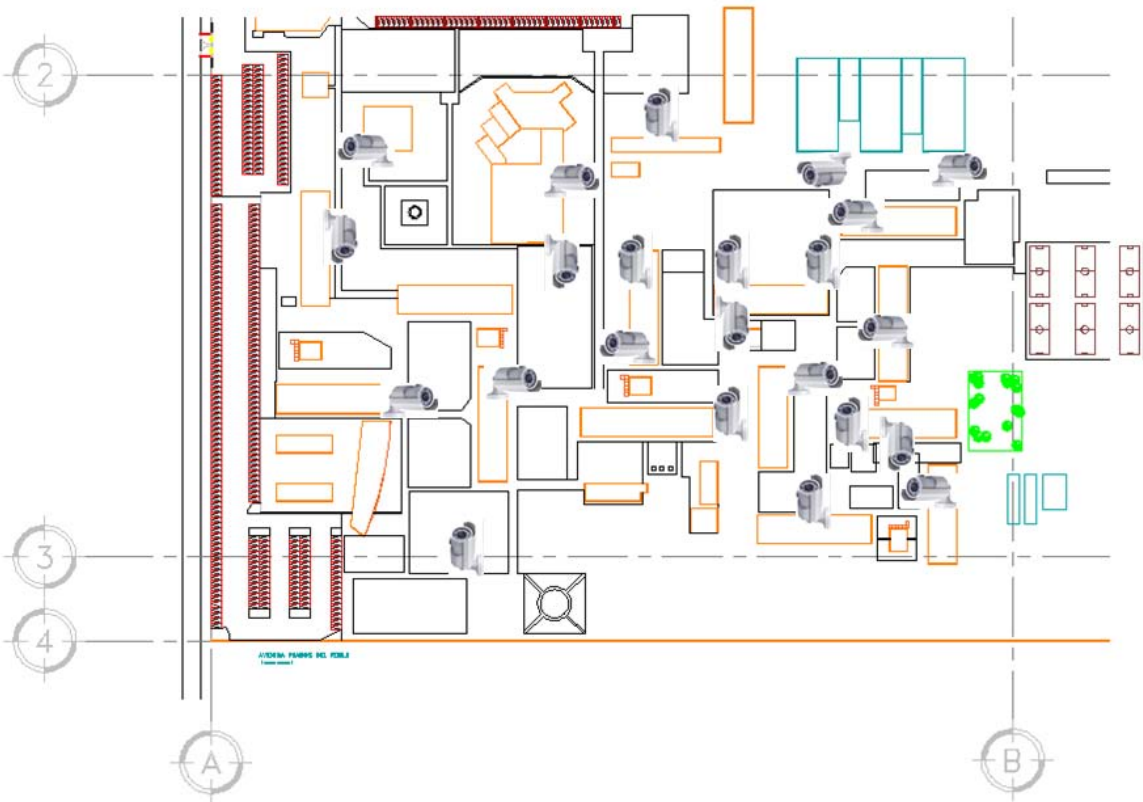


Plano 5.3.4 ZONA 3

ZONA 4: Edificios, Pasillos y Explanadas

La cantidad y el tipo cámaras que se instalarán en esta zona son:

23 Tipo Bala – Estas cámaras vigilarán los pasillos y las explanadas principales de la Facultad, nos proporcionarán imágenes del tráfico de los estudiantes en las rutas principales de la Facultad. En el *plano 5.3.5* se muestra la ubicación de cada cámara en esta zona.



Plano 5.3.5 ZONA 4

Finalmente el sistema de cámaras de video vigilancia para Facultad de Estudios Superiores Aragón contara con: 36 cámaras Tipo Bala ,6 PTZ ,9 Tipo Mini Domo, 16 Tipo Bala HLC, dando un total de 67 cámaras distribuidas dentro del campus universitario.

5.4 TIPO DE INSTALACIÓN

Existen diferentes tipos de instalación las cuales se pueden implementar en esta propuesta, en la *tabla 5.4.1* se observa las ventajas y desventajas de cada una de ellas, posteriormente se explica cuál es la más adecuada.

| TIPO DE INSTALACIÓN | VENTAJAS | DESVENTAJAS |
|---------------------|---|--|
| Inalámbrica | <ul style="list-style-type: none"> • Reducción de cableado. | <ul style="list-style-type: none"> • Interferencia. • Costo. |
| Aérea | <ul style="list-style-type: none"> • Interconexión segura. | <ul style="list-style-type: none"> • Mayor uso de materiales. • Costo. • Menor duración por estar expuesta a la intemperie. |
| Subterránea | <ul style="list-style-type: none"> • Interconexión segura. • Mayor durabilidad. | <ul style="list-style-type: none"> • Levantamiento de suelo. • Costo. |

Tabla 5.4.1 Ventajas y Desventajas de tipos de instalación

Se tiene en cuenta que es complejo y laborioso hacer un levantamiento de suelo, sin embargo; la instalación de tipo Subterránea es más adecuada debido a que se obtiene mayor duración, mayor seguridad y por lo tanto mayor fiabilidad.

5.4.1 CABLEADO

Se pueden utilizar tres tipos de cableado, los cuales se nombran en la *tabla 5.4.2* indicando sus ventajas y desventajas, así mismo se seleccionara cual es el más recomendable para usar en esta propuesta.

| TIPO DE CABLEADO | VENTAJAS | DESVENTAJAS |
|------------------|---|--|
| Par Trenzado | <ul style="list-style-type: none"> • Instalación sencilla • Tecnología bien estudiada | <ul style="list-style-type: none"> • Distancia • Durabilidad • Calidad de imagen |
| Coaxial | <ul style="list-style-type: none"> • Alta Velocidad • Distancia | <ul style="list-style-type: none"> • Costo • Grosor • Manipulación de cableado |
| Fibra Óptica | <ul style="list-style-type: none"> • Máxima calidad de imagen • Gran capacidad • Fiabilidad • Velocidad | <ul style="list-style-type: none"> • Costo • Instalación • Mantenimiento • Cambio de medio |

Tabla 5.4.2 Ventajas y Desventajas de Tipo de Cableado.

A pesar del costo elevado de la Fibra Óptica, es muy útil para este tipo de diseño, debido a la cantidad de datos que se van a generar con las 67 cámaras que se instalaran en la Facultad, obteniendo una excelente calidad de imagen y una velocidad mayor para la transmisión de datos. Además no existirá ningún problema al tener un crecimiento por el uso de más cámaras.

5.5 SISTEMA ELÉCTRICO

El sistema eléctrico es una parte importante en la instalación de las cámaras, primeramente para que éstas sean alimentadas y en segundo caso, para que siempre tengan energía eléctrica en dado caso de que no llegue a existir, debido a diversos factores que se pueden presentar. El sistema eléctrico consta de varias partes las cuales se describen a continuación.

1. **Compañía Local:** Se encarga de suministrar la energía principal para un área solicitada, en éste caso es la Facultad.
2. **Planta de emergencia:** Es una máquina la cual mueve un generador de electricidad mediante un motor de combustión interna. Su función es generar energía eléctrica.
3. **Switch de Transferencia (Transfer):** Se encarga de cambiar de una fuente de alimentación a otra ante la ausencia de una de ellas. Transfiere desde una fuente de alimentación principal, como es la compañía local a una fuente de alimentación secundaria, la cual es una planta de emergencia.
4. **Tablero de Emergencia:** Permite seleccionar un área determinada ante la ausencia de energía eléctrica, la cual es seleccionada por los encargados de la Facultad.
5. **UPS:** Es un sistema de alimentación ininterrumpida cuya función principal es la de proporcionar energía eléctrica ante la ausencia de ésta mediante un banco de baterías.
6. **Tablero de Distribución:** Se encarga de distribuir la energía eléctrica que es proporcionada por la planta de emergencia.

A continuación se muestra un diagrama a bloques, en el cual se aprecia de una mejor manera las partes que componen el sistema eléctrico. *Fig. 5.5.1.*

Diagrama del Sistema Eléctrico

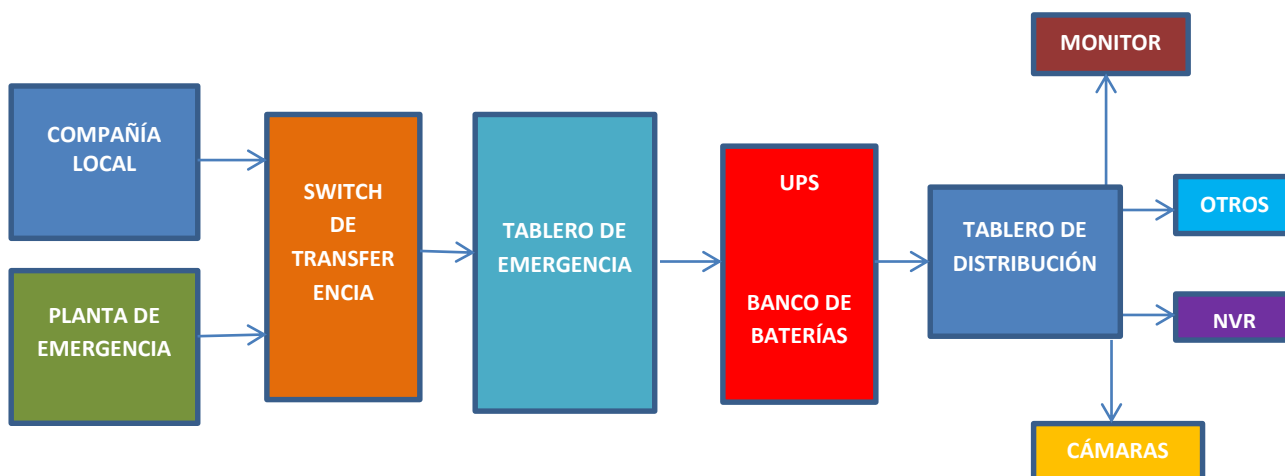


Fig. 5.5.1 Partes de un Sistema Eléctrico

Explicación del Sistema Eléctrico

La energía eléctrica es suministrada por la Compañía Local. Debido a que la zona donde está ubicada la Facultad de Estudios Superiores Aragón sufre de una irregularidad en el suministro de energía eléctrica, se requiere una fuente de alimentación alterna para cubrir la ausencia de la energía proporcionada por la Compañía Local, la cual se denomina como Planta de Emergencia.

Cuando la energía principal se ausenta, empieza a trabajar la Planta de Emergencia, éste cambio de fuente de alimentación de Compañía Local a Planta de Emergencia es realizado mediante el Switch de Transferencia. En el tablero de emergencia se encuentran las zonas seleccionadas para alimentar las principales necesidades eléctricas, como son: alumbrados, equipos de comunicaciones, cómputo, servidores, conmutadores, laboratorios y sistema de cámaras de vigilancia, etc.

Para que la Planta de Emergencia estabilice su voltaje y frecuencia es necesario esperar de 45 a 90 segundos y el tiempo mínimo requerido para evitar el apagado de algún equipo de cómputo es menor a 4 milisegundos, por lo que se requiere contar con un equipo que pueda conmutar debajo de éste tiempo, el equipo se denomina UPS, el cual actúa ante la ausencia de energía conmutando al banco de baterías y esperando a que la fuente de energía alterna se estabilice en frecuencia y voltaje para que así pueda conmutar tomando la energía alterna y suministrarla por medio del Tablero de Distribución a los equipos seleccionados.

5.6 SISTEMA DE CONEXIÓN DE CÁMARAS

El sistema de cámaras de video vigilancia IP que se pretende usar para monitorear las zonas de riesgo en la Facultad consta de los siguientes dispositivos:

1. **Cámara de Video vigilancia:** La cámara de video vigilancia se encarga de captar imágenes en una zona determinada. Existen una gran variedad de tipos de cámaras, depende de la necesidad que se requiera cubrir.
2. **Convertidor de Medios:** El Convertidor de Medios se encarga de transformar dos tipos de señales distintas para que tengan comunicación entre sí, por ejemplo, un medio de luz (Fibra Óptica) a un medio eléctrico (Ethernet) o viceversa.
3. **Switch:** La función básica del Switch es interconectar redes de dispositivos transmitiendo datos de un segmento a otro de acuerdo a la dirección IP, MAC o ambas que tengan como destino las tramas de esta estructura. Actualmente el Convertidor de Medios ya está integrado junto con el Switch.
4. **Access Point:** Se encarga de interconectar dispositivos de comunicación alámbrica con el fin de formar una red inalámbrica.
5. **Router:** Éste dispositivo se encarga de proporcionar conectividad a nivel red. La función principal del Router es enviar paquetes de datos de una red a otra.
6. **NVR:** Es un dispositivo que se encarga de almacenar las imágenes en forma digital en un disco duro, las cuales son capturadas por medio de las cámaras.
7. **Monitor:** Se encarga de ser un visualizador de imágenes, existen de diferentes resoluciones y tamaños.

A continuación se muestra un diagrama a bloques, en el cual se aprecia de una mejor manera las partes que componen el sistema de conexión de cámaras. *Fig. 5.6.1*

Diagrama del Sistema de Conexión de Cámaras

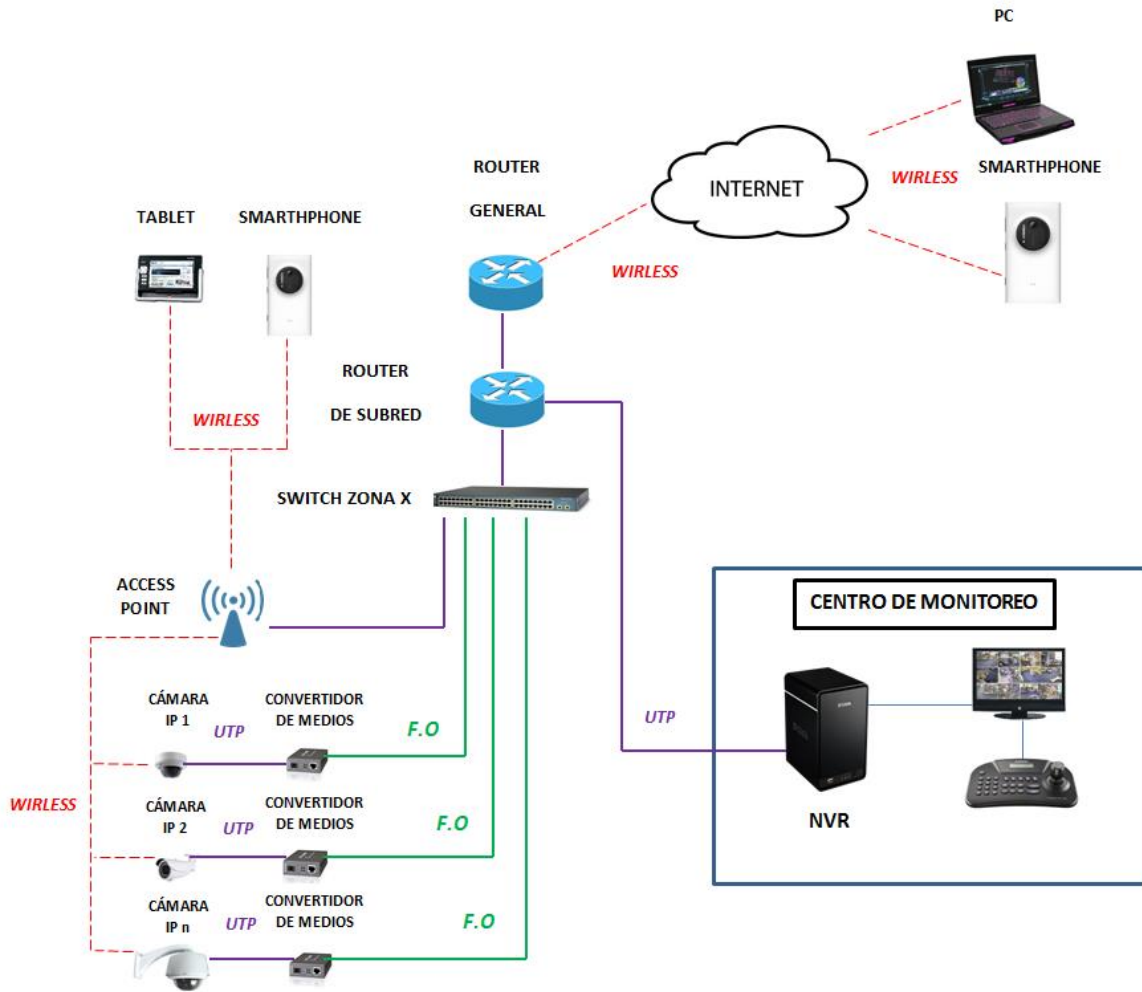


Fig. 5.6.1 Partes del Sistema de Conexión de Cámaras

Explicación del Sistema de Conexión de Cámaras

En la siguiente explicación del diagrama *Fig. 5.6.1*, se desarrolla como estarían conectadas las cámaras de una de las zonas de la Facultad, las demás zonas seguirían el mismo principio. Para que las imágenes captadas por las cámaras se visualicen en el Centro de Monitoreo, pero a su vez se puedan visualizar en cualquier parte de la Facultad y en cualquier parte del mundo, es necesario que la red este conformada de la siguiente manera.

Las cámaras de video vigilancia IP estarán conectadas a un Switch, el cual proporcionará la posibilidad de que los dispositivos estén conectados entre sí y éstos formen una red, sin embargo; para que las cámaras lleguen hasta el Switch, es necesario explicar el cableado que se utilizara.

Como ya se había mencionado antes, el principal medio de enlace es la Fibra Óptica, la cual en el diagrama está representada como F.O. Se usa éste tipo de cableado para cubrir la necesidad de la larga distancia para llegar a las cámaras y tener una buena calidad de imagen. Debido a que la F.O. es difícil de manipular en ángulos muy agudos, el cableado final para llegar a la cámara es de tipo UTP, por lo que se necesita un Convertidor de Medios para conectar la F.O. con el UTP.

En el mismo Switch estará conectado un Router, el cual proporcionará la conectividad a nivel y así mismo se monitoree el sistema de cámaras de video vigilancia vía remota. Por otra parte, al mismo Switch estará conectado un punto de acceso, en el diagrama se representa como Access Point, éste dispositivo proporcionara la señal de internet a las cámaras IP inalámbricamente, formando una red de área local (LAN). Al proporcionar internet inalámbricamente, es posible que otros dispositivos como Tablets, Smarthphones o Computadoras que estén cerca del Acces Point, puedan conectarse a la red local y de ésta manera tengan acceso a internet y la posibilidad de monitorear el sistema en cualquier parte de la Facultad.

Finalmente el NVR estará conectado al Router. Al NVR le llegará la señal de todas las cámaras de video vigilancia y gracias a los discos duros con los que cuenta, se almacenarán las imágenes para que en un futuro si llega a pasar algún suceso no deseado, se pueda revisar lo que haya pasado. Para que la Zona de la Facultad sea visualizada, es necesario contar con un monitor de alta resolución el cual reproducirá las imágenes captadas por las cámaras.

5.7 DIRECCIONAMIENTO Y CREACIÓN DE SUBREDES

A continuación se realizará el direccionamiento IP para cada cámara que se utiliza en el sistema de video vigilancia de la Facultad de Estudios Superiores Aragón, así como la creación de subredes. Una vez teniendo los datos anteriores se realizara el diagrama lógico del sistema IP.

Con la dirección de red 192.168.9.0 se debe de crear 4 subredes, estas subredes representaran las 4 zonas en las que se dividió la Facultad.

Datos:

SUBRED 1 / ZONA 1 = 23 Host (Cámaras)

SUBRED 2 / ZONA 2 = 15 Host (Cámaras)

SUBRED 3 / ZONA 3 = 6 Host (Cámaras)

SUBRED 4 / ZONA 4 = 23 Host (Cámaras)

Con los datos anteriores es posible realizar la creación de sub redes y el direccionamiento IP de las cámaras de video vigilancia. Para la resolución de este problema se ira llevando a cabo en pasos los cuales tendrán su explicación.

Paso 1.- Identificar qué tipo de clase de red se utilizara en el diseño del sistema.

Teniendo en cuenta que la dirección de red es 192.168.9.0 se puede determinar qué tipo de clase es. Se tiene que observar el primer número de la red y posteriormente revisar la tabla que se muestra a continuación (*Tabla 5.7.1*) y ver en qué rango está y así determinar qué clase es. Si el primer número de la dirección es 192, este entra dentro del rango de la Clase Tipo C.

| CLASE | RANGO DEL PRIMER NÚMERO DE LA DIRECCIÓN IP |
|---------|--|
| Clase A | 1 – 126 |
| Clase B | 128 – 191 |
| Clase C | 192 – 224 |

Tabla 5.7.1 Clases

Paso 2.- Máscara

La máscara de subred que se asigna por defecto debido a que se utilizara la Clase Tipo C es la:

255.255.255.0

Si ésta máscara se expresa en binario, se puede obtener los bits que ofrece para obtener el número de subredes y los bits que ofrece para obtener el número de host. En este caso da un total de 24 Bits de Red y 8 Bits de Host.

| | | | | |
|-----------|-------------------------------------|------|------|----------------|
| DIRECCIÓN | 192 | .168 | .9 | .0 |
| MÁSCARA | 255 | .255 | .255 | .0 |
| BINARIO | 11111111.11111111.11111111.00000000 | | | |
| | 24 bits de red | | | 8 bits de Host |

Paso 3.- Número de subredes

Se necesita obtener 4 subredes para cubrir las 4 zonas de la facultad, éstas se obtienen con la siguiente fórmula:

$$2^n \geq 4$$

n= Número de bits que se toma del ultimo octeto.

En este caso debe ser mayor o igual a 4 para cubrir el número de subredes que se necesita. Si se sustituye n = 3, se obtiene 8 subredes lo cual indica que es mayor a 4. Es necesario mencionar que del último octeto se ha utilizado 3 bits, por lo que queda de la siguiente manera:

| | | | | |
|--|-------------------------------------|--|--|----------------|
| | 11111111.11111111.11111111.11100000 | | | |
| | 24 bits de red | | | 8 bits de Host |

Debido a los 3 bits que se han utilizado para la creación de subredes, la máscara de subred queda:

255.255.255.224

Finalmente la dirección de las 8 subredes es la siguiente:

| COMBINACIÓN DE 3 BITS | OCTETO | DIRECCIÓN DE SUBRED |
|-----------------------|----------|---------------------|
| 000 | 00000000 | 192.168.9.0 |
| 001 | 00100000 | 192.168.9.32 |
| 010 | 01000000 | 192.168.9.64 |
| 011 | 01100000 | 192.168.9.96 |
| 100 | 10000000 | 192.168.9.128 |
| 101 | 10100000 | 192.168.9.160 |
| 110 | 11000000 | 192.168.9.192 |
| 111 | 11100000 | 192.168.9.224 |

Tabla 5.7.2 Subredes

Paso 4.- Número de host

Para calcular el número de host primero que nada se debe de tener en cuenta el número de host que se necesita en cada sub red. En la elaboración de éste diseño se piden: 23, 15, 6 y 23 host, por lo que es necesario tener más host disponibles de los que se piden.

Se utiliza la siguiente fórmula:

$2^n - 2 =$ Número de Host

n = número de ceros en el último octeto de la máscara

-2 = se anulan 2 host debido a que se utilizan para el direccionamiento de identificación de red y broadcast.

11111111.11111111.11111111.11100000

Si se tiene en cuenta que son 5 ceros del último octeto de la máscara de red y se sustituye n= 5, da un resultado de 30 host disponibles para cada subred, lo cual es suficiente para cubrir las necesidades de 23, 15, 6 y 23 host que se pide para cada subred.

Paso 5.- Cálculo de Subredes

En la siguiente tabla se encuentra la información de las subredes. Para el desarrollo de la propuesta del sistema de video vigilancia IP para FES Aragón, solamente se utilizan 4 subredes, sin embargo; existe la posibilidad que si en un futuro se llega a requerir de más cámaras de video vigilancia, hay la posibilidad de ocupar las otras subredes restantes.

La máscara es la misma para todas las redes, la dirección de broadcast no se usa por lo que se muestra el rango de direcciones que se pueden utilizar. Este rango abarca desde la primera dirección asignable hasta la última dirección, esto es por cada subred.

| SUBRED | DIRECCIÓN DE SUBRED | MÁSCARA DE SUBRED | BROADCAST | 1ª DIRECCIÓN ASIGNABLE | ÚLTIMA DIRECCIÓN ASIGNABLE |
|--------|---------------------|-------------------|---------------|------------------------|----------------------------|
| 1 | 192.168.9.0 | 255.255.255.224 | 192.168.9.31 | 192.168.9.1 | 192.168.9.30 |
| 2 | 192.168.9.32 | 255.255.255.224 | 192.168.9.63 | 192.168.9.33 | 192.168.9.62 |
| 3 | 192.168.9.64 | 255.255.255.224 | 192.168.9.95 | 192.168.9.65 | 192.168.9.94 |
| 4 | 192.168.9.96 | 255.255.255.224 | 192.168.9.127 | 192.168.9.97 | 192.168.9.126 |
| 5 | 192.168.9.128 | 255.255.255.224 | 192.168.9.159 | 192.168.9.129 | 192.168.9.158 |
| 6 | 192.168.9.160 | 255.255.255.224 | 192.168.9.191 | 192.168.9.161 | 192.168.9.190 |
| 7 | 192.168.9.192 | 255.255.255.224 | 192.168.9.223 | 192.168.9.193 | 192.168.9.222 |
| 8 | 192.168.9.224 | 255.255.255.224 | 192.168.9.255 | 192.168.9.225 | 192.168.9.254 |

Tabla 5.7.3 Subredes y direcciones, Máscara, Broadcast y direcciones útiles

5.8 DIAGRAMA LÓGICO

DIAGRAMA LÓGICO DEL SISTEMA DE VIDEO VIGILANCIA IP

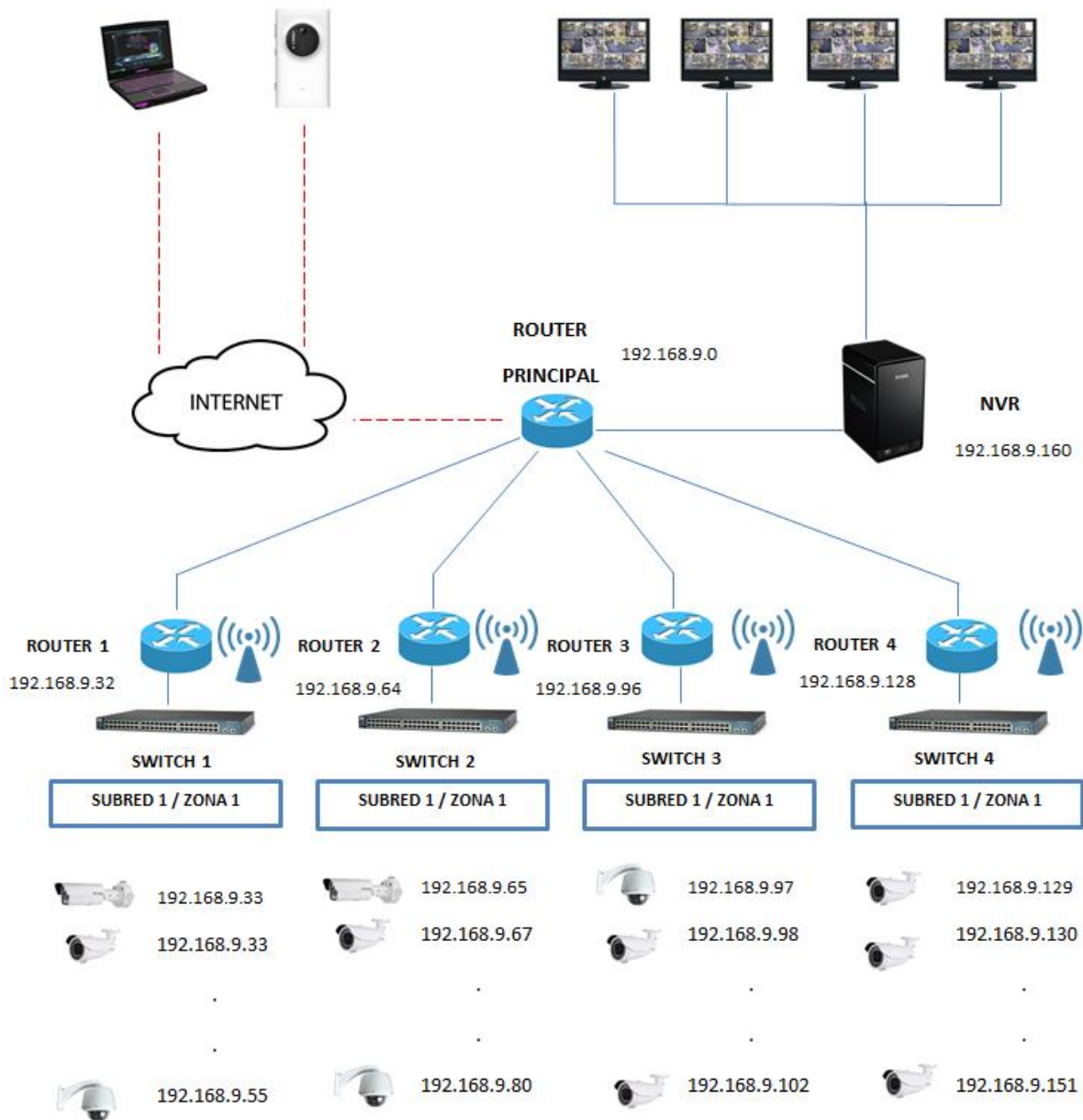


Fig. 5.8.1 Diagrama Lógico

Explicación del Diagrama Lógico

En el diagrama lógico (*Fig. 5.8.1*) se muestran las 4 zonas en las que se ha dividido la Facultad de Estudios Superiores Aragón, así mismo se utiliza 1 subred por cada zona, dando un total de 4 subredes, sin embargo; también el NVR utiliza una dirección de subred, dando un resultado final de 5 subredes a utilizar en el sistema de video vigilancia IP.

De cada subred se utiliza un rango de 30 direcciones IP las cuales se asignan a cada una de las cámaras de video vigilancia. Se dará el caso de que sobren varias direcciones IP, las direcciones que sobren tienen el propósito de que en el futuro estén disponibles si se llegara a necesitar un incremento en el número de cámaras.

Las cámaras de cada zona están conectadas a su respectivo Switch el cual está conectado al Router el cual tiene la dirección de subred. Los 4 Routers que se utilizan en las 4 zonas de la Facultad están conectados a un Router General el cual tiene la dirección IP principal del sistema, este Router está conectado al NVR el cual se encargará de almacenar los datos y juntar todas las señales de las cámaras para que de ésta manera se visualicen en los monitores.

Finalmente, si se quiere monitorear las cámaras de video vigilancia vía remota, existe la posibilidad de que se conecte directamente a internet y entrar por medio del Router General se visualicen las cámaras en cualquier parte del mundo.

CAPÍTULO VI

COSTOS DE

IMPLEMENTACIÓN

6.1 PRESUPUESTO POR ZONAS

Para calcular el presupuesto que se necesitará para llevar a cabo la instalación del Sistema de Video Vigilancia IP para la Facultad de Estudios Superiores Aragón, se ha dividido nuevamente la Facultad en 4 partes, tal como se realizó en el Capítulo 5 para la colocación de las cámaras, las cuales son:

- ZONA 1: Estacionamiento de alumnos
- ZONA 2: Estacionamiento profesores
- ZONA 3: Área deportiva
- ZONA 4: Edificios, Pasillos y Explanadas

En este capítulo se desarrolla una propuesta por zona y finalmente se hace la sumatoria de todas con el fin de obtener un presupuesto total del sistema de video vigilancia. Es importante aclarar que las cantidades son en dólares estadounidenses haciendo una conversión final a pesos mexicanos con un tipo de cambio de 13.5 pesos por un dólar.

Para tomar en cuenta la cotización del diseño de cámaras de video vigilancia se utilizaron diversas marcas. Para el cableado se consultó Fibremex (2014) y Condumex (2014); entre otros. Para el sistema de cámaras y el centro de control se consultó Hikvision catálogos y web (2014), Syscom catálogos y web (2014), entre otros.

6.1.1 DESARROLLO PRESUPUESTO ZONA 1

ZONA 1 Estacionamiento de Alumnos

| Estacionamiento | | | |
|-----------------------------------|-----------------------|--------------------|-----------------|
| Cantidad | Descripción | P. Unitario | Subtotal |
| 1 | Cámara PTZ | 2,179 | 2,179 |
| 2 | Cámara Bala | 449 | 898 |
| 3 | Adaptador | 10.2 | 30.6 |
| 3 | Convertidor de Medios | 110 | 330 |
| 300 | Cable UTP | 0.52 | 156 |
| 500 | Fibra Óptica 6 Hilos | 4.1 | 2,050 |
| 1 | Misceláneos | 215 | 215 |
| | | TOTAL | 5,858.6 |
| Estacionamiento | | | |
| Cantidad | Descripción | P. Unitario | Subtotal |
| 1 | Cámara PTZ | 2,179 | 2,179 |
| 3 | Cámara Bala | 449 | 1,347 |
| 4 | Adaptador | 10.2 | 40.8 |
| 4 | Convertidor de Medios | 110 | 440 |
| 770 | Cable UTP | 0.52 | 400.4 |
| 125 | Fibra Óptica 6 Hilos | 4.1 | 512.5 |
| 1 | Misceláneos | 245 | 245 |
| | | TOTAL | 5,164.7 |
| Entrada y Salida Vehicular | | | |
| Cantidad | Descripción | P. Unitario | Subtotal |
| 12 | Cámara Bala HLC | 449 | 5,388 |
| 12 | Adaptador | 10.2 | 122.4 |
| 12 | Convertidor de Medios | 110 | 1,320 |
| 1,200 | Cable UTP | 0.52 | 624 |
| 220 | Fibra Óptica 12 Hilos | 5.4 | 1,188 |
| 1 | Misceláneos | 860 | 860 |
| | | TOTAL | 9,502.4 |
| Entrada Peatonal | | | |
| Cantidad | Descripción | P. Unitario | Subtotal |
| 2 | Cámara Mini Domo | 556 | 1,112 |
| 2 | Adaptador | 10.2 | 20.4 |
| 2 | Convertidor de Medios | 110 | 220 |
| 200 | Cable UTP | 0.52 | 104 |
| 125 | Fibra Óptica 6 Hilos | 4.1 | 512.5 |
| 1 | Misceláneos | 195 | 195 |
| | | | 0 |
| | | TOTAL | 2163.9 |

| Salida Peatonal | | | |
|-----------------|-----------------------|--------------|----------------|
| Cantidad | Descripción | P. Unitario | Subtotal |
| 2 | Cámara Mini Domo | 556 | 1,112 |
| 2 | Adaptador | 10.2 | 20.4 |
| 2 | Convertidor de Medios | 110 | 220 |
| 200 | Cable UTP | 0.52 | 104 |
| 135 | Fibra Óptica 6 Hilos | 4.1 | 553.5 |
| 1 | Misceláneos | 195 | 195 |
| | | TOTAL | 2,204.9 |

Tipo de Cambio

| | | | |
|------|--|---------------------|-------------------|
| | Precio en Dólares antes de IVA | TOTAL ZONA 1 | 24,894.5 |
| 13.5 | Precio en Pesos Mexicanos con Tipo de Cambio | | 336,075.75 |

6.1.2 DESARROLLO PRESUPUESTO ZONA 2

Estacionamiento Profesores

ZONA 2

| Estacionamiento Profesores | | | |
|----------------------------|-----------------------|--------------|----------------|
| Cantidad | Descripción | P. Unitario | Subtotal |
| 1 | Cámara PTZ | 2,179 | 2,179 |
| 5 | Cámara Bala | 449 | 2,245 |
| 6 | Adaptador | 10.2 | 61.2 |
| 6 | Convertidor de Medios | 110 | 660 |
| 600 | Cable UTP | 0.52 | 312 |
| 600 | Fibra Óptica 12 Hilos | 5.4 | 3,240 |
| 1 | Misceláneos | 215 | 215 |
| | | TOTAL | 8,912.2 |
| Cajas | | | |
| Cantidad | Descripción | P. Unitario | Subtotal |
| 3 | Cámara Bala | 449 | 1,347 |
| 3 | Adaptador | 10.2 | 30.6 |
| 3 | Convertidor de Medios | 110 | 330 |
| 300 | Cable UTP | 0.52 | 156 |
| 300 | Fibra Óptica 6 Hilos | 4.1 | 1,230 |
| 1 | Misceláneos | 245 | 245 |
| | | TOTAL | 3,338.6 |

| Entrada y Salida Vehicular | | | |
|-----------------------------------|-----------------------|--------------------|-----------------|
| Cantidad | Descripción | P. Unitario | Subtotal |
| 4 | Cámara Bala HLC | 449 | 1,796 |
| 4 | Adaptador | 10.2 | 40.8 |
| 4 | Convertidor de Medios | 110 | 440 |
| 600 | Cable UTP | 0.52 | 312 |
| 500 | Fibra Óptica 12 Hilos | 5.4 | 2,700 |
| 1 | Misceláneos | 860 | 860 |
| | | TOTAL | 6,148.8 |
| Entrada Peatonal | | | |
| Cantidad | Descripción | P. Unitario | Subtotal |
| 1 | Cámara Mini Domo | 556 | 556 |
| 1 | Adaptador | 10.2 | 10.2 |
| 1 | Convertidor de Medios | 110 | 110 |
| 100 | Cable UTP | 0.52 | 52 |
| 380 | Fibra Óptica 6 Hilos | 4.1 | 1,558 |
| 1 | Misceláneos | 195 | 195 |
| | | | 0 |
| | | TOTAL | 2,481.2 |
| Salida Peatonal | | | |
| Cantidad | Descripción | P. Unitario | Subtotal |
| 1 | Cámara Mini Domo | 556 | 556 |
| 1 | Adaptador | 10.2 | 10.2 |
| 1 | Convertidor de Medios | 110 | 110 |
| 100 | Cable UTP | 0.52 | 52 |
| 380 | Fibra Óptica 6 Hilos | 4.1 | 1,558 |
| 1 | Misceláneos | 195 | 195 |
| | | TOTAL | 2,481.2 |

Tipo de Cambio

| | | | |
|------|--|---------------------|----------------|
| | Precio en Dólares antes de IVA | TOTAL ZONA 2 | 23,362 |
| 13.5 | Precio en Pesos Mexicanos con Tipo de Cambio | | 315,387 |

6.1.3 DESARROLLO PRESUPUESTO ZONA 3

ZONA 3

Área Deportiva

| Área Deportiva | | | |
|----------------|-----------------------|--------------|-----------------|
| Cantidad | Descripción | P. Unitario | Subtotal |
| 3 | Cámara PTZ | 2,179 | 6,537 |
| 3 | Cámara Bala | 449 | 1,347 |
| 6 | Adaptador | 10.2 | 61.2 |
| 6 | Convertidor de Medios | 110 | 660 |
| 600 | Cable UTP | 0.52 | 312 |
| 925 | Fibra Óptica 12 Hilos | 5.4 | 4,995 |
| 1 | Misceláneos | 215 | 215 |
| | | TOTAL | 14,127.2 |

Tipo de Cambio

| | | | |
|------|--|---------------------|------------------|
| | Precio en Dólares antes de IVA | TOTAL ZONA 3 | 14,127.2 |
| 13.5 | Precio en Pesos Mexicanos con Tipo de Cambio | | 190,717.2 |

6.1.4 DESARROLLO PRESUPUESTO ZONA 4

ZONA 4 Edificios, Pasillos y Explanadas

| Edificios, Pasillos y Explanadas | | | |
|----------------------------------|-----------------------|--------------|-----------------|
| Cantidad | Descripción | P. Unitario | Subtotal |
| 23 | Cámara Bala | 449 | 10,327 |
| 23 | Adaptador | 10.2 | 234.6 |
| 23 | Convertidor de Medios | 110 | 2,530 |
| 2,300 | Cable UTP | 0.52 | 1,196 |
| 625 | Fibra Óptica 12 Hilos | 5.4 | 3,375 |
| 490 | Fibra Óptica 12 Hilos | 5.4 | 2,646 |
| 860 | Fibra Óptica 12 Hilos | 5.4 | 4,644 |
| 780 | Fibra Óptica 12 Hilos | 5.4 | 4,212 |
| 920 | Fibra Óptica 12 Hilos | 5.4 | 4,968 |
| 1 | Misceláneos | 215 | 215 |
| | | TOTAL | 34,347.6 |

Tipo de Cambio

| | | | |
|------|--|---------------------|------------------|
| | Precio en Dólares antes de IVA | TOTAL ZONA 4 | 34,347.6 |
| 13.5 | Precio en Pesos Mexicanos con Tipo de Cambio | | 463,692.6 |

6.2 PRESUPUESTO CENTRO DE CONTROL

Centro de Control

| Centro de Control | | | |
|-------------------|-------------------|--------------|------------------|
| Cantidad | Descripción | P. Unitario | Subtotal |
| 4 | Switch 48 Puertos | 913.78 | 3,655.12 |
| 5 | Router | 392.19 | 1,960.95 |
| 4 | Access Point | 212.51 | 850.04 |
| 4 | NVR 48 Puertos | 4,129 | 1,6516 |
| 600 | Cable UTP | 0.52 | 312 |
| 4 | Pantalla | 1,115.2 | 4,460.8 |
| 8 | Disco Duro 4 TB | 329 | 2,632 |
| 4 | Misceláneos | 525 | 2,100 |
| | | TOTAL | 32,486.91 |

Tipo de Cambio

| | | | |
|------|--|--------------|--------------------|
| | Precio en Dólares antes de IVA | TOTAL | 32,486.91 |
| 13.5 | Precio en Pesos Mexicanos con Tipo de Cambio | | 438,573.285 |

6.3 PRESUPUESTO TOTAL

Finalmente al sumar los Totales de las 4 Zonas más el Centro de Control, se obtiene la siguiente cantidad:

| | | | |
|----------------|---------------------------------------|--------------|----------------------|
| Tipo de Cambio | Precio en Dólares antes de IVA | TOTAL | 129,218.41 |
| 13.5 Cambio | Precio en Pesos Mexicanos con Tipo de | | 1,744,448.535 |

En el presupuesto final se añade la mano de obra, la cual será de un más 30% del monto final del presupuesto

$$129,218.41 \times .30 = 387,65.523$$

A 129218.41 el cual es el costo total del material y equipo del sistema de video vigilancia se le suma el 30% de la mano de obra, por lo que da un presupuesto final de: **Dos millones doscientos sesenta y siete mil, setecientos ochenta y tres pesos con diez centavos.**

| | | | |
|----------------|--|--------------|----------------------|
| Tipo de Cambio | Precio en Dólares antes de IVA | TOTAL | 167,983.933 |
| 13.5 | Precio en Pesos Mexicanos con Tipo de Cambio | | 2,267,783.096 |

CAPÍTULO VII
CONCLUSIONES Y
RECOMENDACIONES

CONCLUSIÓN

El trabajo desarrollado en la presente Tesis, es un diseño de un sistema de video vigilancia IP para la Facultad de Estudios Superiores Aragón para aumentar la seguridad dentro del campus universitario y prevenir situaciones de vandalismo; reduciendo de igual forma el costo de la seguridad. Tras la realización de un análisis a la problemática con la cual cuenta la FES Aragón, se desarrolló una propuesta de ingeniería para proponer una solución al problema planteado. Con estas premisas, es posible concluir que:

- Se considera que el diseño del sistema de video vigilancia IP para la FES Aragón ayudara a aumentar la seguridad dentro de la Facultad y prevendrá situaciones de vandalismo, maltrato a las instalaciones y violencia. El diseño fue pensado para cubrir las zonas de riesgo, utilizando determinado tipo de cámaras dentro del campus según la zona a vigilar. Estas cámaras están conectadas a los equipos de almacenamiento masivo, los cuales están en el centro de control y de ésta manera los encargados de vigilancia pueden monitorear el campus. Por otra parte, el diseño del sistema está pensado para que tenga crecimiento en un futuro, por lo tanto se ha propuesto la implementación tanto de material adecuado como de equipo.
- Se logró diseñar un sistema de video vigilancia IP, el cual es capaz de ser monitoreado las 24 horas del día en cualquier época del año ya sea dentro de la Facultad o en cualquier parte del mundo en donde se tenga el servicio de internet. Esto trae un método de vigilancia más eficaz, más seguro y mucho más cómodo para las personas responsables de la seguridad en la FES Aragón, ya que no se tiene que estar desplazando dentro de la institución para vigilar las áreas.
- Así mismo, se identificó las zonas de alto, medio y bajo riesgo dentro de la Facultad, el tener estas zonas identificadas da la oportunidad de focalizar las principales áreas a cubrir dentro del campus y tenerlas en cuenta en el diseño del sistema de video vigilancia. También se obtuvo el horario y las temporadas en los que el sistema debe estar en funcionamiento.

- Al final de éste trabajo, se obtuvo un resultado satisfactorio de los estudiantes de la FES Aragón, debido a que la mayoría de ellos señalaron que la implementación de un sistema de video vigilancia dentro de la Institución traerá un cambio significativo para la seguridad y el buen uso de las instalaciones.

RECOMENDACIONES

- Es de suma importancia actualizar los planos eléctricos y unifilares de la instalación eléctrica de la Facultad, lo anterior para contar con la información real, de este modo cualquier tipo de sistema que se diseñe en un futuro y use la electricidad de la Facultad podrá contar con los datos reales y necesarios para su elaboración.
- Los componentes que integren al sistema de video vigilancia sean de alta calidad, de esta manera se podrá obtener mayor confianza y durabilidad.
- Los equipos que se usen para la grabación y el almacenamiento, así como el principal medio de transmisión que es la Fibra Óptica deben estar sobrados, esto pensado que en un futuro pueda crecer el sistema de video vigilancia.
- Capacitar a las personas que estén encargadas de la seguridad dentro de la Facultad, para que tengan el conocimiento de monitorear correctamente el sistema de video vigilancia ya sea dentro o fuera de la Facultad.
- La personas encargadas de la Seguridad de la Facultad deben tener contacto directo con la organización pública del municipio de Nezahualcóyotl que se encargue de atender las situaciones de peligro cuando estas se lleguen a presentar.

BIBLIOGRAFÍA

- Ariganello, E. (2011) *Redes CISCO, Guía de estudio para la certificación CCNA 640-802*. México: Alfaomega.
- Bartnikas, R. & Srivastava, K. (2000) *Power and Communications Cables. Theory and Applications*. NY: The Institute of Electrical and Electronics Engineers.
- Forouzan, B. (2003) *TCP/IP Protocol Suite*. NY: McGraw-Hill.
- Gómez, J. (2008) *Guía de campo de Wi-Fi*. México: Alfaomega.
- Grob, B. & Herndon, C. (2003) *Televisión Práctica y Sistemas de Video*. México: Alfaomega.
- Grob, B. (1975) *BASIC TELEVISION Principles and Servicing*. Tokyo: McGraw-Hill.
- Huidobro, J & Roldán, D. (2006) *Comunicaciones en redes*. México: Limusa Noriega Editores.
- Huidobro José (2004) *Manual de Telecomunicaciones*. México: Alfaomega.
- Jardón, H. & Linares, R. (1995) *Sistemas de Comunicaciones por Fibras Ópticas*. México: Alfaomega.
- Matthewson, D. (1983) *Video*. España: Alhambra.
- Merchan, J. (2012) *Diseño e Instalación de Sistemas de Videovigilancia CCTV Digitales*. España: Amv
- Molina, F. (2004) *Redes de Área Local*. México: Alfaomega
- Ramírez, J. (1990) *Generación de Señal de Video Teoría y Práctica*. México. Tesis de Licenciatura. Universidad Nacional Autónoma de México.
- Ramírez, M. (1979) *Diseño y Construcción de un Modulador de Video de Bajo Nivel*. México. Tesis de Licenciatura. Universidad Nacional Autónoma de México.
- Raya, J. & Raya, C. (1997) *Redes Locales y TCP/IP*. México: Alfaomega.
- Roldán, D., Millán R. & Huidobro J. (2006) *Tecnologías de Telecomunicaciones*. México: Alfaomega.
- Ruiz, F. (1991) *Televisión de Color*. España: PURESA.
- Syscom (2013) *Guía de Soluciones para Seguridad Electrónica*. Catalogo Syscom, Segura Inversión en Seguridad.
- Syscom (2014) *Guía de Soluciones para Seguridad Electrónica*. Catalogo Syscom, Segura Inversión en Seguridad.
- Van Norman, H. (1992) *LAN/WAN Optimization Techniques*. EUA: Artech House.

REFERENCIAS WEB

APC. Recuperado el 17 de Julio de 2014 de: <http://www.apc.com/site/products/index.cfm>

Aventura, Security Solutions by Design. Recuperado el 30 de Noviembre de 2013 de:
http://www.aventuracctv.com/es/dvr_tutorial/?index=1

CCTV y su Evolución. Recuperado el 13 de Septiembre de 2013 de:
<http://www.ordenadores-y-portatiles.com/camara-vigilancia.html>

Condumex. Recuperado el 7 de Mayo de 2014 de:
http://www.condumex.com.mx/ES/Paginas/Condumex_cables.aspx

Fernández, E. (19 de agosto de 2011) Los delincuentes nos acosan en la FES Aragón. Recuperado el 12 de marzo de 2014 de: <http://www.lapoliciaca.com/nota-roja/los-delincuentes-nos-acosan-en-la-fes-aragon/>

FES Aragón Historia. Recuperado el 8 de enero de 2014 de:
<http://www.aragon.unam.mx/unam/facultad/historia.html>

Fibremex. Recuperado el 17 de Mayo de 2014 de:
<http://fibremex.com/fibraoptica/index.php?mod=eCommerce&ext=group&id=26>

García, G. (2011) *3er Informe 2011-2012*. Recuperado el 5 de Junio de 2014 de:
http://www.aragon.unam.mx/nuestra_facultad/FES/Aragon/pdf/3ER_INFORME.pdf

Hikvision. Recuperado el 14 de Mayo de 2014 de: <http://www.hikvision.com/es/>

Mitsubishi Electric. Recuperado el 17 de Julio de 2014 de:
<http://www.meppi.com/Products/UninterruptiblePowerSupplies/Pages/default.aspx>

Méndez, E. (10 de febrero de 2013) *Alumnos de FES Asaltados sin parar*. Recuperado el 29 de Noviembre de 2013 de:
<http://www.eluniversaledomex.mx/nezahualcoyo/nota35693.html>

Pulido, N. (07 de febrero de 2013) *Aumentan asaltos a estudiantes de la FES Aragón en alrededores del metro Neza*. Recuperado el 29 de Noviembre de 2013 de:
http://www.periodicoafondo.com/main/index.php?option=com_content&view=article&id=2292:aumentan-asaltos-a-estudiantes-de-la-fes-aragon-en-alrededores-de-metro-neza&catid=1&Itemid=1

Pulido, N. (12 de marzo de 2013) *Aumentan asaltos a estudiantes y profesores de la FES Aragón*. Recuperado el 29 de Noviembre de 2013 de:
<http://www.hoyestado.com/nota.html?ver=9838>

Rojas, J. (30 de septiembre de 2008) *Electrónica y Redes*. Recuperado el 24 de marzo de 2014 de: <http://electronicayredesdelsena.blogspot.mx/2008/09/ups-definicion.html>

S.O.S. Seguridad. Recuperado el 2 de Junio de 2014 de: <http://www.seguridadsos.com.ar/>

Steve's DIGICAMS; The consumer's best source of digital camera information and news. Recuperado el 27 de Noviembre de 2013 de: <http://www.steves-digicams.com/knowledge-center/how-tos/digital-camera-operation/ccd-vs-cmos-whats-the-difference.html#b>

Syscom. Recuperado el 14 de Mayo de 2014 de: <http://www.syscom.mx/>

TELEDYNE DALSA. *CCD Vs CMOS*. Recuperado el 27 de Noviembre de 2013 de: <https://www.teledynedalsa.com/imaging/knowledge-center/appnotes/ccd-vs-cmos/>

TTCS. Técnicas en Cámaras y Seguridad. Recuperado el 8 de Junio de 2014 de: <http://www.ttcs.es/faqs/que-es-una-camara-ip.html>