UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

F A C U L T A D D E I N G E N I E R Í A

RED DE VIDEOVIGILANCIA IP PARA EL INSTITUTO DE INGENIERÍA

T E S I S

Para obtener el título de
INGENIERO EN COMPUTACIÓN

Que presenta:

JULIO GILBERTO DE LEÓN ZARAGOZA

Director de Tésis:

Ing. Marco Ámbriz Magüey

México, D.F. Enero, 2008

RECONOCIMIENTOS

A DIOS y su equipo de trabajo, que se que están ahí, observándome, cuidándome, acompañándome. Se que existen, espero estén orgullosos de mi.

A mi **equipo de trabajo** en la vida, nunca se han ido y estaré con ellos hasta el final: Ama, Apa y Manim.

A la *Facultad de Ingeniería* que me enseño absolutamente de todo y me preparó para la vida real.

Al *Instituto de Ingeniería* que invirtió en mi para lograr el objetivo.

A la gente que he encontrado en mi camino y hasta este momento siguen conmigo. A veces me dio la impresión que creen mas en mi de lo que uno mismo, por eso, no voy fallar: Chemoc, Rodrigo Torres, Carlos Villaseñor, Raymundo Arriaga, Roberto Rodríguez.

A Georgina y Javier y a mi nuevo hermanito José que me dieron la oportunidad de ser parte de sus vidas y me están dando la oportunidad de demostrarme de lo que soy capaz.

A mi director Marco Ámbriz por permitirme ser su grupo selecto y darme la confianza de que puedo hacer las cosas.

A mis maestros Luis Arellano y Pedro Osnaya que me dieron mi primera oportunidad.

A Araceli Martínez que me tendió la mano cuando la necesite y me quede con ganas de estar en su equipo de trabajo.

A mi estimado Robert que me apoyo en todo momento, realmente fue factor en esto.

A Bere, que en muy poco tiempo, entendí que realmente existen seres humanos espectaculares muy cerca de uno que hay que aprovechar porque hoy están, mañana no.

Al que me dio seguridad y apoyo, Andrés Benítez, porque cuando todo esto empezaba, el nunca se negó a acompañarme con los expertos en la materia.

A mis grandes compañeros desarrolladores, Jonathan y Genaro que siempre me daban ganas de platicar con ellos y a veces escuchaban atentos.

A Naye, Mauricio, Tocayo, Amalia, ICH, Cuauhtémoc, Ross, Alejandra, Tatiana, Carlos, Javier, Perla que me gustaba ir a distraerlos para salir de lo cotidiano y ayudaron de alguna manera en esto.

A mis compañeros más significativos de la carrera: Chiquis Triquis, Luis Franco, Joselo, Isaac, Olwin, Luis, Kuix, Oscar, que partieron y no se donde se encuentren en este momento pero quiero que sepan que esta aventura no hubiera sido lo mismo.

Y a una LUNA que me pidió continuar con mi vida, aquí estoy en pie de lucha, lo voy a lograr, te veo allá arriba, en lo más alto.

Estoy ansioso por saber que sucederá el día de mañana, estoy listo. Llego el momento de saber hasta dónde puedo llegar…

Hasta cualquier día.

INDICE TEMATICO

Introducción

El video digital es un elemento utilizado en diferentes ámbitos tales como: entretenimiento, videoconferencias, telemedicina, etc., debido a los beneficios obtenidos, ha extendido su campo de acción hacía aplicaciones anteriormente no consideradas como la videovigilancia. Por otro lado, la seguridad es una necesidad cada vez más requerida que ha ocasionado una búsqueda constante de alternativas tecnológicas (controles de acceso, control de activos, vigilancia en video, etc.) que permitan lograr espacios más seguros para la realización de actividades cotidianas. Las aplicaciones de seguridad basadas en video digital es un tema relativamente moderno que ha sobrepasado lo ofrecido por tecnologías analógicas y hoy en día se realizan fuertes inversiones en investigación para innovar soluciones que ofrezcan la seguridad deseada.

En la actualidad, la industria de la vigilancia dispone de una gran variedad de soluciones que basan su funcionamiento en sistemas digitales que proporcionan todo lo que el video analógico ofrece más otras posibilidades de interoperabilidad, escalabilidad y funcionalidad que sólo son posibles con tecnología digital.

Este trabajo tiene por sustento principal la búsqueda de una solución adecuada de videovigilancia acorde a las necesidades específicas del Instituto de Ingeniería; esto implica la comprensión de una gran diversidad de conceptos y prácticas que a una solución de videovigilancia involucra y las consideraciones más importantes para mantener su vigencia.

Este tema de tesis se compone de 8 capítulos que servirán como referencia en el desarrollo del sistema. Los primeros tres capítulos abarcan los conceptos básicos de generación, transmisión y almacenamiento de video digital, los capítulos posteriores tratarán aspectos de diseño, evaluación y puesta en marcha del sistema. Los tópicos abarcados en cada uno de ellos son los siguientes:

El Capítulo 1 desarrolla el tema de video digital y sus componentes. Aquí se mencionan términos que serán utilizados en capítulos posteriores que permitirán el entendimiento de las tecnologías de videovigilancia existentes hoy en día.

El Capítulo 2 proporciona información general acerca de los fundamentos de las redes de datos. Por ser un sistema basado en video digital, se vuelve importante el estudio de este medio de transmisión como una alternativa para el transporte del video.

En el Capítulo 3 se reconocen las posibilidades de resguardo para el video obtenido. Se identifican los beneficios e inconvenientes de las alternativas así como esquemas redundantes que garantizarán la integridad de la información.

El Capítulo 4 busca identificar los elementos existentes en el Instituto de Ingeniería tales como activos, personal e infraestructura. Esta sección permitirá entender la distribución e importancia de las funciones y actividades realizadas en cada uno de los edificios para establecer las directrices de diseño en la solución.

Como en cualquier sistema de seguridad, en el Capítulo 5 se realiza un análisis de seguridad general. Con base en el reconocimiento realizado en el capitulo anterior, se definen las zonas criticas para el Instituto de Ingeniería. Aquí comienza el planteamiento lógico del sistema de videovigilancia.

En el Capítulo 6 se examinan diferentes tecnologías de videovigilancia existentes en el mercado por parte de fabricantes reconocidos y dedicados a soluciones de seguridad en video. Así también, se definen las consideraciones implicadas en el tratamiento de video digital (transmisión y compresión) para soluciones profesionales.

En el Capítulo 7 se elige la opción tecnológica más viable a utilizar y se realiza el diseño de la solución que abarca la ubicación de los puntos de videovigilancia así como la estrategia de migración de sistemas analógicos a la nueva red de video IP.

Finalmente el Capítulo 8 contempla la puesta a punto del sistema. Se mencionan algunas consideraciones importantes en el proceso de instalación y mantenimiento de los equipos así como los costos implicados en el proyecto.

Además se incluye como material adicional una explicación general acerca de tres aspectos importantes en un sistema de esta naturaleza. Primeramente teoría de lentes que es el principio para la obtención de imágenes de calidad y fundamento para obtener el video esperado. En segundo lugar se menciona una técnica de compresión utilizada en los algoritmos más avanzados basados en transformación. DCT es una técnica de compresión interesante que vale la pena mencionar con más detalle. Finalmente se define el marco legal en el cual se sugiere se base el sistema de videovigilancia del Instituto de Ingeniería tomando como referencia algunas legislaciones existentes en otros países para este tipo de sistemas.

La información presentada a continuación está respaldada en un gran número de fuentes de información existentes en el mundo de la videovigilancia. Este trabajo de tesis busca ser un punto de convergencia de la gran diversidad de conceptos existentes en el ámbito e intenta ser una referencia para cualquier proyecto de videovigilancia sin importar su complejidad o dimensión.

Capítulo 1

Video Digital

Básicamente, un sistema de videovigilancia se compone de tres procesos: generación, transmisión y administración del video. La generación del video está a cargo de cámaras analógicas o digitales que ofrecerán las imágenes para ser transmitidas a través de medios físicos idóneos hacía lugares seguros y apartados para finalmente realizar una administración del contenido que implica monitoreo o almacenamiento de la información obtenida.

Para entender el funcionamiento de cualquier sistema de videovigilancia, es importante conocer sus fundamentos. La obtención y tratado de video digital es el tema inicial de análisis y base de estudio en este primer capítulo.

1.1 Conceptos Básicos

El video digital fue creado con la finalidad de manejar segmentos de video con mayor facilidad y que la calidad de imagen fuera lo mas acorde posible a los niveles de percepción que el sentido de la vista puede interpretar.

El video digital se basa en la transmisión de datos digitales conformados por secuencias de bits (unos y ceros) que tienen por objetivo representar información como texto, sonido e imágenes en datos digitalizados. Una de las ventajas directas de este tipo de tecnología es la posibilidad de manejar mayores *tasas de transmisión* por medio de la compresión y manejar encriptación de datos para su envío privado y seguro; los datos digitales son transportados a través de medios físicos de conducción tales como el cobre, fibras ópticas y ondas de radio por ello, la posibilidad de adecuar video digital a una red de datos es posible.

Un sistema digital tiene como fundamento la estructura de un sistema analógico. En la señal analógica la información se trasmite mediante "*una variación infinita de un parámetro continuo*" por lo tanto, en un sistema que lleva a cabo una grabación, las posibilidades de adquirir nuevos parámetros son latentes ya que cualquier forma de onda es aceptable siempre y cuando no se supere el ancho de banda permisible.

Por ejemplo, señales como el ruido, provocarían distorsión en la señal original siendo imposible diferenciar proporciones en las señales, entonces, un sistema analógico es incapaz de identificar distorsiones. Como la señal final será la adición de cada degradación adquirida durante la transportación, la señal analógica es limitada a no ser trasladada en trayectorias muy grandes porque habría una alta probabilidad de que la señal final esté completamente modificada. Por las desventajas que ofrece un sistema analógico se llevo a cabo la forma de digitalizar el video a partir de una señal analógica que se manipulara por medio de tres operaciones:

- Muestreo
- Cuantificación
- Codificación

1) **Muestreo.** Partiendo de una señal analógica continua cualquiera *x(t)* y un tren de pulsos *u(t),* se tomaran muestras de señal cada cierto intervalo de tiempo partiendo por comodidad de un t = 0[s]. El muestreo de una señal se puede obtener por medio del producto de la señal analógica con un tren de pulsos unitario, obteniendo como resultado una señal cuantificada solamente en ciertos intervalos de tiempo
(Ver Figura 1-1)

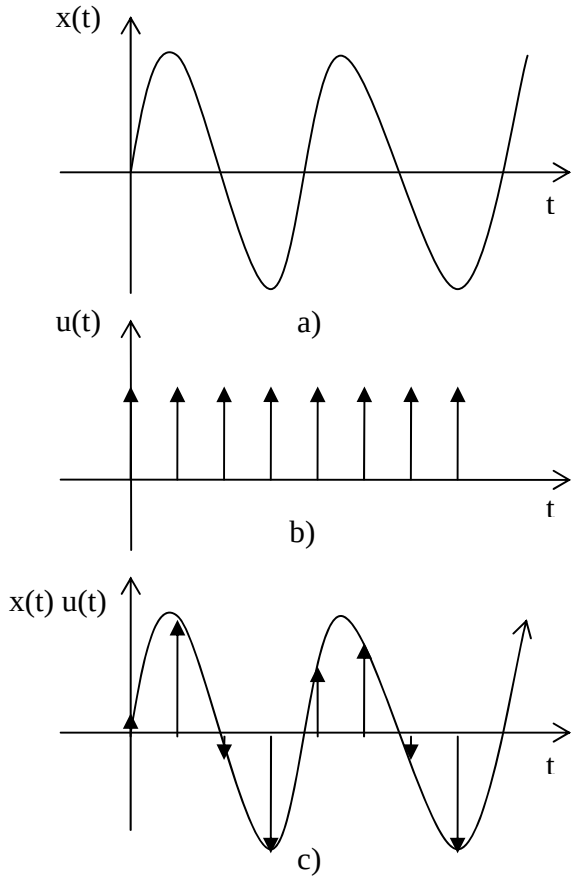


Figura 1-1. *(a) Señal analógica continua, (b) Señal tren de pulsos,*
(c) *Muestreo de una señal analógica.*

2) **Cuantificación.** El segundo paso a tratar en el proceso de análisis de una señal analógica es la cuantificación; se basa en la relación de muestras tomadas de la señal con un nivel asignado previamente, el valor obtenido será representado por medio de una cantidad binaria. Regularmente, la escala tomada es con base a potencias de dos, redondeando los valores de las muestras a un solo valor (superior o inferior) según el valor de la escala. Es importante hacer notar que al hacer una aproximación a cualquier escala, generara un error por cada muestra, la cual aparecerá en el proceso de decodificación digital – analógico. **(Ver Figura 1-2)**

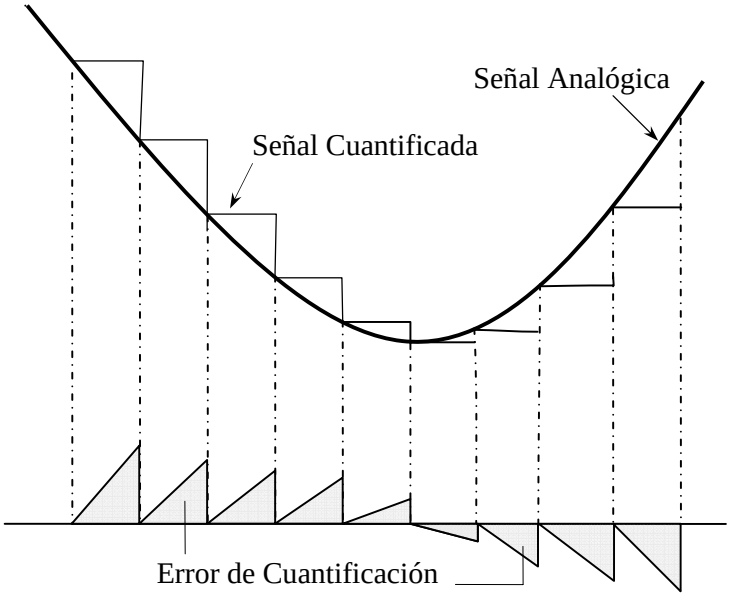


Figura 1-2. *Error de cuantificación.*

El error de cuantificación mencionado se identificara como ruido perceptible, este ruido depende directamente de la resolución de la escala utilizada, entre mas exacta sea la aproximación de las muestras al valor real de la señal analógica menor será el ruido generado en la decodificación.

3) **Codificación.** Es la acción o procedimiento de traducción de un mensaje en la forma más adecuada para entrar a un canal de comunicación o de transmisión**,** con la cual se busca alcanzar características específicas que garanticen la mejor capacidad de comunicación, aprovechando el ancho de banda existente, buscando la total integridad de datos y obviamente reducir lo más posible los costos.

   Una vez muestreada la señal, existe la forma de asignar valores binarios por medio de un nivel de voltaje el cual se considerará como un valor alto o bajo según otro nivel de referencia. Existen diferentes técnicas las cuales se mencionan a continuación:

   › **NRZ** *(Non Return to Zero)*. Este método consiste en asignar un '1' lógico al valor positivo de la señal digital y un '0' lógico al valor negativo.

   Algunas desventajas identificadas en este tipo de codificación es respecto al prolongado envío de ceros ya que el no envío de información está definido por un cero binario, por lo tanto el envío continuo de ceros provocaría una pérdida de la sincronización. **(Ver Figura 1-3)**

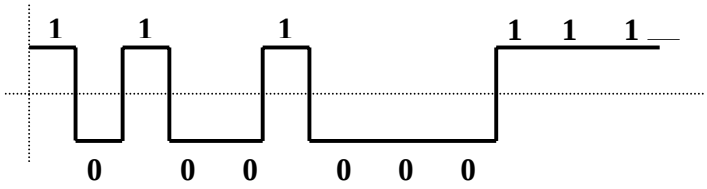


Figura 1-3. *Codificación Non Return to Zero.*

Existen otras versiones para la codificación NRZ:

- **NRZ –L** *(Non Return to Zero Level).* Este tipo de codificación es similar a NRZ, la polaridad de la señal cambia cuando se trasmite un uno lógico o un cero lógico. La idea general de este tipo de codificación es la de establecer niveles altos y bajos de voltaje que representen los unos y ceros de la señal digital.

- **NRZI** *(Non-Return-to-Zero-Inverted).* En está codificación la presencia de un cero lógico no causará un cambio en el nivel de la señal, sin embargo la presencia de un uno lógico, en la señal se producirá un cambio a un nivel alto o bajo dependiendo del estado actual de la señal de envío:

  Si el estado actual es cero, la señal cambiara a un uno lógico, si el estado actual es un uno, la señal cambiara a un cero lógico. **(Ver Figura 1-4)**

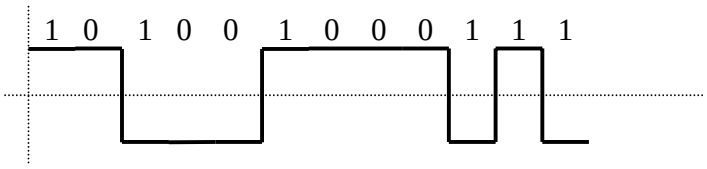


Figura 1-4. *Codificación Non Return to Zero Inverted*

Estos tipos de codificación tienen la ventaja de ser de sencilla implementación y utilizan un eficiente ancho de banda, son utilizados regularmente en grabaciones magnéticas.

› **AMI** *(Alternate Mark Inversion).* Está codificación se caracteriza por utilizar tres diferentes niveles de voltaje para representar la señal digital, Para un cero lógico, habrá un nivel bajo en la señal; Para un uno lógico se tendrá un pulso positivo y negativo en forma alterna.**(Ver Figura 1-5)**

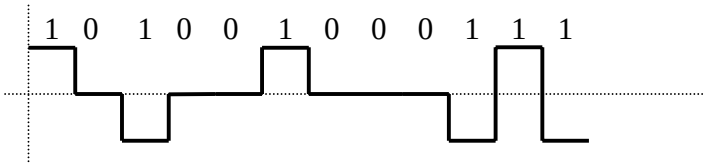


Figura 1-5. *Decodificación Alternate Mark Inversion (AMI).*

La transición que existe cuando se presenta un uno lógico, elimina la existencia de componentes continuas que causa la no pérdida de sincronización en envíos prolongados de unos, también la identificación de errores se facilita por la alternancia existente, sabiendo que en ausencia de alternancia, la información recibida no es correcta.

› **Manchester.** Tipo de codificación *bifásica*[1] donde la transición de la señal se lleva a cabo a la mitad del tamaño del bit. Si el bit de dato es un cero lógico entonces la transición es de alto a bajo voltaje, mientras que si es un uno lógico la transición es de bajo voltaje a alto. **(Ver Figura 1-6)**

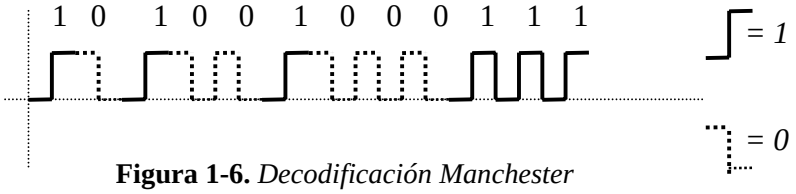


Figura 1-6. *Decodificación Manchester*

Por consecuencia la desventaja que existe en este tipo de señal es que el receptor cuenta con la mitad de tiempo para identificar el valor lógico, reduciéndose el *baudrate*[2] en un 50% de eficiencia.

› **Manchester Diferencial.** Este tipo de codificación es también bifásica y tiene una relación directa, basada bajo el mismo método que Manchester, el proceso es enviar para un bit de dato cero lógico existirá una transición de alto a bajo voltaje al principio y a la mitad del intervalo, para un bit de dato uno lógico la transición será de bajo a alto voltaje a la mitad del intervalo.

[1] Esquema de codificación que fuerza a una transición por cada bit existente en la señal.
[2] Medida de rango de señal el cual corresponde al número de datos enviados por segundo en una señal modulada.

La transición en la presencia de unos y ceros lógicos puede ser en ambos sentidos, de positivo a negativo ó de negativo a positivo dependiendo del estado actual en el que se encuentre el actual bit de envío. **(Ver Figura 1-7)**

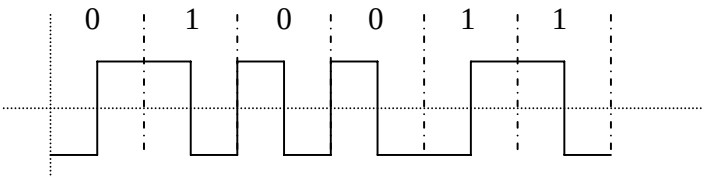


Figura 1-7. *Decodificación Manchester Diferencial.*

Los códigos bifásicos tienen un alto grado de identificación de errores por su inexistente componente de continua, logrando mejores alcances en la sincronización de la señales.

Existen otros tipos de codificación que se basan en cambiar los niveles de tensión constantes por otros valores que ofrezcan una anulación de la componente continua, la técnica utilizada es fijar un número máximo de valores lógicos iguales constantes, una vez establecido esto, se forzará a que el siguiente bit a enviar sea contrario a la secuencia antecesora logrando así romper dicha continuidad. [3]

La digitalización de una señal se lleva a cabo por medio de estas operaciones básicas que indicarán la forma en que la información debe ser transportada a través de la red de datos, cada técnica es definida por el protocolo y tecnología utilizadas.

1.2 Compresión y Codificación de Video

La compresión de video digital tiene la finalidad de reducir el volumen que ocupa cierta cantidad de información buscando evitar una saturación en los medios de comunicación por los que se va a trasmitir y así evitar grandes cantidades de almacenamiento en archivos grandes.

Es importante mencionar que una imagen contiene una gran cantidad de información continua, es decir, la posibilidad de compactarla no es tan sencilla como lo sería un documento de texto ya que este último contiene una gran cantidad de espacios que facilitan el proceso. El grado de compresión es una cantidad representativa de la calidad de la técnica utilizada y está definida por la relación de los datos comprimidos contra los no comprimidos.

Es necesario conocer algunos conceptos que giran en torno de lo que son las imágenes de video:

El brillo de una imagen es representado por los niveles de gris que contienen los *pixeles*[3] que conforman la imagen digital, está representación se puede cuantificar gráficamente por medio de un "histograma de brillo" que contiene en su eje horizontal el brillo representado por una escala de 8 bits (0 a 255) y en el eje vertical el número de píxeles; por lo tanto, el histograma facilitara la forma de identificar la concentración de píxeles contra el brillo de una imagen, y también, si una imagen es oscura o clara junto con su cantidad de contraste. **(Ver Figura 1-8)**

Tomando en cuenta lo anterior, el "contraste" se define como que intensa o desteñida aparece una imagen con respecto a tonos de gris base, para un alto contraste, los píxeles se ubicaran a los extremos de la escala y en un bajo contraste, los píxeles se encontraran concentrados. Ya que en el histograma de brillo están definidas escalas de gris entra un concepto de cuantificación llamado *rango dinámico*. Un rango dinámico es la cantidad de niveles de gris utilizados en la escala, un rango pequeño define pocos niveles de gris y por consiguiente baja resolución de brillo y contraste, a su vez, un rango alto implica una imagen balanceada en la distribución de los niveles de grises.

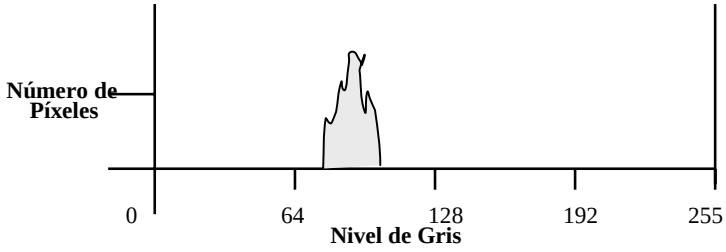


Figura 1-8. *Histograma de Brillo.*

A continuación se exponen algunas imágenes que ejemplifican como un histograma de brillo se ve alterado por características particulares:

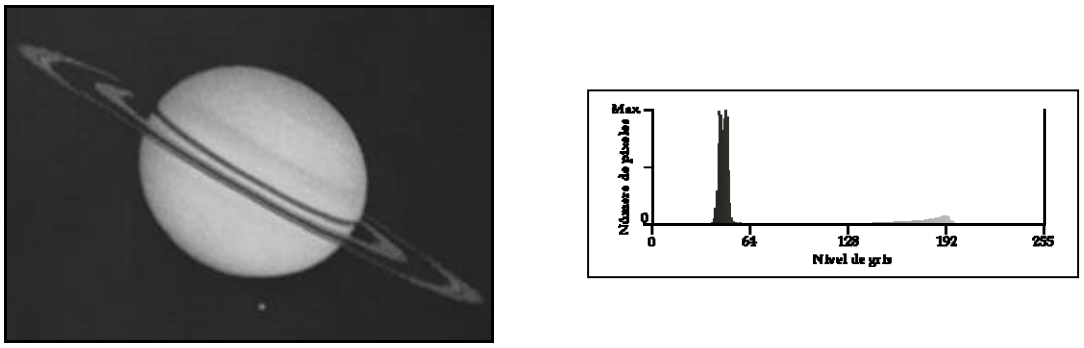


Figura 1-9. *Imagen Global Oscura*

[3] Mínima unidad en la que se puede descomponer una imagen digital, son pequeños cuadros de color ,blanco o negro que en conjunto forman una matriz rectangular base dimensional de la imagen

Como se aprecia en la **Figura 1-9**, una imagen oscura genera un histograma definido en una escala de grises concentrada en un extremo, esto implica una escasez de brillo y un contraste muy pobre, el histograma es una herramienta eficaz para interpretar la cantidad de píxeles acumulados en un área en específico.

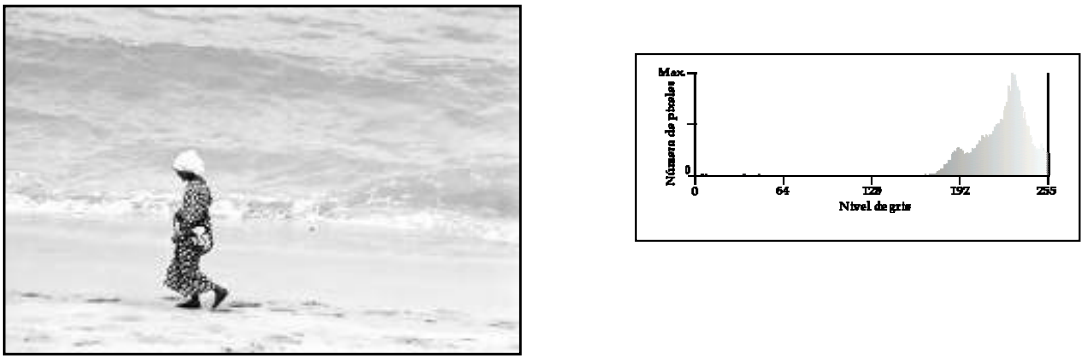


Figura 1-10. *Imagen Brillante*

En la **Figura 1-10** se muestra el caso contrario al anterior, los niveles de gris se encuentran ubicados al lado derecho del histograma, representando a una imagen sumamente clara que tiene un alto grado de brillantez.

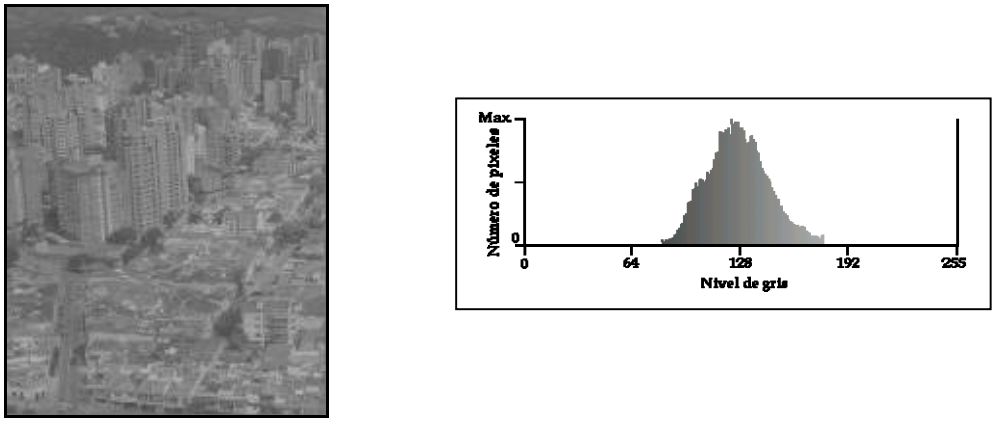


Figura 1-11. *Imagen con Bajo Rango Dinámico y Bajo Contraste*

Existe el caso en el que el rango de dinámico es muy estrecho, esto origina una reducida escala de grises que provoca una imagen con muy bajo contraste **(Figura 1-11)**

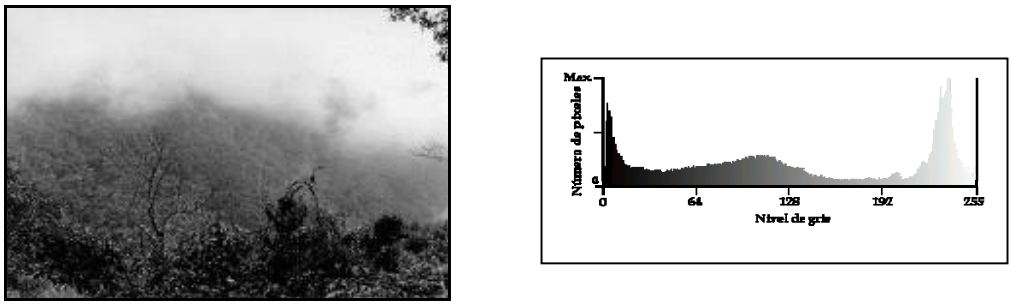


Figura 1-12. *Imagen de Alto Rango Dinámico y Alto Contraste*

A pesar de que el rango dinámico es considerable e indicador de una distribución adecuada, en la **Figura 1-12**, los picos en los extremos del histograma que superan el promedio de altura del resto de la grafica, originan una imagen con mucho contraste donde hay zonas con mucha oscuridad y pero a su vez con mucho brillo provocando una percepción nula de lo que acontece.

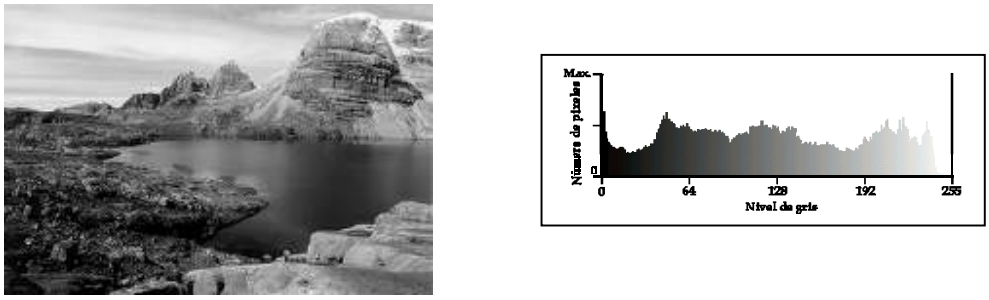


Figura 1-13. *Imagen con Alto Rango Dinámico y Balanceada*

La **Figura 1-13** es completamente adecuada para su certera percepción, su histograma de brillo así lo muestra, donde el rango dinámico se encuentra completamente distribuido, sin picos que deterioren la calidad de la imagen.

Como se pudo apreciar, una imagen tiene características precisas que garantizan su percepción, consideraciones a tomar en cuenta como contraste, brillo, rango de magnitud, son solamente algunos parámetros de suma importancia en el proceso de compresión de imágenes. Por lo tanto, para realizar el proceso de compresión, algunas características de redundancia en pixelaje e imágenes se pueden aprovechar:

- *Compresión por redundancia entre píxeles*. En ocasiones existen semejanzas entre píxeles, como mismo grado de brillo, contraste y color que pueden ser utilizados para predecir valores de pixeles adyacentes. Con base en este principio, algoritmos

de compresión como **Lempel-Ziv** contemplan esa característica para su funcionamiento.

- *Compresión por redundancia psicovisual.* El ojo tiene diferentes grados de sensibilidad que dependen de la información que recibe, pero en toda imagen existen elementos que no son contemplados por el sentido de la vista. Un ejemplo muy claro es recabar información de un objeto que repite el mismo estado una gran cantidad de tiempo, ese mismo estado generaría redundancia en el total de información a procesar.

En la **Figura 1-14** se muestra una imagen monocromática con 256 niveles de grises que definen un estado comprensible de la imagen:

Figura 1-14. *Imagen monocromática 256 niveles de gris**

Llevando a cabo una compresión a solamente 16 niveles de grises con una relación de compresión 2:1 **(Ver Figura 1-15)**, se obtuvo una imagen completamente distorsionada por la aparición de nuevos contornos que deterioran su percepción:

Figura 1-15. *Imagen de monocromática 16 niveles de gris.*

La alternativa de compresión por redundancia psicovisual proyecta una mejor sensibilidad con un mismo grado de compresión de la imagen *2:1*, la imagen no llegara a ser la misma ya que concretamente hablando se ha desechado una parte de la información pero su apreciación es significante**.(Ver Figura 1-16)**

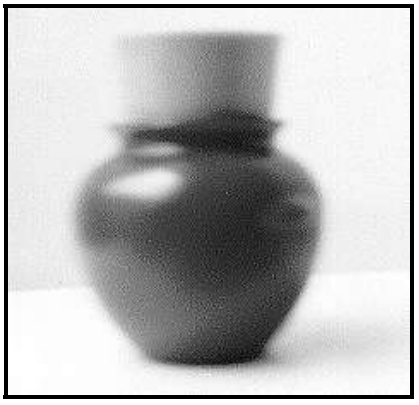


Figura 1-16. *Imagen monocromática a 16 niveles de gris sin redundancia***.**

> *Compresión con pérdidas.* Estas técnicas de compresión llegan a obtener la tasa de compresión más alta de todas, ya que aquí directamente se desechan datos para alcanzar una menor magnitud y por lo tanto una velocidad de bits inferior.

La posibilidad de reducir un archivo de tamaño siempre es factible pero, *¿Que tan benéfico es disminuir el tamaño de una imagen cuando entre más información se pierda más deteriorada terminará?*; algunos métodos que utilizan este tipo de algoritmos son: JPEG, compresión fractal, EZW, SPIHT, etc.

> *Compresión sin pérdidas.* Esta metodología mantiene el 100% de la información, la totalidad de los datos se almacenan solamente en un espacio más reducido. Estas técnicas son basadas en métodos estadísticos y en algunos tipos de codificaciones que se verán más adelante.

Se ha dado una visión general de lo que implica comprimir una imagen de video, sin embargo, la eficiencia de cada técnica de compresión se debe a los algoritmos de codificación utilizados que buscan encontrar de mejor manera las redundancias existentes y la eliminación de la información.

Las técnicas de codificación de imágenes pueden ser aplicadas perfectamente a la codificación de video ya que esta señal puede considerarse como una secuencia finita de imágenes.

La codificación simplemente consiste en definir un correspondiente entre cada uno de los símbolos en un alfabeto fuente y respecto a uno de los símbolos del alfabeto destino (*alfabeto código*); el alfabeto fuente contiene los símbolos originales que se desean

codificar y el alfabeto código contiene las *palabras*[4] en que se codificaran los símbolos originales, que a su vez serán trasmitidas a través de un canal de comunicación.

Las técnicas de codificación sin perdidas se mencionan a continuación:

- *Codificación de longitud finita*. En este tipo de codificación se le asigna un tamaño de la palabra específica a los símbolos que conforman el alfabeto, sin tener en cuenta las probabilidades con las que se presentan los símbolos. El código más usado para esta codificación es el código Gray donde las palabras de código consecutivas difieren en un solo bit, característica importante para la detección de errores. Las razones fundamentales por las cuales es elegible esta técnica por sobre el resto, cuando no se desean perdidas, es cuando *el numero de símbolos es igual a una potencia de dos y todos los símbolos tienen la misma probabilidad de suceder.*

- *Codificación de longitud variable.* La técnica utilizada para comprimir la información redundante es por medio de la asignación de palabras código a niveles de gris existentes. La variabilidad consiste en asignar palabras pequeñas a los niveles de gris más frecuentes y palabras grandes a las de menor repetición. El método mas frecuentemente utilizado es la codificación *Huffman* que a continuación se menciona.

  El método de Huffman se basa en el histograma de brillo de las imágenes, donde se convierten los valores de brillo en diferentes códigos dimensionalmente variables, los valores de brillo que se repiten un gran número de veces serán representados por palabras de dimensión pequeña y los valores no repetitivos con dimensiones mas grandes, para así describir una imagen integra comprimida con una cantidad reducida de bits.

  Un ejemplo muy representativo es cuando se desea enviar información acerca de un estudio en específico, donde se desea reducir al máximo el tiempo de transmisión, el número de veces que se presentan las frecuencias serán asignadas a un código Huffman **(Ver Tabla 1-1).**

Valor	Frecuencia %	Código Binario	Código Huffman
0	10	000	010
1	25	001	11
2	30	010	00
3	5	011	0111
4	**20**	**100**	**10**

Tabla 1-1. *Comparación codificación binaria y codificación Huffman.*

[4] Conjunto de "n" bits. Típicamente, 8, 16, 32 ó 64.

Como se puede observar, una codificación binaria natural generaría un gran número de bits a trasmitir al incrementarse el valor del dato, sin embargo, para la codificación de Huffman cada valor tiene un número diferente de bits, haciendo notar, que los números que con más frecuencia se presentan, contienen la menor cantidad posible de bits representativos a diferencia de las frecuencias menos frecuentes que se les asigna gran cantidad de bits.

Existe la forma de representar los datos y observar la eficiencia de la codificación de Huffman por encima de la codificación binaria.

Serie de valores a trasmitir:

2 4 0 2 2 4 0 3 2 1 4

Con base en la codificación binaria:

010 100 000 010 010 100 010 011 010 001 100

Con base en la codificación de Huffman:

00 10 010 00 00 10 010 0111 00 11 10

El número de bits utilizados para trasmitir 11 valores es de 33 para una codificación binaria normal y 26 valores para una codificación basada en codificación Huffman. La compresión de imágenes Huffman generalmente proporcionará razones de compresión de alrededor de 1.5:1 a 2:1.

- *Codificación aritmética.* Esta técnica codifica una secuencia de entrada de símbolos del alfabeto mediante un número de punto flotante. A cada símbolo componente de la palabra se le asigna un intervalo entre 0 y 1, de tal manera que la amplitud de cada intervalo esté basada en la probabilidad de cada símbolo. Es necesario definir el orden de envío de los símbolos para que en el proceso de decodificación se recupere el mismo orden.

  El proceso de codificación se lleva a cabo a través de los siguientes pasos:

  1. Seleccionar el primer símbolo de la secuencia de entrada y definir el intervalo asociado a este símbolo.
  2. Se localiza el siguiente símbolo y también se define su intervalo. Se multiplican los extremos del intervalo de este segundo símbolo con la longitud del intervalo del primer símbolo; el resultado se le suma a límite inferior y superior del

intervalo del primer símbolo para definir los nuevos límites del segundo símbolo y por consecuencia su amplitud.
3. El proceso se repite para todo el resto de los símbolos de la palabra; finalmente se obtendrá un intervalo final del que se escogerá un valor representativo dentro del intervalo que represente a todos los símbolos.

Este tipo de codificación no está exenta de fallas, por un lado, la precisión numérica o el número de decimales que hacen falta aumenta con la cantidad de símbolos del alfabeto fuente y el otro problema se presenta cuando los extremos del intervalo están muy cercanos pudiéndose producir errores en la fase de decodificación.

· *Codificación de Shannon-Fano.* Esta técnica es muy sencilla de implementar y es formada con base en la probabilidad de aparición de los símbolos a utilizar.

1. Primeramente se adecuan los símbolos a trasmitir en orden ascendente y se les asigna un valor de probabilidad a cada uno de ellos.
2. A continuación la cantidad total de símbolos se dividirán en dos subconjuntos los cuales estarán formados con base en la probabilidad de cada símbolo, la suma de cada uno de los subconjuntos, debe ser aproximadamente igual entre ellos.
3. A los símbolos del primer conjunto se les asignará un 1, y a los símbolos del segundo subconjunto se les asignará un 0 lógico.
4. Repetidamente se hará el mismo para cada subconjunto nuevo generado, hasta obtener un código binario para cada símbolo.

En este tipo de codificación se alcanzan eficiencias muy altas ya que en cuanto más probabilidad exista del símbolo una menor cantidad de bits son enviados, característica táctica de otros métodos de codificación ya antes mencionados.

Existen otras técnicas de codificación basadas en pérdidas de algunas características de las imágenes que en definitiva no podrán ser apreciadas por un ojo humano. La idea general es trasformar la imagen original en otra equivalente y en esta eliminar cualidades no muy significativas.

Es importante mencionar que hablando de capacidad de compresión directamente, estas técnicas alcanzan un alto grado que las convierte en las eficientes, los datos son reducidos a un factor de compresión de 10:1 con degradaciones no notables y 100:1 con degradaciones sumamente notables.

A continuación se muestran las técnicas más usadas por métodos de compresión con perdidas.

· *Codificación por Truncamiento.* Técnica por medio de la cual se eliminan datos en ámbitos de *muestreo espacial* [5] y resolución de brillo.

[5] Los píxeles próximos dentro de una imagen tienden a parecerse.

En la reducción espacial se eliminarán una cantidad de píxeles determinados consecutivamente (uno si y uno no) el tamaño de la imagen será reducido a un tamaño considerable. Al momento de descomprimir la imagen se puede reconstruir a un tamaño reducido que permitiría que las degradaciones no fueran apreciadas por el espectador o también reconstruir la imagen recuperando los píxeles eliminados por medio de una interpolación de estos, logrando así su tamaño original, donde naturalmente las probabilidades de error en la imagen se verían reflejadas.

Por medio de la resolución de brillo, se truncan todos los valores de brillo de los píxeles, ocasionando así una representación de datos compuestos por menos cantidades de bits. Tomando como base un píxel definido por 8 bits, se puede truncar la brillantez del bit a 3 solamente, logrando un factor de compresión de 2.66. Al descomprimir la imagen se puede obtener una calidad de brillo reducida cuando no importan detalles en la imagen ya que regularmente se genera un efecto denominado como *posterizing*[6] que denigra la calidad de imagen, otra alternativa es compensar de alguna manera ese truncamiento realizado por medio de un patrón de ruido de la misma magnitud denominado *dither noise*[7], con esto se logra la eliminación del efecto de posterizing y la calidad de imagen se acrecienta considerablemente.

- *Codificación Predicativa.* Este tipo de codificación alcanza grandes niveles de compresión (3:1 o mayores), la base fundamental es determinar el brillo de cualquier píxel a partir del brillo de su píxel previo, con esto reducimos los tiempos de codificación que solamente están sujetos a la diferencia de información de los píxeles.

  La modulación por diferencias de pulsos (*PDCM*) es la metodología base de este tipo de codificación. Teniendo una imagen común donde cada píxel está definido por 8 bits representativos de brillo, se determina el valor de brillo del primer píxel, a continuación se determina el valor de brillo de su píxel adyacente, se realiza la sustracción de brillos dando por resultado el valor a codificar para el segundo píxel; este proceso es continuo para cada uno de los píxeles logrando tanto un numero menor de valores codificados como cantidades que pueden ser representadas con un número menor de bits.

  Un ejemplo representativo de este método se muestra a continuación:

  Supongamos que se tienen 5 píxeles, cada uno con 8 bits representativos de brillo, se determinan sus valores de brillo de cada uno y se hace la sustracción correspondiente entre píxeles adyacentes:

[6] Efecto de gradación de tonos que son reducidos a un número sólido de colores. Por ejemplo en lugar de una transición delicada de gris a negro, esta es realizada con base en cuatro colores básicos, blanco, negro y algunos cuantos grados de gris.

[7] Señal anexada a una señal base por medio de ruido con la finalidad de reducir distorsión de una señal.

Píxel	*8b/ pix.*	*Val. PDCM*
P_1	33	33
P_2	55	22
P_3	29	-26
P_4	39	10
P_5	68	29
	$(8_b)(5) = 40_b$	$(6_b)(5) = 30_b$

Como se puede observar, los valores obtenidos por la modulación de diferencia de pulsos pueden ser definidos digitalmente únicamente por 6 bits, por tanto se tiene un numero de bits totales mucho más reducido.

Ya que esta técnica se basa en la suposición de que píxeles continuos tienen un valor de brillo similar, los resultados obtenidos no salen de la capacidad de 6 bits, pero puede presentarse el caso de que algún pixel presente un brillo considerable (realmente improbable) y genere un desbordamiento en la sustracción, en este caso, se usa el código mayor posible para los píxeles siguientes hasta que el codificador alcanza el valor real de brillo de la imagen original, por consecuencia cuando se descomprime esta imagen habrá manchas donde existieran transiciones bruscas de brillo.

- *Codificación por Bloques*. Este método se basa en analizar un bloque de píxeles (*disposición bidimensional de píxeles*) como un entero en el cual se buscan patrones repetidos.

Para esta codificación se toma como referencia una tabla de diferentes patrones de brillo de los píxeles también llamado *libro de códigos;* haciendo un análisis de cada pixel se buscan patrones de brillo que se aproximen con los patrones definidos en el libro. El libro empieza con información base (*256 entradas*) para una imagen de 8 bits, cada una representa un patrón simple de brillo para un pixel; conforme aumenta el proceso de comparación va aumentado la información del libro, cuando se completa la codificación se adjunta el libro para su posterior decodificación.

Naturalmente al hablar de aproximación habrá que tomar en cuenta la inevitable existencia de error que puede ser controlada de acuerdo con el uso que se pretende hacer con la imagen, que dependiendo si va a ser utilizada para observar detalles con el ojo humano podría controlarse el error de distorsión de imagen. El proceso de descompresión es exactamente el mismo basándose en los patrones del libro para retornar a valores originales.

Los niveles de compresión alcanzados son de 3:1 y 2:1, esta técnica tiene la desventaja de utilizar más recursos computacionales con respecto a las técnicas mencionadas con anterioridad.

- *Codificación por Transformación.* Este tipo de codificación se basa en la codificación por bloque mencionado anteriormente, diferenciándose en la no utilización de libros para la codificación de los bloques de píxeles.

  Lo que se denomina como una trasformación es simplemente representar una imagen en el dominio de la frecuencia. Para este caso, los elementos que serán la base del mapeo serán los valores de brillo de los píxeles, que regularmente serán agrupados en el nuevo dominio, en sus zonas de baja frecuencia. Cuando existe mucha redundancia en imágenes, las frecuencias se repiten y en el proceso transformación se pierden por tener valores muy pequeños. En este tipo de codificación los bloques de píxeles que se manejan son pequeños 4x4 u 8x8 píxeles, los componentes fundamentales de la frecuencia son evaluados, desechando aquellos valores de frecuencia de baja magnitud, los valores sobrantes será la información que conformará la imagen comprimida.

  Existen trasformadas de frecuencia que respaldan formatos de video, la calidad de una trasformada se mide con base en la cantidad de componentes obtenidas siendo más eficiente aquella que consiga menos número ya que será menor cantidad de información a enviar.

  Una herramienta muy útil es la *Trasformada Discreta de Coseno* (DCT) utilizada como estándar en los sistemas de codificación por trasformación, el DCT comprime la mayor parte de la información en el menor número de coeficientes que son obtenidos con base a trasformaciones bidimensionales de cada imagen.

Se ha dado una visión de lo que implica el proceso de compresión y codificación de imágenes en general, una vez comprendidas algunas de las técnicas más utilizadas, es tiempo de hablar acerca de cómo se clasifican los estándares de compresión de video, conocidos como formatos.

1.3 Formatos de Video Digital

El manejar un sistema de videovigilancia es un proceso realmente demandante en recursos para cualquier red de datos y más aun cuando no se tienen los recursos adecuados para llevarlo a cabo, factores como ancho de banda, tipo de imágenes y el formato de compresión utilizado son determinantes para lograr la eficiencia de un sistema.

Normalmente cuando se desea llevar a cabo una transmisión de una señal de video los recursos necesarios son bastantes (*Estándar CCIR 601 → 165 Mbps*); como estas capacidades (en una red que no es exclusiva para envío de video) no son alcanzables, la necesidad de realizar esta función debe lograrse por medio de reducir de alguna manera esa inmensa cantidad de datos, por tanto se ha buscado encontrar formatos de video digital que se basan en métodos de codificación diversos, con los cuales se ha alcanzado

una gran eficacia en el manejo de información de gran diversidad a través de un mismo medio. A continuación se mencionan sólo algunos ejemplos:

· **JPEG** (*Joint Photographic Experts Group***)**

Es el estándar más utilizado en la actualidad ya que puede operar con imágenes a color o blanco y negro (permite utilizar hasta 16, 777,216 colores definidos por 24 bits), este formato existe con pérdidas o sin pérdidas donde el rendimiento de compresión es mucho menor para el segundo.

La tecnología utilizada en este estándar es el conjunto de varias técnicas que actúan consecutivamente para imágenes estáticas. Hablando del formato con perdidas, el primer paso es cambiar la imagen al dominio de la frecuencia por medio de la codificación por transformada donde se logra que los componentes con menor frecuencia sean eliminados, el resto de los componentes (con mayor cantidad de frecuencia) se codifican por medio de DPCM y después por el método de codificación de Huffman. Para el estándar JPEG sin perdidas solamente se utilizan codificación DPCM y Huffman en conjunto.

El formato JPEG tiene muchas variantes, ya que se pueden fijar los requerimientos de la imagen, como la cantidad de elementos retenidos por la codificación de transformada para buscar diferentes tasas de compresión logrando así, diferentes niveles de calidad según sea el caso.

· **MPEG**. (*Moving Picture Experts Group***).**

Este estándar fue en conjunto definido por *ISO/IEC y CCITT*[8] donde se buscaba comprimir archivos de imágenes en movimiento con base en estándares ya existentes como *H.261* que se utiliza principalmente para videoconferencia alcanzando velocidades de transmisión de *2 Mbits/s;* H.261 se puede ver como versión simplificada de la compresión de video MPEG

Existen diferentes clasificaciones para MPEG las cuales se mencionan a continuación

La compresión de la técnica ***MPEG -1*** se basa en el método de trasformada a través de DCT que como ya se mencionó se busca reducir las secuencias repetitivas por medio de la estimación de movimientos para secuencias de video.

Tomándose como base una secuencia de 4 imágenes, se puede comprender como es interpretada la secuencia por *MPEG -1*. **(Ver Figura 1-17)**

[8](*International Organization for Standardization*) /(*International Electrotechnical Commission*) y (*International Telegraph and Telephone Consultative Committee)*

Figura 1-17. *Secuencia de 4 imágenes individuales*
(Fuente: http://www.chiariglione.org/mpeg/standards/mpeg-4/mpeg-4.htm)

La frecuencia de la izquierda es la primera imagen de la secuencia, JPEG analizaría a cada imagen individualmente de tal manera que lograría una secuencia como la original.

MPEG-1 analiza la secuencia de las imágenes comprobando la redundancia entre estas, es decir, el ambiente que existe detrás de la figura principal no tendría caso que se codificara 4 veces, una sola ocasión pueden ser procesados estos datos y comprimidos para su envío, para obtener un ancho de banda más reducido. MPEG-1 se basa en componer *streams* de bits de aproximadamente 1.5Mbps y una resolución de 352 x 240 pixeles.

La compresión de la técnica ***MPEG-2*** se llevó a cabo ya que se buscó mejorar las capacidades que ofrece MPEG–1, la posibilidad de manejo de imágenes a mayor escala con base en menor grado de compresión no se hizo esperar. Si se desea manejar una tasa de transferencia más grande entonces la compresión tendrá que disminuir; entonces para una tasa más alta habrá menor compresión y un tamaño más grande a manejar pero la calidad de video será mejor.

El manejo de las imágenes es similar que en MPEG-1 ya que se utiliza la codificación de transformada a través de DCT así como codificación por Huffman. Ya que el nivel de compresión de este formato es mucho más bajo, es necesaria la utilización de mayor ancho de banda, la resolución obtenida puede alcanzar magnitudes de *720 x 486* píxeles a un nivel de calidad de televisión. Otras características que lo hacen superior a su antecesor es la posibilidad de codificar imágenes de TV de alta definición y manejar mayores componentes de color que MPEG-1. Actualmente es utilizado en DVDs y en SVCD

De las últimas técnicas de compresión creadas por Moving Picture Experts Group es ***MPEG-4*** *(ISO / 14496)* para el cual se buscó abarcar una mayor cantidad de aplicaciones junto con un menor consumo de ancho de banda. Aumento sus capacidades para manejar objetos en 3D e imágenes con una calidad extremadamente alta. Alcanza a manejar video de una resolución de 4096 x 4096 píxeles, una cantidad muy grande que garantiza su capacidad de manipulación de imágenes. Una de las características más significativas que se alcanzó con este ultima técnica fue la capacidad de diferenciar entre un fondo y un objeto, es decir un plano estático será codificado solamente una vez y grabar los objetos en movimiento.

MPEG-4 tiene la capacidad de utilizar objetos audiovisuales, los cuales son solamente representaciones de objetos reales o virtuales que se representan en forma visual o auditiva. Cada objeto visual puede ser compuesto por sub-objetos los cuales incrementan la complejidad de cada objeto virtual.

Otro ámbito que maneja eficazmente esta innovadora técnica es la de Planos de Objetos de Video los cuales son las instancias de un objeto de video en un tiempo determinado, con esto se busca reducir el proceso de codificación en distintos planos componentes de una escena en general. [8]

Existe una capacidad de relación entre técnicas MPEG utilizadas, una secuencia MPEG-1 puede ser grabada como video MPEG-2 o MPEG-4 y viceversa. En el caso que una secuencia MPEG 4 sea grabada como MPEG-1 las características nuevas no serán utilizadas.

Se puede observar en la siguiente tabla como se fue desarrollando el formato MPEG a través del tiempo.

MPEG	1	2
Máximo Ratio de Bits (Mbps)	1.86	15
Alto de Imagen (px)	288	576
Ratio de Imágenes (fps)	30	30
Ancho de Imagen (px)	352	720

- **AVI** (*Audio Video Interleave*).

Es un formato de video de los más utilizados hoy en día; fue definido por Microsoft y está basado en un formato denominado como RIFF[9]. AVI es un estándar conocido como *de facto*[10] convirtiéndolo en un formato bastante utilizado por su manejo simultáneo de audio y video en un mismo envío de información.

El formato de los datos no está definido en la técnica, sino en un elemento externo denominado codec que tiene la función de interpretar la secuencia simultánea de audio y video para procesarlas. Así también esta información compuesta debe ser almacenada entrelazadamente para poder ser interpretada en el destino con secuencias de video acordes con su sonido respectivo.

Como en el formato RIFF, existen fragmentos componentes denominados chunks, donde cada uno tiene asignadas etiquetas que identifican su estructura. El primer chunk

[9] *Resource Interchange File Format* es una estructura de archivo marcada para recursos de archivos multimedia que define formatos de archivo por medio de un bloque llamado *Chunk*; en el cual se establece el formato de un fichero de datos de un archivo AVI.

[10] Patrón que no ha sido estructurado por un organismo de estandarización, sin embargo ha sido muy aceptada por diversos usuarios.

es la cabecera y en esta se define la información general del archivo como las dimensiones de la imagen; el segundo chunk contiene la información entrelazada de audio y video. Un codec tiene la facultad de interpretar algunas etiquetas, para las cuales se escogerá el mejor codec que procese dicho flujo de datos sin la intervención del usuario

El reproductor separa los elementos de video y audio y son alojados en el buffer de memoria y los coloca en el códec correspondiente. En el códec de video se almacenan todo el conjunto de elementos de video y audio. El reproductor solamente se encargaría de coordinar las imágenes y el sonido adecuadamente.

· **WMV** (*Windows Media Video*).

Este formato es basado en el formato ASF (*Advanced System Formats*) que es visto como un contenedor multimedia de audio y video digital en la cual dependiendo al tipo de archivo que se maneje es como se identifica el archivo por medio de otra extensión.

Los archivos que manejan información de audio son definidos por la extensión .wma (*Windows Media Audio)* y los que manejan video o ambos son clasificados con la extensión .wmv, aunque podrían utilizar la extensión .asf indiferentemente. Como ya se mencionó los archivos ASF contienen una amplia variedad de contenidos digitales por esto la necesidad de mencionar estándares de los tipos de archivos manejables para el caso de video se establece lo siguiente:

Cada stream ASF tiene asignados valores que lo identifican, un archivo ASF puede ser identificado como ASF_Video_Media, por tanto este contendrá algunos campos que definen sus propiedades:

- *Encoded Image Width*. Especifica el ancho de la imagen codificada en píxeles. (32 bits de tamaño máximo).
- *Encoded Image Height.* Especifica la altura de la imagen codificada en píxeles (32 bits de tamaño máximo).
- *Reserved Flags.* Especifica banderas reservadas siendo fijado a dos.
- *Format Data Size.* Especifica el tamaño del formato de dato utilizado en bytes.
- *Format Data.* Especifica los detalles del formato de la imagen en una estructura que incluye información como tamaño de la imagen, nivel de compresión, resolución horizontal utilizada, resolución vertical, etc.

Los archivos *.wmv* pueden ser interpretados por versiones de reproductor de Microsoft tales como Reproductor de Windows Media 7, Reproductor de Windows Media para Windows XP y Reproductor de Windows Media 9 series.

· **MOV** *(QuickTime Format).*

Es una extensión de fichero que se aplica a un formato video para QuickTime; incluye audio, animación, video y capacidades interactivas.

La *movie* utilizada en QuickTime se basa en una serie de operaciones las cuales son una descripción de la estructura de las muestras multimedia que deben indicar al dispositivo reproductor: qué tipo de archivo media se presenta, donde están alojados los datos, cómo y cuándo representar cada componente. Un componente o muestra es manejado en otras técnicas como segmentos de información (*audios simples* o *video frames*), para esos casos en particular, se analiza cada muestra como un todo y se procesa. En el caso de una *movie,* cada muestra no es un elemento componente, estas se alojan fuera y se van utilizando según los requerimientos

Por lo tanto una *movie* es una estructura que permite a una computadora localizar e interpretar los datos requeridos, es decir, cuando se reproduce, el reproductor obtiene e interpreta las muestras descomprimiéndolas y conformándolas como sea necesario, presentándolos en la secuencia apropiada.

Existe un término conocido como *movie file* que es un archivo contenedor de una copia de la estructura del movie o también puede almacenar solo una referencia de una estructura.

Si un file movie contiene la estructura puede también incluir la cantidad de datos utilizados en cada secuencia, llamándose así como *archivo autónomo* ya que contiene información completa de si mismo. Cuando esto sucede solo restaría ser trasmitido por un reproductor simple para su ejecución. **(Ver Figura 1-18)**

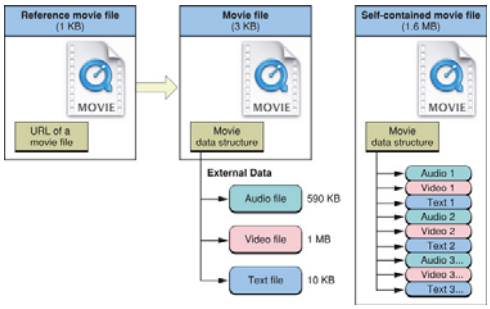


Figura 1-18. *Contenido del archivo movie file*[*]

*http://developer.apple.com/documentation/QuickTime/RM/Fundamentals/QTOverview/index.html

Una película de video está formada por *tracks*, cada track especifica su propio contenido, el tipo de formato multimedia que contiene: audio, video o texto, una referencia donde se especifica la muestra de datos están alojados y el formato de compresión utilizado.

La referencia puede estar apuntando hacía muchas alternativas de almacenamiento: una ubicación en la red, un servidor, a un bloque de memoria, etc. Los tracks en general se clasifican en tres (audio, video y texto) para cada uno de ellos pueden existir muchas referencias por ejemplo: cuando se maneja el video por medio de una secuencia de imágenes, cada una de éstas tendrá su propia referencia.

En una misma movie se pueden incluir múltiples tracks (de audio video y texto) como por ejemplo múltiples track de texto, cada una de ellas en diferente idioma. Un gran número de tracks de video involucrados pueden estar basados en diferentes técnicas de compresión que lo hacen mucho más complejo.

Existen otras características para una movie en QuickTime que son tracks visuales donde se especifican las propiedades para poder reproducir tracks al mismo tiempo con diferentes especificaciones como el grado de transparencia o translucidez. A grandes rasgos está es una explicación de la representación de un formato de video por medio del reproductor QuickTime creado por Apple.

La elección del formato de video a utilizar depende de muchos factores, calidad, disponibilidad, compatibilidad entre muchas otras; una vez identificados los formatos de archivos más importantes da lugar a estudiar la forma en que la información fluye en el traslado de la información.

1.4 Cámaras de Video Digital.

Las cámaras digitales son elementos básicos en el proceso de recopilación de información digital en forma de video o imagen. Existe una gran variedad de cámaras de video las cuales se clasifican con base en el tipo de información que manejan y por los periféricos que las interconectan.

Una de ellas son las cámaras analógicas, estas tienen un número infinito de puntos de información los cuales no pueden ser representados en su totalidad, haciéndola más ineficaz en aspectos como edición y manejo de la información. Las cámaras digitales se basan en imágenes digitales las cuales son obtenidas a través de un medio electrónico y su información es representada por medio de pulsos eléctricos, lo cual facilita su manejo a través de medios de transmisión utilizados en cualquier red de datos.

Las cámaras digitales usan elementos sensibles a la luz, los cuales registran e interpretan ondas de luz provenientes del objeto. La lente de la cámara enfoca la imagen en un sensor

de imágenes llamado *CCD*[11] , el cual definirá la resolución de la imagen determinado por el numero de sus *células fotoeléctricas*[12], esté número se expresa en pixeles y entre más pixeles se manejen mayor será la resolución; una cámara digital de imagen maneja hasta veinte millones de píxeles.

El proceso de transformación numérica del color que almacena un píxel depende tanto del modelo de color usado como de la profundidad de color manejado. La profundidad de color se refiere a la cantidad de bits que maneja cada píxel, el modelo de color es el esquema a utilizar para la representación de toda una gama de colores, el modelo más utilizado es el RGB (Red, Green, Blue) que permite generar cualquier color a partir de estos tres colores básicos Rojo, Verde y Azul; variando la proporción, por medio de ocho bits para cada color, se puede conseguir la tonalidad de color deseado, por ejemplo cuando una de las componentes vale 0, quiere decir que ese color no es usado, en cambio si vale 255 significa que el color es utilizado en su máxima tonalidad.

El tamaño del CCD es un factor importante en la calidad de la imagen, un sensor de tamaño pequeño puede ocasionar interferencias en la imagen por la proximidad de sus elementos fotosensibles por lo tanto a veces es conveniente tomar en cuenta ese detalle y algunos otros tales como el factor de relleno. Los tamaños de CCD están definidos en pulgadas, el tamaño estándar actual es de 2/3" pero existen otros formatos comunes utilizados actualmente de 1/3 y 1/2 de pulgada.

El factor de relleno es el porcentaje del área del sensor que es sensible a la incidencia de la luz, idealmente este debería ser del 100%, desafortunadamente esto no se logra por efectos como *blooming*[13] . Antes de llegar al sensor óptico, debido a que el sensor *CCD* es un dispositivo monocromo, la imagen pasa por medio de un patrón de colores el cual tiene por objetivo clasificarlos, logrando con esto que el sensor interprete la información en porcentajes de luz roja, azul y verde. **(Ver Figura 1-19)**

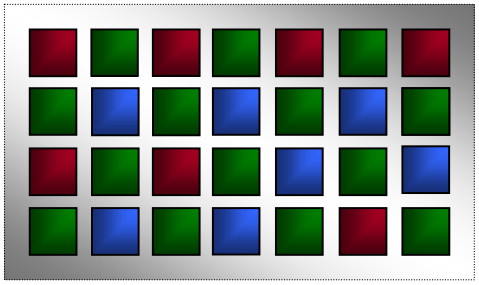


Figura 1-19. *Patrón de Colores*

[11] Charge Couple Device es un sensor de imagen con diminutas células foto eléctricas que registran la imagen.
[12] Elemento sensible a la luz que es capaz de producir una respuesta eléctrica.
[13] Efecto generado por la saturación en la capacidad de los píxeles, píxeles vecinos son invadidos con información errónea generando una mancha blanca en sentido vertical.

En algunos modelos de cámara profesionales se usan tres diferentes sensores CCD cada uno interpreta un color diferente del modelo básico. La mayoría de los CCD llevan a cabo una captura de imagen en dos campos (*escaneo entrelazado)* los cuales conformaran la información completa de la imagen, en un campo se capturan líneas pares y en otra impares. Actualmente se han incluido CCD con capacidades de *escaneo progresivo* el cual genera imágenes completas en un solo campo, líneas pares e impares son capturadas continuamente. La luminosidad de los objetos puede llegar a saturar el patrón de colores básico lo cual generaría un descontrol en la interpretación de color, para ello se utiliza un *iris* el cual ajustará la sensibilidad a exposiciones de luz muy variadas, en exposiciones de gran luminosidad, contienen un filtro de densidad neutra que evitan la saturación en el CCD.

Ya que el CCD ha capturado y filtrado la imagen, llega la parte de la digitalización de la señal, que consiste en interpretar la señal por medio de una base en el tiempo y un convertidor analógico – digital que proporcione una aproximación digital por medio de muestreo de esta. En este momento se tiene una señal con componentes analógicos RGB los cuales se busca sean convertidos a formato digital para su envío, por medio del convertidor se realiza dicha conversión tomando muestras definidas por la base de tiempo las cuales representaran a la señal analógica continua. Se pueden obtener señales digitales muy exactas a la señal original, para esto se necesitaría reducir el intervalo de muestreo base, sin embargo definitivamente no es conveniente ya que el convertidor funcionaría mucho más lento.

Hablando un poco más de las señales analógicas clasificadas en colores, se puede muestrear dichas señales con base en su número de bits que las conforman (*8 bits por cada color básico).* Partiendo de la información de color, las señales de video de rojo, verde y azul son combinadas con la finalidad de obtener dos señales equivalentes, una corresponde al brillo y otra parte al color denominadas:

a) *Luminancia (Y).* Señal que contiene solamente información referente a variaciones de brillo, este valor representa la cantidad blanco y negro siempre componentes de cualquier imagen. La señal de luminancia se forma combinado 30% de la señal roja, 59% de la señal verde y 11% de la señal azul.

$$Y = 0.30R + 0.59G + 0.11B$$

Se pueden lograr valores de luminaria que representan solamente escalas grises, blanco y negro en una imagen. **(Ver Figura 1-20)**

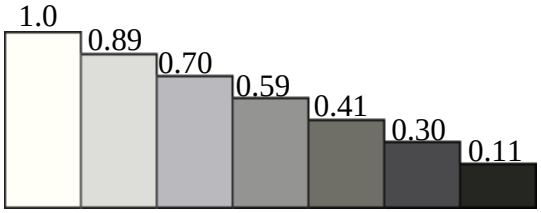


Figura 1-20. *Valores de Luminancia*

b) *Crominancia (C).* Señal que contiene información en color, la cual está representada por dos ecuaciones las cuales en caso de trasmitir una imagen monocromática deben anularse, por lo tanto para representar una señal a color se deben incluir 3 señales una de ellas definida por Y, las dos restantes deben deducirse a partir de los tres colores primarios, a cada uno de estos se le restará el valor de luminancia (*R-Y, G-Y, B-Y)*, analizando un poco estas tres expresiones, se puede determinar que la diferencia de color G-Y es la que tiene coeficientes menores consecuentemente está más expuesta al ruido, por lo tanto las otras dos señales a digitalizar son :

$$R\text{-}Y = 0.70\ R - 0.58\ G - 0.11\ B \quad \textbf{(Cr)}$$

$$B\text{-}Y = -0.29\ R - 0.58\ G + 0.88\ B \quad \textbf{(Cb)}$$

El proceso de conversión del espacio RGB se lleva a cabo aplicando las expresiones anteriores tomando en cuenta que el ojo humano es mucho menos sensible al color que al brillo, la señal de luminancia se muestra a una frecuencia de 13.5 Mhz, mientras que Cr y Cb se hace a 3.375, en otras palabras, Cr y Cb se muestrean cuatro veces menos que Y , por lo tanto se dice que tener un formato 4: 1: 1 (4 muestreos I, 1 muestreo Cr y 1 muestreo Cb). **(Ver Figura 1-21)**

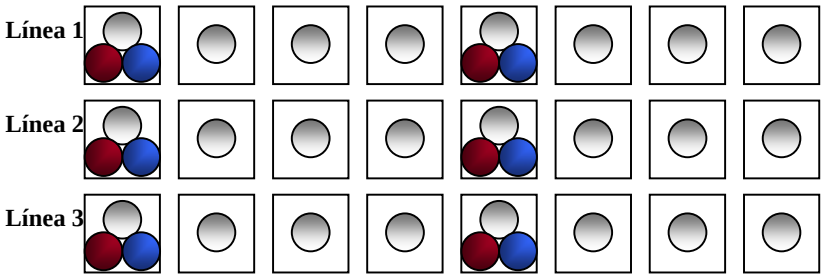


Figura 1-21. *Muestreo 4:1:1, las muestras de color Cr,Cb se presentan cada 4 muestras de luminancia.*

Una vez digitalizadas las imágenes se lleva a cabo la compresión de las señales, recordemos que este proceso se realiza por medio de un dispositivo llamado codec. El proceso de codificación es basado en técnicas ya estudiadas entre las que se encuentran *Transformada Discreta de Coseno, Redundancia entre Píxeles,* etc. Algunos dispositivos de compresión tienen capacidades anexas que regulan la calidad de una imagen tales como *balance de blancos*[14], *nitidez de la imagen*[15], etc.

Para una cámara analógica la información será almacenada en cintas las cuales almacenarán toda la información recabada, en el caso de cámaras de red basadas en el

[14] Control que busca ajustar el brillo de los colores rojo, verde y azul para que la parte más brillante de la imagen aparezca en color blanco.

[15] Característica de la imágenes con un alto grado de calidad en detalles, relacionada con la capacidad de un píxel para interpretar información con base en el número de bits asociados a él.

protocolo IP la parte de comunicación sobre este estándar es incluida, la información no es almacenada directamente en la cámara de video sino que es trasmitida por medio de una interfaz conectada a un dispositivo de almacenamiento masivo denominado DVR (*Digital Video Recorder*) el cual contendrá todo los datos digitales que conforman al video.

En las cámaras de video de red se contienen otros complementos como módulo *ethernet / wifi*, que son la parte del sistema que permite conectar a la cámara en los enlaces físicos de red tales como un router o switch. También incluyen una unidad central de procesamiento (*CPU*) con el cual se puede llevar a cabo los procesos inteligentes de una red como gestión de la conectividad (10/100 Mbps) y gestión con un servidor web. Otros dispositivos como DRAM, memoria FLASH se encargan de controlar los movimientos de la cámara así como la detección de movimiento.

Las cámaras de video digital tienen en general los mismos componentes (lentes, sensores, patrones de color, etc.), sin embrago las cámaras diseñadas para su uso en una red de datos incluyen módulos mucho más avanzados los cuales controlan todo lo que conlleva una cámara bajo un sistema de seguridad tales como comunicación remota a ella y movimientos programados los cuales la cámara llevará a cabo.

La resolución es una característica importante que definirá el tamaño de la imagen capturada por la cámara. En el video analógico se utilizan líneas de TV (*TVL)* ya que la tecnología del video analógico procede de la televisión. Para un sistema digital, la imagen está formada por pixeles. En gran parte de América, Japón, Corea del Sur y Taiwan se utiliza el estándar NTSC (*National Televison System Committe*) (525 líneas horizontales transmitidas a 29.91 veces por segundo). Para Europa y África se utiliza PAL (*Phase Alternating Line)* (625 líneas horizontales transmitidas a 25 veces por segundo). Para Francia, países de la Unión Soviética y África del Norte se utiliza SECAM (*SEquential Couleur Avec Memoitre)* (525 líneas horizontales a 25 frames por segundo).

Cuando el video analógico es digitalizado, el tamaño de la imagen está en función del número TVL utilizado. En NTSC, el tamaño máximo de imagen es de 720 x 480 píxeles. La resolución más utilizada es 4CIF (704x 480) y 2CIF (704 x240). **(Ver Figura 1-22)**

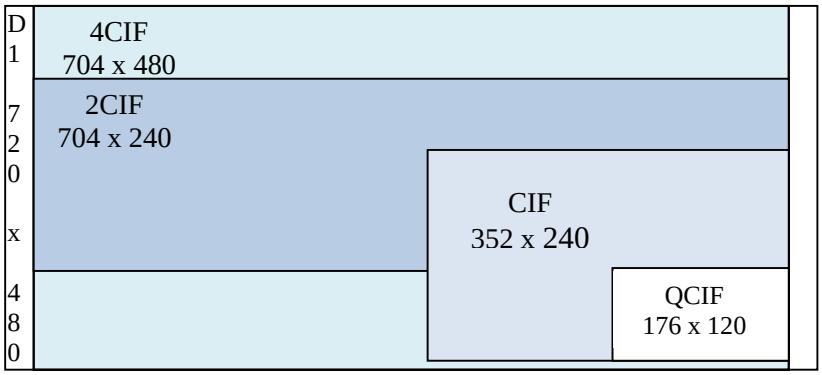


Figura 1-22. *Resoluciones NTSC*

Algunas resoluciones utilizadas en cómputo han sido adoptadas en el ámbito de la videovigilancia con lo cual se proporciona una mejor flexibilidad debido a que en la mayoría de los casos la videovigilancia IP es desplegada en computadoras personales tales como VGA (640 x 480 pixeles), QVGA (320 x 240) , XVGA (1024 x 768), etc.

A mayor resolución mayor cantidad de detalles en la imagen, que para el caso de la videovigilancia esto es una ventaja para la identificación. Para el caso de grabadores de video la resolución máxima obtenida será la correspondiente a 400 000 pixeles (0.4 Megapixeles).

Las nuevas tecnologías en cámaras de IP ofrecen resoluciones de 1.3 Megapixeles (1280 x 1024), 3 veces más que las cámaras analógicas. Las cámaras IP aportan beneficios en las relaciones de aspecto de la imagen. Un circuito cerrado de televisión usa una proporción de 4:3 lo que significa que la imagen tiene cuatro unidades de ancho por 3 unidades de alto. Para las resoluciones de alta definición el ratio de aspecto es de 16:9.

Los beneficios de alta definición no son aplicables para monitores de pantallas estándar. La utilización de gran tamaño de imágenes traerá consigo aumento en costos y utilización del medio de transmisión para el envío de estas.

1.5 Audio

Es un elemento importante en aplicaciones de videovigilancia ya que puede esclarecer imágenes que parecieran confusas. El sonido son ondas que viajan por medio del aire hasta sensores localizados en el oído humano el cual puede ser creado por muchos orígenes en forma analógica como una representación eléctrica de una señal que cambia su nivel.

Las señales analógicas siempre están presentes, sin embargo, las señales de audio están siendo convertidas a señales digitales por muchos beneficios. Las señales analógicas tienen la desventaja de ser más inmunes al ruido que las señales digitales lo que evita su transmisión confiable en los medios. Las señales de audio digitales se utilizan en forma comprimida o no comprimida y pueden manejarse en dos formas diferentes. Un método es utilizar de manera independiente las señales de audio o usar audio y video digital en un único envío.

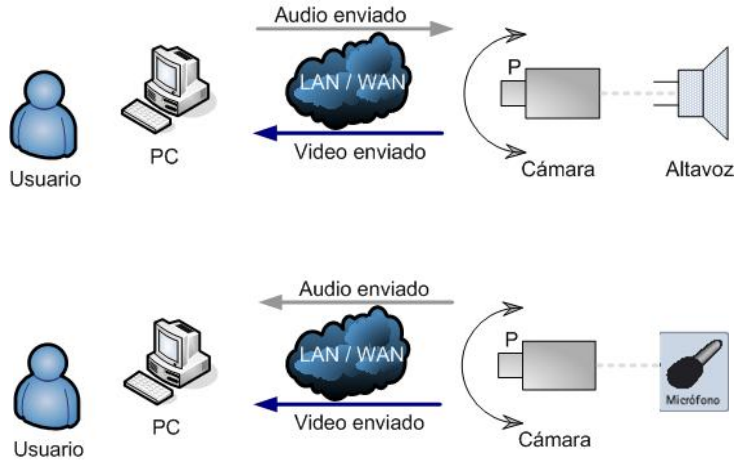
Cuando el audio es separado del video existe mayor trabajo en el envío de la información por el trato diferente de elementos componentes, pero existe mayor flexibilidad ya que las señales de audio pueden ser encaminadas de manera diferente que aquellas de video. Cuando se utiliza como un único elemento, las posibilidades de perdida se ven reducidas por la menor cantidad de señales enviadas.

Con lo que respecta a soluciones de videovigilancia, cada señal de video y audio es convertido en un stream IP que es enviado a su destino por medio de una red de datos. Una gran ventaja de utilizar tecnología basada en IP es que puede ser combinada con otros

sistemas. Cuando muchas funciones se logran integrar pueden consolidarse soluciones mucho más completas que finalmente es lo que determina la eficiencia de un sistema de está naturaleza.

La integración del audio es prácticamente sencilla porque la necesidad de cableado adicional se omite a diferencia de sistemas analógicos donde se debe instalar cableado alterno para las señales de audio. Una de las capacidades de las cámaras IP es la captura de audio para ser digitalizado, comprimido y enviado en la red. En aplicaciones reales de videovigilancia se utilizan diferentes modos de audio:

Modo Simplex. El audio se envía del usuario a la cámara o el audio se envía de la cámara al usuario



Modo Half Duplex. El envío se realiza en ambos sentidos nunca al mismo tiempo

Full Duplex. El audio se envía en ambos sentidos al mismo tiempo

Es este capítulo se mencionaron fundamentos acerca de señales digitales y lo que implica su utilización. Se detalló el proceso de transformación con base en señales analógicas y se mencionó la compresión del video como factor importante para reducir cantidades de información; la eficiencia de compresión dependerá de las características de las imágenes implicadas así como del método utilizado. Así también se identificaron algunos de los formatos digitales más utilizados en video digital con el fin de conocer aquellos que se encontrarán en soluciones de videovigilancia. En los sistemas diseñados para videovigilancia un factor importante es el audio, situaciones comprometedoras pueden auxiliarse de señales de sonido para lograr entender el significado real del suceso y ser una prueba incuestionable con valor legal.

Una vez comprendido el proceso de generación del video digital es posible analizar su transmisión en redes de datos basadas en el protocolo IP. Este tipo de medios de comunicación han dado buenos resultados en el ámbito computacional y ha tomado un gran auge en el ámbito de la videovigilancia por lo cual a continuación es objeto de estudio.

Capítulo 2

Redes de Computadoras

La transmisión de video digital es un aspecto importante a considerar debido a que en materia de seguridad es necesario alojar contenidos en lugares remotos de difícil acceso. Una red de videovigilancia IP no es más que el flujo de datos en forma de imágenes por medio de un canal de comunicación hasta un medio de almacenamiento donde se mantendrá la información recabada. Las redes de computadoras han sido una alternativa tan eficaz en el envío de datos digitales que actualmente se ha vuelto una alternativa bastante utilizada por la mayoría de las soluciones existentes para envíos de video.

2.1. Conceptos Básicos

Una red de computadoras se origino por la necesidad de compartir información y recursos de manera fácil y eficiente. Con el paso del tiempo las necesidades fueron aumentando en materia de disponibilidad y seguridad lo que permitió el desarrollo de nuevas tecnologías que soportarán estas características. Así se logro tener diferentes tipos de información en un mismo medio lo que origino a tener lo que hoy se le conoce como *redes de datos.*

La identificación de una red para su clasificación está fundamentada en características especiales, por lo tanto, una red pequeña traerá consigo una menor cantidad de distancias a comunicar donde los dispositivos que la conforman están alojados bajo un mismo espacio físico de funcionamiento mientras que en redes de cobertura amplia sus componentes se encuentran totalmente distribuidos.

En seguida se mencionan tres grupos principales para clasificar una red:

1) Por su *extensión geográfica*:

- **Red de Área Local**. Su espacio de trabajo es reducido, generalmente se encuentran en oficinas o edificios, una red de área local pude o no tener conexión a *Internet* y su *latencia*[1] es muy baja. También es llamada LAN (*Local Area Network).*

- **Red de Área Metropolitana**. Su campo de acción está relacionado con distancias grandes de cobertura tales como ciudades; se conforma por redes de área local interconectadas entre sí y puede ser pública o privada. También es llamada MAN (*Metropolitan Area Network*).

- **Red de Área Extensa**. Su campo de acción abarca países o continentes, no tiene topología característica ya que es asimétrica (sin topología definida), Internet es un claro ejemplo de este tipo de red; también es llamada WAN (*Wide Area Network*).

2) Por la forma en que *comparten información*:

- **Centralizada.** El control de sus recursos es establecido desde un punto de administración en específico, la compartición e instalación de software es por medio de una central que regula el funcionamiento de toda la red.

[1]Retraso temporal que experimenta una señal en su viaje por los medios físicos.

- **Peer to Peer**. En este tipo de red todos los usuarios toman el rol de administrador para sus propios equipos, la compartición y distribución de la información es responsabilidad de cada usuario.

3) Por su *arquitectura:*

- **ArcNet.** *(Attached Resource Computer Network)* fue desarrollado por Datapoint Corporation basándose en una arquitectura de bus que utiliza el método de acceso al medio llamado *token-passing*[2]. .ArcNet funciona adecuadamente bajo medios de transmisión como cable coaxial, par trenzado o fibra óptica, logrando una capacidad de 2.5Mbs en transmisión de datos.

- **Ethernet**. Es la arquitectura más popular utilizada en la actualidad, fue creada por Xerox Company, convirtiéndose en el estándar actual IEEE 802.3 para la conexión de redes. Utiliza una topología de bus empleando un método de transmisión de datos denominado *Carrier Sense Multiple Access with Collision Detection (CSMA/CD*).

  Su funcionamiento está basado en monitorear el canal de comunicación para enviar datos. Cuando se desea enviar la información, se identifica si el medio está disponible, de ser así, se realiza el envío hasta el destinatario, en caso de que dos computadoras envíen información al mismo tiempo, habrá una colisión en el canal originando pérdida de información, este método permitirá que se identifique la existencia de dichas colisiones, y futuros envíos tendrán que esperar un tiempo determinado para un nuevo intento.

  Las velocidades que alcanza esta arquitectura son 10Mbps banda base, existiendo en general 3 clasificaciones principales:

  - ***10BASE2*** (Ethernet de cable delgado): Permite segmentos de red en cable coaxial de hasta 185 m de longitud.
  - ***10BASE5*** (Ethernet estándar): Permite segmentos de red en cable coaxial de hasta 500m de longitud.
  - ***10BASE-T***: Transporta tramas Ethernet en cables económicos de par trenzado.

  Buscando satisfacer nuevas necesidades de transferencia de información se crearon nuevas versiones:

  FastEthernet o *100BASE-T* soporta velocidades de transmisión de hasta 100Mbps. Este tipo de tecnología tiene como base la primera arquitectura Ethernet pero

[2] Método de acceso en la topología de anillo en el cual existe un conjunto de bits llamado token que se traslada de una computadora a otra, una computadora no puede trasmitir a menos de que lo tenga en posesión.

oficialmente controlada por el estándar IEEE 802.3u, los esquemas de cableado que utiliza son:

- ***100BASE-TX.*** Par trenzado de alta calidad compuesto por dos pares de cables.
- ***100BASE-T4.*** Par trenzado de una calidad normal compuesto por 4 pares de cables.
- ***100BASE-FX.*** Utilizado en enlaces a través de fibra óptica.

GigaEthernet. Arquitectura la cual soporta transmisión de datos de hasta 1Gbps, esta arquitectura esta controlada por el estándar IEEE 802.3z.

10GEthernet. Es el más rápido de los estándares. IEEE802.3ae define una versión a una velocidad nominal de 10Gbits/s. Este estándar contiene siete tipos de medios para redes para LAN, MAN y WAN.

- **Token Ring**. Fue ideado por IBM, su funcionamiento se basa en el método de acceso al medio denominado token passing o acceso de señales, alcanza velocidades de 4Mbps a 16Mbps. El proceso de funcionamiento es hacer pasar un grupo de bits denominado token por medio de la topología de anillo, así la computadora que quiera enviar información debe tener en su poder el token correspondiente para tener la facultad de enviar información, una vez alcanzado el destino, se libera el token y pasa a la siguiente computadora para su posible utilización. Este tipo de arquitectura se vuelve mucho más eficiente que Ethernet en redes con un alto índice de actividad.

- **AppleTalk**. Es una arquitectura de red que está incluida en los sistemas operativos Macintosh, siendo una colección de protocolos referentes al modelo OSI 3 que garantizan la funcionalidad de red. Cualquier dispositivo conectado a una red Appletalk es considerado como un nodo. Una ventaja de esta estructura de red es que no necesariamente los equipos conectados deben ser Macintosh ya que admite tecnologías como Ethernet y Token Ring, otra ventaja por la que se identifica esta arquitectura es la de compartir los recursos existentes en la red como si fueran archivos o impresoras logrando una operabilidad de recursos completa.

2.2. Topologías de Red

Es el arreglo de los componentes que conforman una red a través de los medios de comunicación, para su implementación se deben considerar factores importantes como número de equipos a instalar, método de acceso al medio, la forma de administración de la red, entre otras.

Existen dos características que definen la topología en una red:

[3] Arquitectura conformada por 7 capas que estandariza niveles de servicio y formas de interacción en computadoras que intercambian información a través de la red definida por ISO *(International Standard Organization)*

- *Topología Física*. Es la disposición física de los componentes de una red, así como su ubicación geográfica en la cual se encuentran colocados.
- *Topología Lógica*. Es la forma en que la información viaja a través de los medios físicos, aquí se incluyen los métodos de comunicación así como la rutas de envío de datos entre nodos[4] de red.

A continuación se mencionan los diferentes tipos de topología con base en su distribución física:

- **Bus**. En este tipo de topología todas las computadoras están conectadas a un mismo canal de comunicación, ocasionando que solamente un equipo pueda utilizar el medio de transmisión a la vez para el envío de información, utiliza el tipo de arquitectura Ethernet y por consecuencia el método de acceso al medio *CSMA/CD.*

  Al bus lineal por el cual viajan los datos también se le conoce como *backbone* o *segmento.* Cabe mencionar que en los extremos del bus es necesario colocar un dispositivo llamado *terminador* el cual garantiza que una señal no ocupe indefinidamente el canal de comunicación después de no encontrar el equipo destino. **(Ver Figura 2-1)**

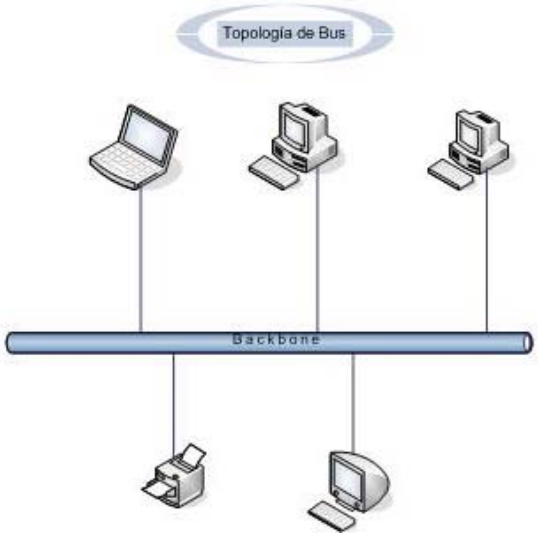


Figura 2-1. *Topología de Bus*

- **Estrella**. Este tipo de topología se conforma de un dispositivo llamado concentrador (*Hub*[5]) o conmutador (*Switch*[6]), en el cual las computadoras se conectan con

[4] Elemento que es conectado a la red y es capaz de comunicarse con otros elementos de la red, por ejemplo equipos cliente, servidores, repetidores, etc.
[5] Componente de conectividad que provee conexión centralizada para equipos de cómputo, existen tres clases de *hubs*, activos, pasivos e inteligentes.
[6] Dispositivo de interconexión de redes que opera en la capa 2 del modelo OSI, conecta dos segmentos de red diferentes en los cuales circularan datos dependiendo de una dirección física destino.

segmentos de cables propios que garantizan la operabilidad de la red. Tiene una gran capacidad de escalabilidad ya que solamente se limita por la cantidad de puertos que pueda manejar el dispositivo central considerando la posibilidad de incremento en el número de los puertos por medio de conexiones en cadena entre conmutadores.

La desventaja de realizar una centralización es la vulnerabilidad de la red a un sólo punto, el cual en caso de verse afectado no habrá conexión posible en ninguno de los nodos. Sin embargo en caso de que un nodo falle, los demás equipos podrán trabajar normalmente en la red.

El proceso de instalación de esta topología es moderadamente complicado ya que por cada equipo que se desee instalar se necesitará un único segmento de red que establezca la conexión con el concentrador, su configuración es sencilla ya que para cualquier modificación, se lleva a cabo un procedimiento entre el equipo y el componente central. **(Ver Figura 2-2)**

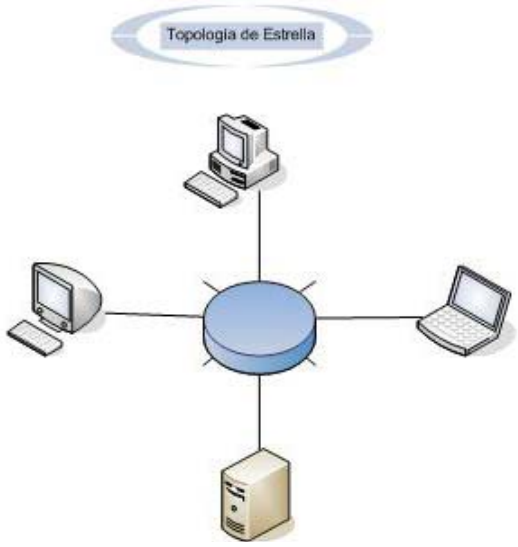


Figura 2-2. *Topología de Estrella*

- **Anillo.** En esta topología los datos se trasladan por medio de un sólo canal de comunicación que conecta a todos los equipos de cómputo cíclicamente, la información viaja en un sólo sentido, así que no es necesario algún tipo de enrutamiento ya que todas las computadoras que no son destino sirven como repetidores para las señales eléctricas que viajan en el medio físico.

  Una ventaja es la poca cantidad de cable que se necesita para la conectividad de las máquinas y la posibilidad de expansión, ya que cada nodo funciona como repetidor de manera que constantemente se regeneran las señales eléctricas.

  Una desventaja en este tipo de red es la pérdida de funcionalidad por fallas en alguna de las computadoras que forman parte de su estructura, la pérdida de alguna de ellas

conlleva a un anillo incompleto que ocasiona una imposibilidad de flujo de información. **(Ver Figura 2-3)**

Existen topologías de anillo compuestas, diseñadas para reducir tiempos de respuesta en el tránsito de información en la red. Se establecen dos canales de comunicación en los cuales existirá para cada uno un flujo en sentido opuesto que ayudará a un traslado de información mucho más libre y eficaz, disminuyendo tiempos de espera que provocaría la llegada de un token en cada canal de comunicación.

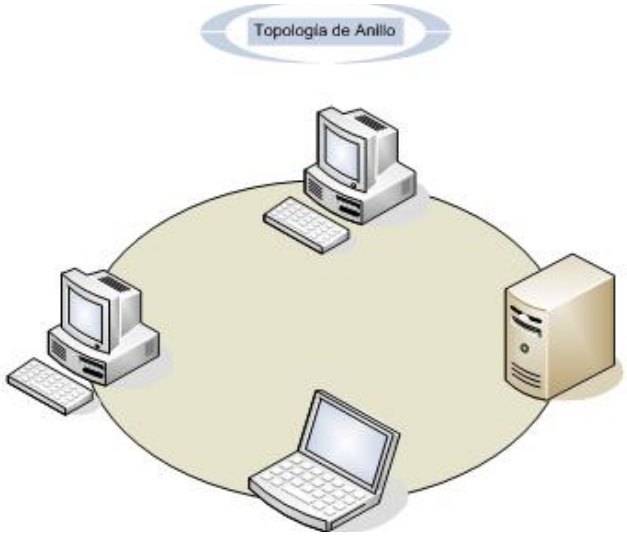


Figura 2-3. *Topología Anillo*

- **Malla.** Tipo de topología que tiene por característica redundancia de los enlaces que hay entre los equipos de cómputo que la conforman, cada computadora está conectada directamente con todos los equipos de cómputo restantes con la finalidad de lograr una comunicación eficaz y siempre fiable.

  Las ventajas que respaldan a esta estructura es la rápida detección de fallas ya que si un nodo de la red no funciona adecuadamente, se puede identificar dónde la conexión no está siendo llevada a cabo. Así también, sí un equipo pierde conectividad en la red, los demás equipos de cómputo pueden comunicarse normalmente sin verse afectados en el envío de información o tiempos de respuesta.

  La desventaja principal en este tipo de redes es el costo de instalación de los equipos ya que cada equipo necesita *n-1* puertos de comunicación, donde *n* es el número total de computadoras existentes en la red de malla.

  Se puede conocer la cantidad total de cables dentro de toda la red con base en el total de equipos que la conformarán:

  Nº de Cables = *n(n-1)/2*,

  n es el número total computadoras que conforman a la red.

Naturalmente al tener una gran cantidad de cables, el mantenimiento de la red se vuelve sumamente complicado. (**Ver Figura 2-4**)

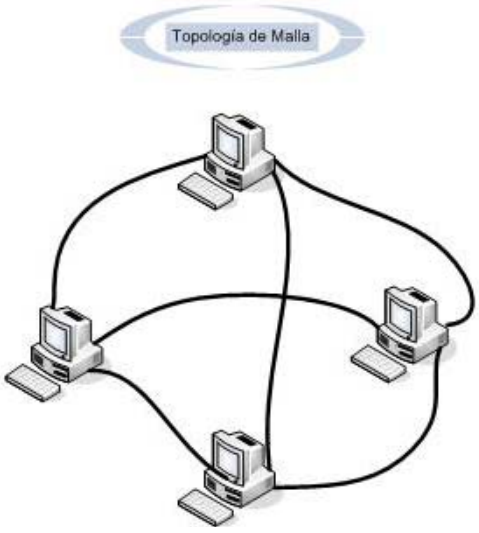


Figura 2-4. *Topología de malla*

Es importante hacer mención que este tipo de enlaces son utilizados para interconectar redes y no computadoras, ya que la complejidad de conexión por cada computadora sería extremadamente compleja.

- **Híbridos**. Esta topología está definida por ser una composición de dos o más topologías físicas, siendo el tipo de diseño de red más usado en la actualidad. Se logra una eficiencia adecuada por la complementación que puede brindar una topología a otra, sin embargo estos diseños tiene un costo elevado ya que su administración y mantenimiento deben controlar segmentos de red diferentes los cuales generan la utilización de equipo adicional que garanticen la conectividad. Esta estructura es utilizada para conectar redes de datos de grandes magnitudes. La conexión de un grupo de computadoras no sería la mejor opción de elementos a conectar ya que su fin principal no contempla enlaces en un mismo segmento.

  Algunos diseños se presentan a continuación:

  - *Estrella /Bus***.** Es una combinación de las topologías bus y estrella; muchos de los diseños en estrella están conectados a un mismo bus de comunicaciones regularmente por medio de concentradores, si una computadora falla no se ve afectada la red y el resto de las computadoras pueden seguir con la comunicación, si algún concentrador falla todas las computadoras conectadas a los puertos de ese concentrador fallarán de igual manera.(**Ver Figura 2-5)**

    Una desventaja de este tipo de topología es el costo de crecimiento ya que la escalabilidad de la red es por medio del incremento en el número de concentradores

que la conformarán, por lo tanto una red mucho mas amplia, implica una inversión mayor.

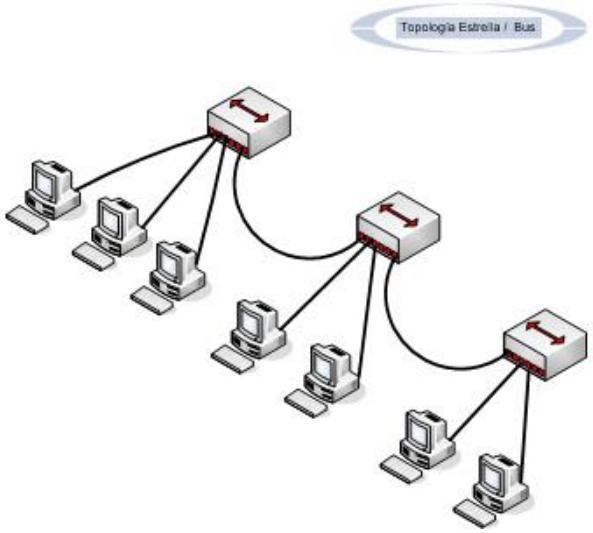


Figura 2-5 . *Topología Estrella / Bus*

- *Estrella /Malla*. Es una combinación de las topologías estrella y malla, proporciona una mayor fiabilidad que la topología estrella sencilla, se utiliza en estructuras grandes de comunicación donde las cargas de trabajo son distribuidas, es muy utilizada en las centrales telefónicas.**(Ver Figura 2-6)**

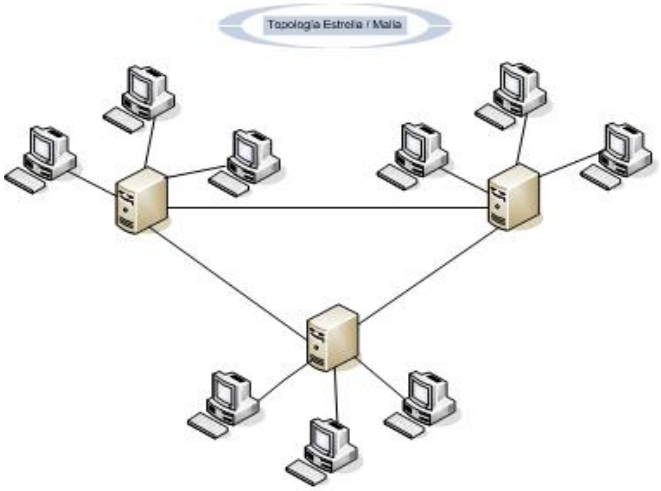


Figura 2-6 . *Topología Estrella / Malla*

Una vez contemplado el esquema físico de una red se presenta el esquema lógico.

Una topología lógica se refiere a la forma en que la información se traslada a través de los medios de comunicación *sin importar* la topología física existente.

Es importante mencionar los esquemas lógicos, ya que la integridad de las señales depende de un buen flujo lógico. El esquema lógico de la actividad de los datos esta determinado por tres formas principales:

- *Lógica de Bus.* Aquí se generan y se envían señales sin saber la ubicación del receptor, los datos se trasladan a través de toda la red en búsqueda de su destino, todas las computadoras analizan el paquete, siendo aceptado sólo por el destinatario, el resto de los equipos lo desechan. Las estaciones no siguen ningún orden para utilizar la red, sino que cada máquina accede a la red para transmitir datos en el momento en que lo necesita; esta topología también es conocida como *broadcast*, siendo esta la forma en que funciona Ethernet. La topología física asociada a esta característica lógica de red es de Bus, por lo tanto las máquinas que componen la red buscaran siempre la posibilidad de enviar información a través de un único medio originando colisiones por el envío simultáneo de paquetes.

- *Lógica de Estrella.* En este esquema el flujo de la información está definido en una sola dirección. Las topologías físicas que soportan estos esquemas lógicos son *estrella* y *bus*; en el caso de la estrella, todos los datos se dirigen al concentrador y después estos son redirigidos en un orden definido.

- *Lógica de Anillo.* En esta topología la dirección de flujo es un solo sentido. Si una máquina en un extremo desea enviar información a otra máquina, esta información debe fluir a través de todas las computadoras hasta llegar a su destino. Las topologías físicas afines son la de anillo y la de bus.

2.3. El modelo OSI

En la búsqueda de homogenizar a fabricantes de comunicaciones y las tecnologías que utilizan en sus sistemas, *ISO (International Standard Organization)* logró crear un patrón, esto es, un modelo que integra a los diferentes sistemas (*Digital Equipment Corporation - DECnet, Arquitectura de Sistemas de Red* – SNA, *TCP/IP)* que hasta ese momento se les conocía como *sistemas cerrados,* logrando que las comunicaciones entre ellos fueran posibles sin importar la preferencia del usuario.

El estándar se basa en dividir el proceso de comunicación en *capas*[7], las cuales a pesar de tener servicios y funciones específicas, están relacionadas entre sí para poder lograr en conjunto una comunicación íntegra; dividiendo en pequeñas partes la comunicación, se logra tener un proceso mucho más especializado y una comunicación completamente definida.

Este modelo es denominado *OSI (Open Systems Interconection*), y su finalidad es la de establecer los lineamientos para llevar a cabo comunicación entre los sistemas abiertos,

[7] Entidad que realiza por sí sola una función especifica.

está compuesto por siete capas que realizan una tarea particular, existiendo una relación directa entre capas adyacentes que garantizan la integridad en la comunicación.

A continuación se analizan las sietes capas: **(Ver Figura 2-7)**

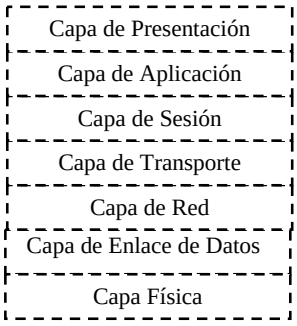


Figura 2-7. *Capas del Modelo OSI (Open System Interconection)*

1. *Capa Física*. Primera capa del modelo OSI, en este nivel se llevan a cabo un gran número de procesos eléctricos los cuales tiene como finalidad el envío de la información directamente a través del medio físico entre los que se encuentran: par trenzado, fibra óptica, etc. .

   Así también garantiza la conectividad física pero nunca la fiabilidad de ésta, controla y regula *tramas*[8] provenientes de la capa de *enlace de datos* para que sean acordes con el canal utilizado. Otras funciones que se realizan en esta capa son la siguientes:

   - Define la codificación de los datos de la trama de enlace de datos en un patrón de unos y ceros para su transmisión.
   - Establece la técnica y el tipo de transmisión.
   - Define el modo de operación de la línea de datos.
   - Regula la velocidad y la dirección de la transmisión de los datos.

   Por lo tanto esta capa proporciona los elementos físicos y eléctricos para realizar la conectividad y garantizar la funcionalidad en los sistemas.

2. *Capa de Enlace de Datos*. Segunda capa que tiene por finalidad garantizar el envío de datos confiablemente a través del enlace físico. Su función es llevar a cabo el enlace lógico, esto es, que el receptor determine sin ambigüedades los mismos datos que el emisor le ha enviado, acto fundamental para la entrega ordenada de la información que va segmentada en pequeños bloques denominados *frames o tramas,* a los cuales se les agrega una secuencia especial de bits al principio y al final que contiene información detallada que lo identifica en la red. **(Ver Figura 2-8)**

[8] Unidad de envío de datos, consta de cabecera, datos y cola.

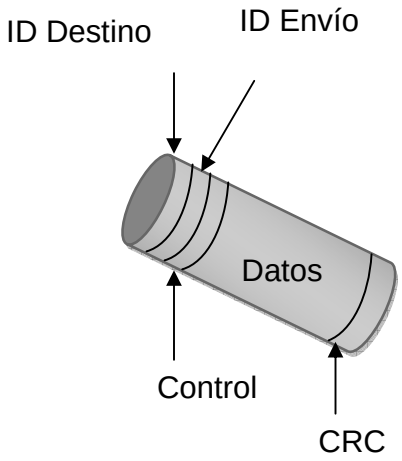


Figura 2-8. *Frame utilizado en la capa de enlace de datos.*

ID Destino. Representa la dirección de la computadora para la cual la información está siendo enviada.
ID Envío. Representa la dirección de la computadora origen que está enviando la información.
Control. La información contenida nunca es fija, por lo tanto, aquí se delimitan por medio de etiquetas, el inicio y final del segmento de información enviada, también se incluye información acerca del tipo de ruteo y segmentación.
Datos. Aquí esta contenida la información que se desea enviar.
CRC. Es una metodología que confirma por medio de un valor numérico si la información enviada y recibida es la misma, es llamado *método de redundancia cíclica*[9].

La importancia de esta capa en el modelo de referencia OSI, originó el estándar IEEE 802 en el cual se detalla el comportamiento de la capa de enlace de datos por medio de su segmentación:

Enlace de Control Lógico (LLC). Esta subcapa está definida en el estándar 802.2 y soporta los modelos de interconexión ***connectionless***[10] **y** ***connection-oriented***[11], su principal función es la de establecer y finalizar los enlaces de comunicación, controlar el trafico de los *frames* así también la secuencia de éstos.

[9] Algoritmo que analiza la integridad de la información; el equipo origen incluye en el frame un número obtenido por medio de un cálculo matemático hecho a un inicio de la transmisión; a su llegada al destino, el cálculo es vuelto a hacer, en caso de que los resultados sean los mismos, los datos son reales y correctos, de lo contrario, los datos cambiaron en la transmisión y se solicita un nuevo reenvío.
[10] Los datos son agrupados en paquetes lo cuales no tienen un camino específico, la información es enviada sin establecer una conexión directa con el destinatario.
[11] Se basa en la conectividad establecida con el destinatario antes del envío de la información, así se garantiza una conectividad siempre existente entre nodos

Control de Acceso al Medio (MAC). Esta subcapa tiene relación directa con la NIC (*Network Interface Card)*, siendo responsable de controlar el método de acceso al medio reconociendo las direcciones que contiene cada uno de los *frames*, comprueba la inexistencia de errores en éstos y garantiza la autenticidad de los datos.**(Ver Figura 2-9)**

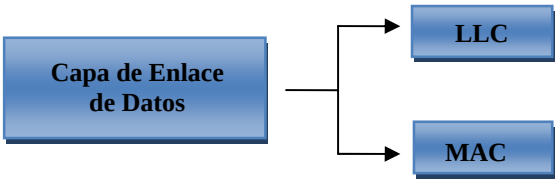


Figura 2-9. *Subcapas LLC y MAC (Proyecto 802)*

3. *Capa de Red*. Esta capa tiene la finalidad de proporcionar la conectividad y la identificación del camino más óptimo para el envío de la información entre redes. Proporciona a la capa de transporte servicios que dividen los segmentos de información en *paquetes*, estos son mucho más complejos ya que contienen las direcciones lógicas o direcciones IP de los nodos que establecerán comunicación.

   Por esto, su funcionalidad debe abarcar el conocimiento de la topología de red utilizada y también conocer el caso en el que los equipos se encuentren en áreas geográficamente diferentes. Uno de los dispositivos de comunicación que tiene su funcionalidad en esta capa es el *router*[12] el cual puede dividir los datos en segmentos en pequeñas unidades las cuales serán re-ensambladas por la capa de red del computadora destino.

4. *Capa de Transporte*. Ofrece servicios a la capa de sesión aceptando paquetes provenientes de ésta, segmentándolos adecuadamente para su envío por medio de la red. La principal tarea de esta capa es la de garantizar que los datos sean enviados correctamente y que su envío tenga una correcta secuencia.

   En el caso de la existencia de circuitos virtuales, establece, mantiene y termina la conexión en dichos circuitos. Garantiza la transferencia de información y re-ensambla los segmentos en el nodo destino para su integración. Una vez que la información es recibida por el destino manda una notificación de recibido y garantiza que los datos enviados sean los mismos que los recibidos, en caso de la existencia de una duplicación, la capa de transporte se encarga de desecharla

5. *Capa de Sesión*. Esta capa permite que aplicaciones ubicadas en diferentes computadoras establezcan la conexión que definirá el enlace, aunado a esto las

[12] Dispositivo que interconecta segmentos de red, haciendo pasar datos por medio de redes tomando en cuenta la información generada en la capa de red.

actividades que realiza son: controlar y finalizar la conexión establecida para la comunicación; asimismo establece los lineamientos de conexión tales como protocolos, tiempos de envío y recepción.

La idea que se maneja de una comunicación por medio de una sesión es la de llevar a cabo una serie de peticiones entre aplicaciones ubicadas en diferentes redes por medio de protocolos específicos en este nivel. Aquí existen puntos de recuerdo en la transferencia de la información denominados ***checkpoints,*** que son registros los cuales permiten llevar un control de los datos trasmitidos correctamente y en caso de que la red falle, solamente habrá la necesidad de enviar los datos a partir del último checkpoint registrado.

6. *Capa de Presentación*. Utiliza técnicas especializadas de compresión y de codificación sirviendo como enlace con las capas inferiores del modelo OSI. Su principal funcionalidad es adecuar la información generada por el usuario por medio de su codificación, para poder ser enviados datos a través de los enlaces físicos de la red.

   La capa de presentación tiene el objetivo de interpretar, comprimir y adecuar el formato de los datos a las condiciones existentes. Existen algunos esquemas de conversión y de .encriptación que permiten a computadoras con diferentes sistemas operativos se puedan comunicar entre si.

7. *Capa de Aplicación*. Esta capa tiene una relación directa con el usuario convirtiéndose en el punto origen para cualquier envío de información. A pesar de no ofrecer servicios a alguna otra capa tiene funciones tales como identificar la disponibilidad de los elementos que participan en la comunicación, así como comprobar la sincronización de las aplicaciones utilizadas.

   Las aplicaciones que se manejan en este nivel tienen procesos característicos de comunicación que son controlados con protocolos, que estos a su vez, utilizan servicios de la capa de aplicación para estructurar el esquema de conexión.

2.4. El Conjunto de Protocolos TCP / IP

Un protocolo tiene la función de establecer procedimientos para la comunicación entre computadoras, en algunas ocasiones puede existir la unión de dos o más protocolos donde cada uno de ellos con base en el modelo de referencia *OSI,* actúan particularmente en cada nivel logrando una comunicación libre de errores e íntegra. Al trabajo conjunto de protocolos se le denomina "*pila de protocolos"*.

TCP/IP se ha convertido en el conjunto de protocolos estándar para la comunicación entre los diferentes tipos de computadoras. Una de las ventajas más claras es su utilización universal a través del *Internet*, logrando conectar computadoras con sistemas operativos diferentes y con gran variedad de elementos físicos.

La arquitectura *TCP/IP* se estableció con el objetivo de buscar esa homogeneidad mencionada, logrando su aceptación en cuatro niveles básicos; posteriormente serviría

como plataforma base para la estructuración del modelo de referencia OSI, donde cada una de estas capas corresponde a uno o mas niveles de este modelo. Las capas que mas se ven influenciadas por el conjunto de protocolos *TCP/IP* son la capa de *Aplicación, Transporte* y *Red.*

Esta pila de protocolos se ha adoptado como patrón en comunicaciones tanto en redes de área local como en redes de área extensa, por ello, otros protocolos se han incluido con el conjunto *TCP/IP* aumentando las capacidades de este conjunto de protocolos de comunicación. **(Ver Figura 2-10)**

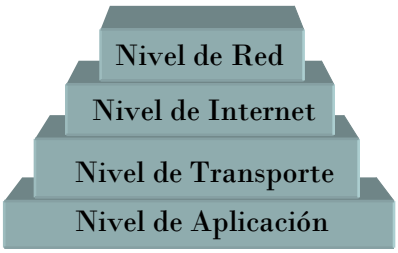


Figura 2-10. *Arquitectura TCP / IP*

- ***Nivel de Red.*** Hay una analogía directa con la capa física y de enlace de datos del modelo de referencia *OSI,* por lo tanto es un enlace directo con la arquitectura física y la capa de red que maneja direccionamiento de los datos a través de los medios físicos de comunicación.

- ***Nivel de Internet.*** Aquí existe una relación directa con la capa de red del modelo de referencia OSI, existiendo una gran cantidad de protocolos los cuales direccionan la información a través de la red, exactamente la funcionalidad que se maneja en el estándar OSI.[2]

  Cada protocolo tiene una función específica que es utilizada en el proceso de envío y recepción de datos, los cuales se mencionan a continuación:

  - *Internet Protocol* (**IP**). Es utilizado para direccionamiento y enrutamiento de datos por medio de una *comunicación sin conexión* o *connectionless.* Cada paquete enviado contiene información relevante que lo hace ser identificado a través de etiquetas que se van colocando a dicho paquete, tales como: *dirección origen y destino de las computadoras implicadas en la comunicación, un identificador del protocolo utilizado, un valor checksum*[13], *un campo TTL*[14]. Realiza el procedimiento de ensamblado y desensamblado de los paquetes en la red.

[13] Método utilizado para identificar errores existentes en el envío de datos. Se lleva acabo la suma de todas las unidades que conforman los datos en la máquina origen y se registra ese valor; la máquina destino vuelve a realizar la misma suma y los resultados se comparan, si los valores son iguales, no hay error en la información, de lo contrario, existen errores.

[14] *Time to Live* es un indicador que hace mención acerca del tiempo que debe estar cada paquete en la red en su proceso de envío, una vez que el dato es enviado el TTL se decrementa mientras no sea alcanzado el host destino, sí el TTL de un paquete termina, el paquete es eliminado completamente.

- Address Resolution Protocol (**ARP**). Antes de ser enviado un paquete de datos a través de la red, este debe incluir la dirección lógica y dirección física del nodo destino. El protocolo ARP puede solicitar la dirección física por medio del conocimiento de la dirección lógica; Con una consulta propia, la computadora origen trata de identificar si contiene información sobre la dirección física destino, en caso de que no contenga la información, lleva acabo una petición general (bro*adcast)* a todas las computadoras, de la cual, solo una responderá ofreciéndole dicha información que complementará los elementos necesarios para que el paquete pueda ser enviado.

- Reverse Address Resolution Protocol (**RARP**)**.** Este protocolo es utilizado cuando se desea obtener la dirección lógica de una máquina conociendo su dirección física. Un servidor ARP contiene información de las direcciones físicas existentes por medio de una base de datos; cuando se recibe una petición de resolución de dirección, el servidor ARP consulta la base de datos para identificar la dirección lógica solicitada.

- Internet Control Message Protocol (**ICMP**). Este protocolo es utilizado principalmente para establecer notificaciones de estado de la información una vez que ya ha sido enviada. Este tipo de mensajes son parte de los paquetes que se envían a nivel de Internet también llamados *datagramas*. (Ejemplos: tiempo de existencia excedido, petición de información, problemas de parámetros, destino inalcanzable, etc.).

- ***Nivel De Transporte.*** Esta capa tiene similitud con la capas de Transporte y Sesión del modelo de referencia OSI, ya que se encarga de establecer y finalizar la conexión en el proceso de comunicación. También ofrece servicios de transporte para dicha información que se conoce como servicio de extremo a extremo. A nivel de esta capa se manejan dos protocolos los cuales son utilizados conforme a las características de conexión necesitada.

  - Transmition Control Protocol (**TCP**). Protocolo *orientado a conexión* que establece una conexión que se le denomina simplemente sesión. Para lograr una conexión confiable, se establecen números de secuencia los cuales garantizarán que la información enviada llegue en correcto orden y que los datos enviados estén completos.

    El primer número que se define es el *número de secuencia* (*ISN)* que es simplemente un digito que se utiliza para monitorear el orden de los paquetes y llevar un control numérico de su flujo cubriendo la posibilidad de recuperación en caso de perdida.

    Cada nodo (origen y destino), debe generar su propio número de secuencia, siendo el número de secuencia destino dependiente del número de secuencia origen. Para lograr una sincronización en los números de secuencia en ambos lados de la conexión, se intercambian los segmentos donde están incluidos los ISN junto con un bit de control denominado *SYN,* una vez que son enviados mutuamente los ISN's, cada uno

de ellos debe ser notificado de la llegada correcta de los números de secuencia, el proceso es el siguiente:

1. El solicitante envía un paquete indicando el número de puerto que desea usar, y su número de secuencia inicial.
2. El destino notifica con su número de secuencia propio, que es el número de secuencia del solicitante más una unidad.
3. El solicitante recibe el número de secuencia del destino, y este confirma la llegada, regresando al solicitante el numero de secuencia mas uno.

Algunas de las especificaciones que debe tener un paquete en el protocolo TCP/IP para garantizar la fiabilidad de los datos son:

- Un puerto destino y origen TCP.
- Un valor de checksum para garantizar la integridad de los datos.
- Un número de notificación que indique que paquetes ya han llegado a su destino.

La finalidad de ocupar puertos en *TCP/IP* es la de llevar un registro de las aplicaciones utilizadas al mismo tiempo a través de la red. Así también el protocolo TCP/IP utiliza la herramienta llamada "*sliding window* ", en la cual por cada paquete enviado no se regresa una confirmación al destino, se espera una cantidad de paquetes establecida (tamaño de ventana) y se confirma su arribo correcto y en orden por el destinatario. En caso de que exista un error en el proceso de envío se re-envía los datos erróneos identificados.

User Datagram Protocol (**UDP**). Este protocolo utiliza una comunicación no orientada a conexión, sus funciones son las mismas en establecer y terminar las conexiones establecidas. Regularmente es ocupado en cantidades reducidas de información donde garantizar su integridad no es requerida. UDP utiliza puertos para registrar aplicaciones, pero no utiliza la misma asignación de puertos que TCP/IP.

- ***Nivel de Aplicación*.** En esta capa se manejan los protocolos que tienen la mayor interacción con el usuario, el direccionamiento y la administración de la red son manejados por protocolos y servicios específicos como correo electrónico, transferencia de archivos, etc. Siendo parte fundamental para la presentación de los datos al usuario.

  Post Office Protocol (**POP**). Protocolo que tiene la finalidad de gestionar y transferir mensajes de correo electrónico entre dos máquinas. El *puerto*[15] que generalmente utilizan es el *110* y un servidor POP puede ser accedido solamente a una bandeja de entrada.

  Simple Mail Transfer Protocol (**SMTP**). Protocolo utilizado para el transporte de mensajes a través de la red de datos. Para llevar acabo la comunicación se establece una conexión directa entre el emisor (cliente) y el receptor (servidor de correo

[15] Conexión física y lógica para el envío y recepción de datos.

electrónico) por medio de un programa cliente en el cual se utilizan comandos particulares para establecer un lenguaje de comunicación común.

File Transfer Protocol (**FTP**). Protocolo de conexión remota que utiliza TCP entre servidor y cliente en ambas direcciones; es un protocolo útil en el envío de grandes bloques de datos. Utiliza los puertos 20 y 21 que son utilizados para el envío de información y para el flujo de control respectivamente.

Internet Group Management Protocol (**IGMP**). Protocolo de manejo de grupo que es utilizado por máquinas cliente para reportar a los participantes de un grupo cliente con routers de multicast.

Point to Point Protocol (**PPP**). Protocolo de enlace de datos para la transmisión de paquetes TCP/IP sobre conexiones telefónicas entre un equipo e Internet.

2.5. Transmisión de Video Digital

El objetivo principal en la transmisión de video de seguridad es mantener una eficiencia adecuada y minimizar el impacto que pueda tener la transmisión en la red. El tráfico de video digital se caracteriza por ser constante, predictivo y estable, por ello es posible establecer una dimensión constante en el medio de transmisión para el flujo de este tipo de información.

Fundamentalmente un aspecto muy importante a tratar en la transmisión de video es el estado del *ancho de banda*, para este caso existe la forma de optimizarlo por medio de técnicas especializadas de envío basadas en la transmisión sobre IP.

Como ya se mencionó con anterioridad, la comunicación en una red de datos basadas en el protocolo de comunicación IP es a través del uso del datagrama IP, que es la unidad básica para el envío de información, dentro de ellas está contenidas información del emisor y receptor. Existen tres tipos de datagramas IP en función del tipo de dirección destino:

- *IP Unicast*. El receptor es el único destinatario, todos los posibles datagramas IP enviados serán procesados en una única dirección destino.

- *IP Broadcast*. El receptor se vuelve en un conjunto de equipos los cuales procesaran una misma información al mismo tiempo.

- *IP Multicast*. Se compone de un conjunto de direcciones receptoras finales las cuales esperan datagramas de esa dirección en específico.

El envío de la misma información a múltiples usuarios, lleva consigo una serie de beneficios para el rendimiento de la red de datos si se utiliza eficientemente tecnología Multicast. Considerando como ejemplo el envío de video integro por un canal de comunicación se necesitaría un ancho de banda disponible de 1.5 Mbps.

Hablando de la comunicación unicast, el servidor enviaría segmentos de video por cada cliente, esto daría como resultado un requerimiento mucho mayor de ancho de banda donde cada cliente necesitaría, por cada paquete de video, 1.5 Mbps para su visualización, es decir para 33 clientes es posible que el ancho de banda total requerido en la red fuera de 49.5 Mbps (solamente para un mismo paquete), obviamente se vería afectado el rendimiento general de la red por muy moderna que esta sea. Aunado a esto, los dispositivos de enlace tales como switches o routers estarían enviando información repetida por sus canales haciendo que peticiones de envío de otra índole sean descuidadas. **(Ver Figura** 2-11**)**

La información que encontramos en Internet está basada en la comunicación unicast, es decir, que el destinatario de la información tiene una dirección IP específica. Por tanto este tipo de comunicación es una buena alternativa en aplicaciones habituales tales como *www* o *ftp*, sin embargo se vuelve ineficiente cuando se desean trasmitir gran cantidad de información tales como video.

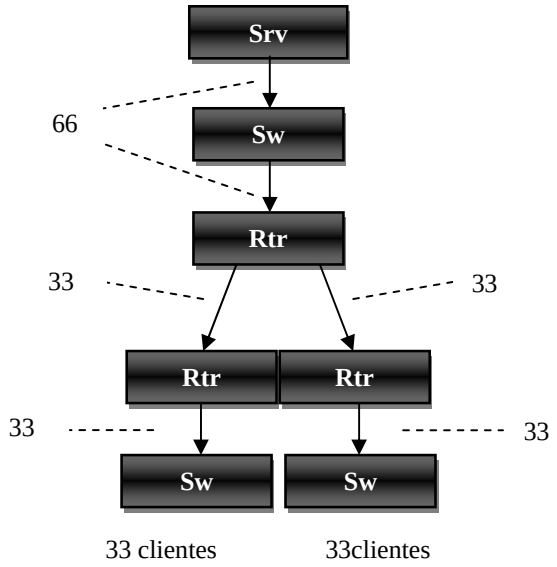


Figura 2-11- *Red Unicast. (Srv:Server, Rtr:Router, Sw:Switch)*

Por otro lado en un ambiente multicast, el objetivo es enviar un simple segmento de video para un grupo de observadores destinatarios; el segmento de video se replica para el número de solicitudes requeridas por los elementos que conectan a la red (routers y switches) y así satisfacer a los clientes que necesiten la visualización del video. Con este método solamente se utilizarán 1.5 Mbps fijos para el proceso permitiendo el resto de ancho de banda para otros usos.

Una característica importante en este tipo de comunicación es que el servidor de video origen solamente conoce una única dirección destino de un grupo en particular y ya que el envío de información no es individualizada, cualquier computadora cliente puede acceder o dejar el grupo multicast sin problema alguno. **(Ver Figura 2-12)**

Un equipo cliente puede pertenecer a más de un grupo destino, sin importar la localización geográfica o el número de clientes ya existentes dentro del grupo final.

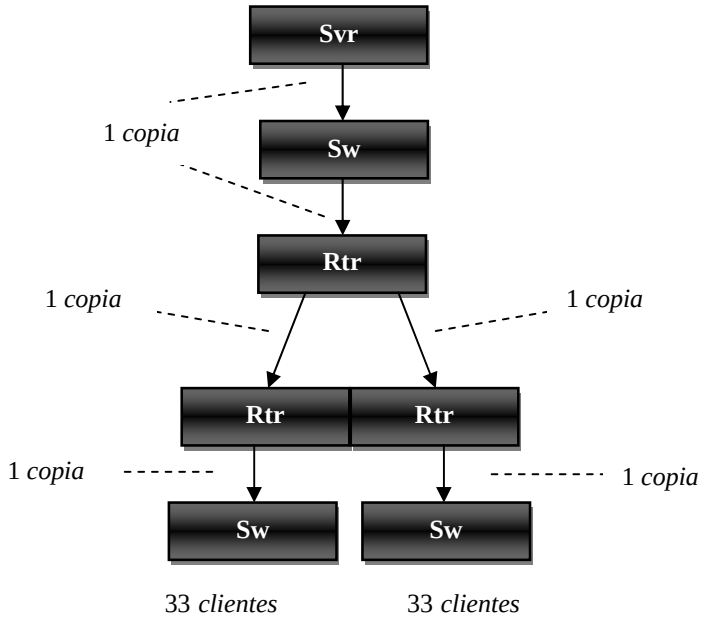


Figura 2-12. *Red Multicast (Srv: Server, Rtr: Router, Sw: Switch)*

Las direcciones de los grupos destinos son identificados por direcciones IP *clase D*[16]. Existen dos tipos de grupos:

- **Permanentes**. Son grupos estandarizados (fijos) los cuales contienen equipos clientes que no dependen de esta permanencia.
- **Transitorios**. Grupos generados según las necesidades de comunicación.

Representado en algunos pasos, el proceso de Multicasting en el envío de video es el siguiente:

1. El cliente manda un mensaje de unión *IGMP*[17] al router multicasting más cercano, la MAC destino es incluida en un grupo cliente por medio de una dirección IP del tipo D.
2. El router admite la petición y utiliza un protocolo de multicasting (DVMRP, MOSPF, PIM, CBT) para incluir el segmento donde se encuentra el cliente nuevo en la distribución.

[16] Clasificación de una dirección IP que en su primer octeto contiene la secuencia 1110, por lo tanto las direcciones posibles 224.0.0.0 a 239.255.255.255.
[17] Internet Group Management Protocol

3. Las futuras distribuciones de video generado serán controladas por el router de multicasting para la red de ese cliente. Cabe mencionar que la dirección MAC destino corresponde a la dirección IP tipo D del grupo.
4. Un switch recibe el paquete multicast y examina su propia tabla de distribución para identificar al destino, en caso de que este no exista, el paquete será enviado a todos los puertos dentro del domino broadcast.
5. Con IGMP (versión 2) el cliente puede dejar de pertenecer al grupo enviando un mensaje IGMP a su router de distribución respectivo. En la primera versión de IGMP, el cliente dejaba la sesión, y el router identificaba su ausencia por medio de una búsqueda en su renovación de distribución de todo el grupo, cuando no recibía respuesta alguna del cliente, era el indicador para dejar de enviar copias hacía esa dirección MAC. Una identificación se hacen continuamente en búsqueda de actualizaciones en los miembros de los grupos, cada máquina cliente retarda su contestación a la petición un determinado tiempo, esto con la finalidad de no saturar el canal con reportes simultáneos.

Trasmitiendo por broadcast se abarca un gran número de equipos los cuales recibirán la señal de video sin necesitarla, es decir, cada cliente se verá interrumpido por cada mensaje de broadcast. Hablando un poco de los diferentes tipos de broadcast, se clasifican por medio de sus alcances:

- **Direcciones broadcast limitadas**. Contempla todos los octetos como unos (255.255.255.255), se usa en redes que soportan broadcasting, abarca todos los destinos de una subred y no más allá.

- **Direcciones broadcast de red.** Se utiliza en una red sin subredes, en los bits que corresponden a las computadoras (*host*s) se colocan unos, por lo tanto aquí se abarcarán todos los hosts destino de una red en particular.

- **Direcciones de broadcast de subred**. Se pone en unos la parte destinada para los host de la dirección local.

- **Broadcast a todas las subredes.** Se coloca toda la parte local en unos.

La transmisión de archivos multimedia viaja a través de la red con base en dos tiempos de distribución: En *vivo y Bajo demanda.*

La transmisión en vivo se lleva a cabo en el mismo intervalo de tiempo que en el emisor original, ofreciendo audio y video reales en la computadora cliente sin importar su ubicación geográfica. Este tipo de transmisión es realizada tanto por métodos de distribución Unicast en Internet e Intranet y para distribuciones multicast solamente en intranets ya que la disponibilidad de los enlaces de distribución en Internet no pueden ser controlados directamente. La transmisión bajo demanda se basa en la distribución de video pre-grabado y almacenado en un servidor de video, el cual será consultado cuando este se necesite. Esta también es llevada a cabo en la Internet y en redes locales en una distribución unicast, sin embargo la posibilidad de hacerlo en distribuciones multicast no ha alcanzado resultados aceptables que lo definan como una posibilidad real.

2.6. Consideraciones de Transporte

Cuando el video es transportado sobre IP, existen factores que pueden afectar la integridad de la información para lo cual existen diversas opciones para controlar efectos negativos para el video:

Traffic Shaping.

Son técnicas utilizadas para hacer sencillo el manejo de video en la red. El objetivo principal es reducir diferencias considerables en el bit rate de un grupo de streams. Con un bit rate controlado mayor cantidad de video puede ser transmitido. En el caso MPEG, frame I requiere mucho más datos que un frame B; sí el codificador MPEG envía la información exactamente como fue creada, el bit stream tendrá sobresaltos cuando un I frame sea creado.

Los codificadores MPEG más recientes ya incluyen técnicas para regular el bit rate generado por medio de más canales para el enlace de datos y así lograr contener los cambios bruscos de rates. Sin embargo *shaping* debe ser utilizada cuidadosamente ya que puede generar retrasos intolerantes en aplicaciones con video.

Buffering

Se trata de una colección de memoria utilizada de forma temporal para almacenar información. En redes IP donde los niveles de utilización de ancho de banda están cambiando considerablemente, resulta útil almacenar imágenes para posteriormente ser recreadas. Para MPEG, buffering es utilizado para realizar estimaciones de movimiento así también en la decodificación para utilizar la interpretación.

Los buffers de gran capacidad ofrecen un respaldo en retrasos de llegada de los frames así como de manera desordenada. Buffering puede ser de gran ayuda para realizar funciones tales como traffic shaping o corrección de errores.

Ciertamente, la utilización de buffering también trae efectos negativos en algunas aplicaciones en las cuales la interactividad es utilizada, por ejemplo la videoconferencia. Los buffers pueden aumentar el costo del equipo para codificadores o decodificadores.

Firewalls

Con la existencia de firewalls a nivel perimetral o de manera personal, la transmisión del video puede verse afectada de dos diferentes maneras. Primeramente el firewall puede bloquear a usuarios de acceder al origen del video. Otra forma es la interferencia del trafico por el bloque de paquetes UDP, usualmente este tipo de trafico es bloqueado ya que es susceptible de ser modificado por paquetes ajenos.

Multiplexing

En un sistema distribuido de video con varios orígenes, es necesaria la utilización de multiplexores para la combinación de señales. La salida de un multiplexor pude ser una sola señal que contenga múltiples streams de video, multiplexing puede ser utilizado por muchas razones:

- Un único stream es más sencillo de transportar y manejar que una gran cantidad de streams pequeños.
- Cuando distintos rates de streams son combinados, el ancho de banda puede ser utilizado más eficientemente por la correspondencia entre picos y valles en cada stream.
- Cuando las cantidades de ancho de banda están delimitadas, es conveniente configurar tantos streams como sea posible para completar la capacidad del canal.

El proceso de multiplexing puede ocasionar pequeños retrasos en las señales de video. Así también la utilización de multiplexores generará un costo mayor en el origen ya que la mayoría de los decodificadores incluyen sus propios demultiplexores.[1]

En este capítulo se mencionó la teoría básica sobre redes de computadoras. Primeramente se señaló la clasificación de una red de acuerdo a su extensión geográfica, a la manera de compartir su información y a su arquitectura. En segundo lugar se definieron las topologías de red existentes y se identificaron las ventajas y desventajas de cada una de ellas así como algunos criterios para su utilización. Posteriormente se incluyó una descripción del modelo OSI donde se mencionó su importancia en el proceso de comunicación y como su estructura está definida por capas con funciones particulares. Finalmente, se aprendió la importancia del conjunto de protocolos TCP/IP para establecer procedimientos de comunicación libres de errores así como la forma de transmitir video y algunas consideraciones a tomar en cuenta.

La transmisión de información es un aspecto importante a considerar en el diseño de un sistema de videovigilancia, con los conceptos abarcados en este capitulo, la idea de transmitir video digital a través de este tipo de medios basados en IP se fortalece por lo magníficos resultados obtenidos en el campo informático. Así, llega el momento de estudiar otro elemento indispensable en un sistema de esta naturaleza como es el almacenamiento.

Capítulo 3

Medios de Almacenamiento

Los medios de almacenamiento son unidades físicas de un sistema que tienen la finalidad de conservar permanentemente información; la integridad y disponibilidad son características esenciales para el almacenamiento de datos. Actualmente, los requerimientos de almacenamiento han ido en incremento, por esto, se han logrado opciones tecnológicas acordes a necesidades específicas diferentes, a continuación se desarrollan algunas opciones.

Por la cantidad de información que se almacena, los dispositivos de almacenamiento se pueden englobar en dos grandes grupos: *primarios* y *secundarios.*

Se hace mención como medios de almacenamiento primarios a aquellos dispositivos que sirven de almacenamiento temporal para programas y operaciones de procesamiento; antes que cualquier dato o programa sea operado, debe ser trasmitido a un medio de almacenamiento primario.

Las computadoras tienen dos tipos de medio de almacenamiento primario *ROM*[1] y *RAM*[2], los datos utilizados por cualquier procesamiento son almacenados en reservas primarias hasta que son requeridos por el procesamiento, durante el proceso los resultados intermedios y finales de todas las operaciones lógicas son recabados para posteriormente enviarlos a un medio de almacenamiento secundario.

Por lo tanto un medio de almacenamiento secundario es un dispositivo para almacenar definitivamente información ya procesada que será almacenada por medio de un proceso mecánico de escritura en dos tipos de tecnologías: *Ópticos y Magnéticos.* Algunas características que definen a un medio de almacenamiento secundario son su gran capacidad de almacenamiento y altas velocidades en transferencia de información.

En el ámbito de la videovigilancia, el almacenamiento secundario es el elemento con mayor valor ya que es el pilar para el registro y permanencia de eventos. Existen diversas opciones para brindar respaldo con dispositivos de almacenamiento tales como SAN y NAS diseñados específicamente para tareas de resguardo masivo.

La planeación de un buen esquema de grabación permitirá la utilización eficiente de las unidades, con contenidos recientes y útiles para el usuario. La cantidad de video almacenado está en función de las capacidades del propio disco duro. Es importante tener presente que el almacenamiento es lo más costoso de una solución de videovigilancia ya que las cantidades de información originadas son demasiadas por lo tanto gran cantidad de unidades para este fin se vuelven necesarios.

.

[1] Memoria de solo lectura que contiene intacta su información almacenada, regularmente es utilizada para consulta sobre configuraciones físicas de la computadora.

[2] Memoria de acceso aleatorio donde se puede leer y escribir, se utiliza principalmente para almacenar resultados intermedios y datos no permanentes.

3.1 Dispositivos Magnéticos

Entre los medios de almacenamiento magnéticos más conocidos se encuentran los discos duros, disquetes y las cintas magnéticas. La forma en que operan este tipo de tecnologías es a través de campos magnéticos en materiales, donde las partículas reaccionan a este efecto orientándose a determinadas posiciones que definen a la información.

El **disco duro** es una pila de discos (*platters*), donde se almacena información magnéticamente, cada disco tiene dos superficies posibles para almacenamiento: *superior* e *inferior*. En cada superficie existen pequeños elementos capaces de ser magnetizados para representar la información lógicamente, logrando así la representación de la información por medio de bits (ceros y unos). Todos los discos están acoplados en un eje de rotación común el cual servirá como base de giro.

Existen elementos llamados cabezas (*heads*) que están ensambladas en pila y son las encargadas de la lectura y escritura de la información en los discos, generalmente, cada disco duro incluye una cabeza por cada superficie, por lo tanto el número de discos es la mitad del número total de cabezas; colocando una cabeza por cada superficie se puede lograr una disminución en el tiempo de traslado lineal que originaría escritura en ambas caras del disco.

Las cabezas pueden trasladarse al interior o exterior del disco ya que están soportadas por un brazo mecánico, aunado a esto, la pila de discos gira para poder acceder a cualquier parte física del disco.

El proceso de lectura/escritura no se hace por medio del contacto físico del disco sino a través de una pequeña bobina de hilo que se acciona dependiendo del campo magnético detectado, produciendo una cantidad de corriente acorde a ese valor para ser representada como dato por la parte electrónica de cualquier disco duro.

En cada cara de disco existen delgados circuitos concéntricos llamados pistas (*tracks*), las cabezas se mueven del exterior al interior a través de las pistas, con base en esto, se origina el terminó *cilindro* el cual representa al par de pistas en caras opuestas de un disco; cuando un disco duro contiene múltiples discos, un cilindro incluirá la mismas pistas de todos los discos en fila.

Cada pista es dividida en *sectores* los cuales son las unidades mínimas de información que se puede leer o escribir en un disco duro, comúnmente cada sector esta compuesto de 512 bytes; cada pista del disco está dividida varios sectores, así la dimensión de las pistas exteriores es mayor que las interiores. **(Ver Figura 3-1)**

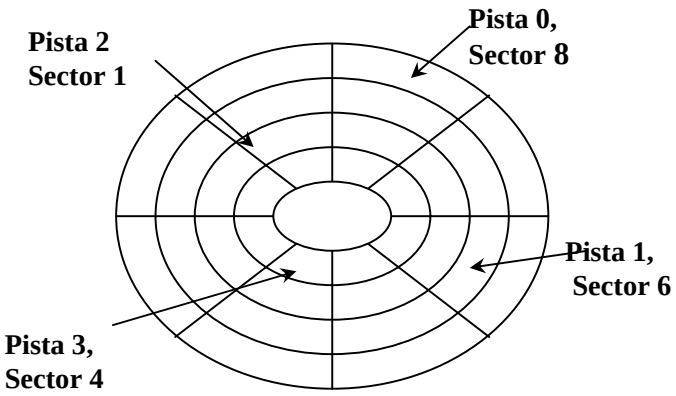


Figura 3-1. *Pistas y sectores en disco duro*

NOTA: Las cabezas y cilindros se empiezan a enumerar desde cero y los sectores desde uno.

La forma de obtener la capacidad de un disco duro es por medio de sus elementos ya mencionados; por ejemplo para un disco duro de 6,253 cilindros, 16 cabezas y 63 sectores, se puede obtener su capacidad total haciendo un producto entre estos valores, para este ejemplo, se tendría como resultado 6, 303,024 sectores, si cada sector almacena 512 bytes entonces la capacidad máxima del disco duro es de 3, 227, 148, 288 bytes ≈ 3 Gbytes.

La eficiencia de un disco duro se mide con base en tiempos específicos recabando información contenida en él, existen 3 tiempos indicadores fundamentales:

- Tiempo de búsqueda. Es el tiempo que tardan las cabezas en encontrar la pista donde se encuentra la información a partir de su estado actual, hoy en día estos tiempos se han reducido considerablemente logrando magnitudes de 2 milisegundos en una búsqueda entre pistas adyacentes, así como tiempos de búsqueda entre el intervalo de 10 milisegundos y 15 milisegundos para distancias no adyacentes.

- Latencia. Una vez definida en su posición la cabeza lectora, debe haber un tiempo de espera para que el disco logre colocar el sector deseado debajo de la cabeza lectora, los tiempos de latencia promedio equivalen al tiempo que tarda el disco en lograr media revolución, los discos actuales alcanzan 10 000 revoluciones por minuto, generando una reducción considerable en el tiempo de latencia.

- Transmisión de datos. Este tiempo toma como base la velocidad de transmisión de los datos una vez ya encontrados, es decir, la interfaz por la cual el disco duro se comunica

con la tarjeta madre para el procesamiento, esto depende del tipo de conexión que utilice el disco.

Las unidades de disco en general pertenecen a una clasificación llamada *dispositivos de almacenamiento de acceso directo*, que son aquellos dispositivos para los cuales su información puede ser consultada sin importar la ubicación de los datos, al inicio, en medio o al final los tiempos de acceso serán generalmente los mismos. Los *dispositivos de acceso en serie* son otra clasificación en medios de almacenamiento que se caracterizan por acceder a los datos en forma serial, en otras palabras, información ubicada en el centro del dispositivo será consultada una vez que los datos iniciales hayan sido contemplados en el proceso de búsqueda.

La **cinta magnética** es otro dispositivo con material magnetizable el cual contiene en una cara, cinta de plástico base para el material ferromagnético; la información se almacena en forma de pequeñas marcas sobre registros paralelos y también en pistas horizontales al eje longitudinal de la cinta; es una buena alternativa para almacenar gran cantidad de información en forma secuencial que no requiera ser accedida en un segmento especifico, comúnmente se utiliza en el respaldo de información para unidades de disco duro.

Los registros de la cinta son separados por espacios en blanco los cuales permiten identificar la posición de cada registro, cuando un registro está siendo analizado, la cinta magnética detiene su movimiento para que pueda ser contemplado el registro adecuadamente y no reinicia su actividad de movimiento hasta que el registro actual no ha sido completamente leído. La longitud de los registros es variable, por esto, la posibilidad de registros pequeños es latente, esto ocasionaría que la cantidad de espacios en blanco aumente proporcionalmente ocasionando que el movimiento de la cinta sea constantemente detenido; una solución a esta situación es conjuntar registros pequeños para generar un bloque mayor de información. **(Ver Figura 3-2)**

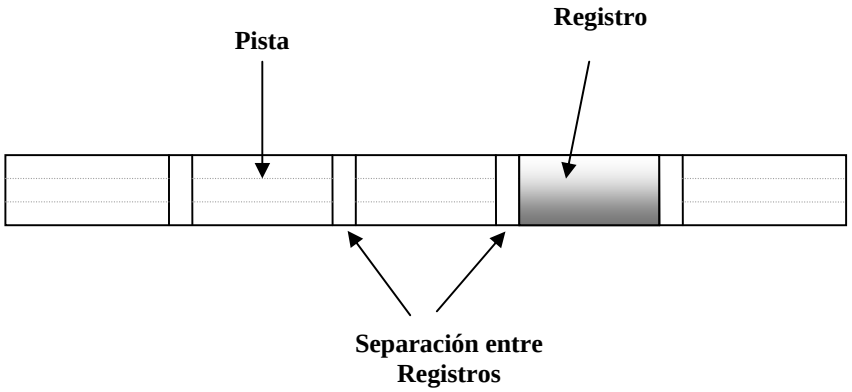


Figura 3-2. *Elementos de una cinta magnética*

Una cinta magnética común contiene 9 pistas donde cada una de ellas contiene nueve cabezas de lectura y escritura, una de las pistas es ocupada para paridad, en el resto el proceso de lectura se realiza por patrones magnetizados que inducen pulsos eléctricos a bobinas de lectura que conforman los datos a procesar; de igual forma el proceso de escritura se realiza a partir de pulsos eléctricos que magnetizaran la superficie de la cinta con información.

Existen algunas tecnologías las cuales se han ido desarrollando con base en necesidades de almacenamiento cada vez más requeridas, las tres tecnologías principales son LTO, SDLT y DLT.

- *LTO (Linear Tape Open)*. Es una tecnología de almacenamiento desarrollada en conjunto por *HP*, *IBM* y *Certance.* Está tecnología ha sido desarrollada durante algunos años logrando en el 2004 que la tercera generación de LTO estuviera disponible para su uso, velocidades de transferencia de datos de 80 a 160 Mbps y capacidades de almacenamiento mayores a los 800 Gbytes fueron alcanzadas superando a generaciones predecesoras que almacenaban de 200 a 400 Gbytes. Sin embargo actualmente existen nuevas generaciones en proceso de desarrollo; para la cuarta generación se planea lograr como máxima capacidad de almacenamiento 1.6 Tb (*Terabytes)* y una transmisión de 240 Mbps; en la quinta generación se espera alcanzar los 3.2 Tb de almacenamiento y velocidades cercanas a los 360 Mbps y finalmente una sexta generación con 6.4 Tb y 540 Mbps.

- *DLT (Digital Linear Tape)*. Tecnología usada para el almacenamiento de información que utiliza un algoritmo especial de compresión conocido como *DLZ1 (Digital Lempel Ziv 1)* que facilita el almacenamiento masivo y recuperación de archivos de grandes dimensiones a grandes velocidades. En la unidad de DLT, los datos son escritos en la cinta en pistas, algunas cintas pueden almacenar de 20 a 40 Gb de datos sin comprimir y de 40 a 80 Gb de datos comprimidos.

- *SDLT (Super Digital Linear Tape).* Es una extensión de DLT pero con más capacidades en almacenamiento, las cintas de este tipo pueden almacenar hasta 300 Gbytes de datos no comprimidos o hasta 600 Gbytes de datos comprimidos, convirtiéndolo en una alternativa aceptable para el almacenamiento masivo.

Existen tanto características positivas como negativas para las cintas magnéticas las más significantes serían:

Ventajas:

- Una cinta magnética es de menor costo a un disco y las dimensiones son mucho menores a las de otros dispositivos.
- A pesar de sus dimensiones, es posible grabar una gran cantidad de datos en ella, hasta 800,160, 625 caracteres en cada pulgada.

Desventajas:

- El acceso directo es definitivamente imposible ya que para acceder a un registro intermedio habrá que recorrer forzosamente los primeros registros, haciendo los tiempos de localización de información relativamente altos.
- Partículas de polvo y suciedad pueden afectar físicamente a la cinta, originando una perdida de información irreversible, por ello es fundamental llevar un control cuidadoso de esta y no exponerla a cambios bruscos de temperatura.

El **disco flexible** es otro medio de almacenamiento magnético que actualmente ha sido desplazado por las nuevas tecnologías ya adoptadas pero fue base importante de almacenamiento en equipos portátiles y computadoras personales por más de 20 años.

La idea general de funcionamiento es la de leer y escribir datos en una pequeña base metálica cubierta por plástico, similar a un cassette de audio, ambos lados del disco contienen esta composición de elementos que duplican su capacidad de almacenamiento.

El disco flexible incluye el concepto de pistas en sus componentes que son arreglos de círculos concéntricos los cuales permiten acceder a un archivo determinado sin tener que hacer una búsqueda secuencial, por medio de cabezas lectoras que se posicionan en la pista correcta.

De igual manera que en el disco duro, las pistas están enumeradas y se dividen en bloques denominados sectores.

Conociendo el número de pistas y sectores se puede saber la capacidad del disco, que se limitan a 1.44Mb y en otras épocas a 160Kb y 720 Mb

Capacidad = (# caras) (# pistas) (# sectores) (capacidad del sector)

A continuación se puede observar un cuadro comparativo de capacidad de almacenamiento para un disco flexible. **(Ver Tabla 3-1)**

Tamaño	5 1/4	5 1/4	3 1/2	3 1/2
Capacidad	360 Kb	1.2 Mb	720 Kb	1.44 Mb
Pistas	40	80	80	80
Sectores/Pista	9	15	9	18
Cabezas	2	2	2	2
Rotación/min	300	360	300	300

Tabla 3-1. *Capacidades de Almacenamiento Discos Flexibles*

3.2 Dispositivos Ópticos

Esta técnica de almacenamiento vino a revolucionar la forma de almacenar gran cantidad de datos digitales en unidades completamente portables. El primer acercamiento se hizo con los discos compactos de música (*CD*) alrededor de la década de los ochenta, la información es grabada por medio de una tecnología óptica de almacenamiento por láser.

A grandes rasgos, un haz láser va identificando o generando, proceso de lectura o escritura respectivamente, orificios en la superficie del disco de material plástico, cubierta a su vez, por una capa transparente que la protege de polvo y suciedad; este principio es el mismo que se utilizó en los antiguos discos de vinilo, teniendo como diferencia, que es información digital la almacenada, no analógica; y que el lector de información es un láser emisor variable.

En un disco óptico se grabará la información en forma secuencial como si se tratará de una cinta magnética, donde los datos de inicio están alojados en una espira que comienza en el interior y termina en el exterior; aunado a esto, existen divisiones lineales conocidas como sectores los cuales hacen la identificación de zonas mucho menos complicada y se identifican con una numeración consecutiva: *sector 0, sector 1, sector 2, etc.*; sin embargo, el acceso a cierta información siempre será secuencial, ocasionando que los tiempos de acceso sean altos.

El dispositivo que se encargará de la lectura de los datos para un disco compacto es un láser de baja potencia; dicha luz emitida al alcanzar la superficie del disco detecta sus deterioros (*orificios)* que tienen dimensiones extremadamente pequeñas: *profundidad = 0.12 micras, anchura = 0.6 micras*[3], entre los orificios existen partes planas denominadas *mesetas* que no representan información alguna. La diferencia entre un orificio y una meseta estriba en que una meseta refleja la luz láser recibida mientras que los orificios la dispersan, la luz reflejada es enviada a un fotodiodo que capta las variaciones recibidas.

Los datos en un disco compacto están almacenados cíclicamente, entonces si se desea leer datos en forma adecuada deben ser leídos todos a una misma velocidad por el láser. En un movimiento circular la velocidad angular que alcanzan todos los puntos no son las mismas, la rapidez dependerá de la distancia existente del centro de giro, por lo tanto entre más alejado este un punto de su centro más rápido girará. Definitivamente se necesita que el disco varíe la magnitud de giro dependiendo al sector que necesite leer para lograr una lectura de pistas siempre constante.

Por lo tanto la clasificación de los discos ópticos es:

1. *Discos Compactos de Lectura y Escritura*
2. *Discos de Video Digital*

[3] Unidad de longitud equivalente a una millonésima parte de un metro, se abrevia **μm**

Discos Compactos de Lectura y Escritura

CD – R. Disco compacto de solo lectura que su información es generada y almacenada desde su fabricación, siendo inalterable por el usuario. Generalmente se utilizan para almacenar documentación, y controladores de tecnologías y aplicaciones particulares. Anteriormente si se deseaba duplicar la información contenida, era necesario hacer la petición directamente con el fabricante. Actualmente existe la posibilidad de reproducir una copia por medio de unidades ópticas de lectura y grabación (*quemador).*

CD-RW. Disco compacto que permite escribir y leer su contenido múltiples ocasiones, el cambio de propiedades ópticas en su superficie son la base en esta tecnología. Una de las ventajas más notorias es la posibilidad de actualizar los datos contenidos, cuantas veces sea necesario y su reutilización constante. Naturalmente su costo a razón del disco de solo lectura se incrementa considerablemente.

Las dimensiones entre pistas adyacentes para un disco compacto son de *1.6 micras,* teniendo una anchura de *0.6 micras.* **(Ver Figura 3-3*)***

Figura 3-3. *Superficie de un disco compacto*

Discos de Video Digital

Las cantidades de información y las características de los datos almacenados han originado la creación de otros dispositivos de almacenamiento denominados DVD (*Digital Versatile Disc)*, que alcanzan almacenamientos mucho mas grandes (hasta 25 veces mas información) teniendo las mismas dimensiones y aspecto de un disco compacto normal. La forma de lograr estas magnitudes de almacenamiento bajo un mismo espacio es el uso de ambas caras del disco y en algunos tipos dos capas por cara.

Las cantidades de información de almacenamiento alcanzadas por el DVD va desde los 4.7GB hasta los 17 GB. Por esto, su creación fue para almacenar películas

principalmente; sin embargo actualmente un DVD puede contener **DVD-Video** *(video y audio),* **DVD-Audio** *(audio de alta calidad)* y **DVD –Data** *(múltiples datos).*
Dependiendo en su capacidad de almacenamiento a través de sus capas y el número de lados que utilizan, estos discos son clasificados.

DVD5: Un lado para almacenamiento, una capa simple, 4.7 GB de almacenamiento posible.
DVD9: Un lado para almacenamiento, dos capas, 8.5 GB de almacenamiento posible.
DVD10*:* Dos lados para almacenamiento, una capa simple por lado, 9.4 GB de almacenamiento posible.
DVD14: Dos lados para almacenamiento, capa doble de un lado, capa simple de otro, 13.3GB de almacenamiento posible.
DVD18: Dos lados para almacenamiento, capa doble por ambos lados, 17.1GB de almacenamiento posible.

Existen dos estándares principales para discos versátiles de video, *DVD –R* y *DVD +R,* soportados por **DVDForum**[4] y **DVD+RW Alliance**[5] respectivamente. La razón de la existencia de dos entidades de estandarización se debido a que el costo de licenciamiento de tecnología era muy alto por parte de DVDForum por lo que se busco crear un estándar con costos de licenciamientos menores. Como DVD+RW Alliance no cubre las normas establecidas por DVDForum no se les permite usar su logo identificador (DVD), por lo tanto estos últimos utilizan un propio logo que los identifica comercialmente (RW).

Definitivamente el + y – son estándares similares que han coexistido mutuamente, casi todos los lectores pueden leer ambos formatos, llevando así los dos logos posibles.

DVD-R y **DVD-RW**

DVD –R no es un formato reescribible y es compatible con el 93% de los reproductores de DVD.
DVD –RW es un formato reescribible y es compatible con el 80% de los reproductores de DVD.

DVD+R y **DVD+RW**

DVD +R no es un formato reescribible y es compatible con el 89% de los reproductores de DVD.
DVD +RW es un formato reescribible y es compatible con el 79% de los reproductores de DVD.

[4] Asociación internacional de fabricantes de hardware, firmas de software y abastecedores de contenidos de discos versátiles de video, que tiene por objetivo intercambiar y diseminar ideas e información para productos DVD.
[5] Alianza realizada por compañías de dedicadas al almacenamiento óptico y fabricantes de electrónica Dell, Hewlett-Packard Company, MCC/Verbatim, Philips Electronics, etc., que buscan desarrollar una compatibilidad universal en el formato DVD para permitir convergencias transparentes entre computadoras personales y productos electrónicos.

La velocidad de transferencia de los datos está dado por múltiplos de 1350 KB/s, por lo tanto una unidad lectora de 16x permite una transferencia equivalente: 16 x 1350 = 21.09 MB/s, esto lo hace mucho más eficiente a las velocidades alcanzadas por un CD común que son múltiplos de 150 KB/s.

Las dimensiones entre pistas adyacentes para un DVD es de 0*.74 micras*, teniendo una anchura de *0.4 micras.* Ya que las dimensiones manejadas son definitivamente más pequeñas, la capacidad de almacenamiento para un DVD es considerablemente mayor con respecto a un CD. **(Ver Figura 3-4** *)*

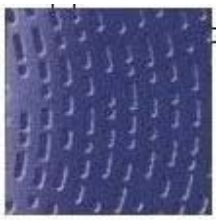


Figura 3-4. *Superficie de un DVD.*

Por lo tanto, los dispositivos de almacenamiento óptico ofrecen un gran número de ventajas, una de las de más peso es la gran capacidad de almacenamiento que las caracteriza, no se ven afectados por campos magnéticos, la humedad y el calor, son resistentes a los golpes mientras su superficie no se vea deteriorada considerablemente.

3.3 Sistema de Almacenamiento Masivo (RAID)

Redundant Array of Inexpensive Disks es un arreglo de múltiples discos duros independientes que incrementan considerablemente el desempeño a comparación de un *SLED*[6]. Un sistema de discos en RAID mejora el rendimiento de entrada y salida para una computadora que si solamente utilizara una única unidad de almacenamiento, sin embargo, dicho arreglo es percibido por la computadora como una única unidad de almacenamiento.

Un sistema RAID mejora el almacenamiento de los datos y garantiza la disponibilidad de éstos debido a su capacidad a tolerancia a fallos que una unidad de almacenamiento simple no tiene. Así también, datos perdidos a causa de una falla en algún disco duro pueden ser recuperados de las otras unidades restantes que conforman el arreglo. Comercialmente RAID tiene cinco modelos para el almacenamiento de la información, cada uno con capacidades eficientes de resguardo y recuperación en caso de fallas.

RAID maneja algunos conceptos como base de su estructura física.

- Disk Striping. Esta técnica escribe datos a través de múltiples discos, segmentando cada unidad de almacenamiento en partes las cuales pueden tener tamaño variable. La

[6] *Single Large Expensive Disks* es el tradicional arreglo de discos duros usados en mini computadoras y mainframes. Estos discos fueron utilizados a la mitad de los años sesentas hasta finales de los ochentas.

segmentación es colocada de manera secuencial a través de todos los discos que conforman el espacio total.
Por ejemplo, en un arreglo de cuatro discos, el segmento 1 será escrito en el disco 1, el segmento 2 será escrito en el disco 2 y así sucesivamente. Con esto disk striping aumenta el desempeño ya que se accederán a múltiples unidades.
(Ver Figura 3-5)

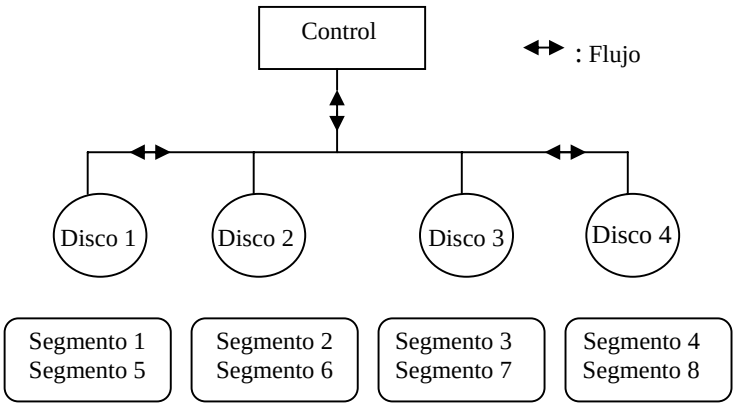


Figura 3-5. *Sistema Disk Stripping*

- Disk Spanning. Esta técnica permite a múltiples unidades de disco funcionar como una gran unidad; permite superar la carencia de espacio en disco y simplifica la forma de almacenamiento combinando los recursos existentes. Por ejemplo, 4 discos duros de 400 MB cada uno, pueden ser combinados para ser identificado por el sistema operativo como una simple unidad de 1600 MB.

  Para que realmente exista una ganancia en el rendimiento, los discos lógicos deben tener la misma capacidad y deben ser contiguos. Por ejemplo los discos lógicos 1 y 2 pueden ser configurados como spanning a diferencia de los discos lógicos 1 y 3 no podrían serlo.**(Ver Figura 3-6)**

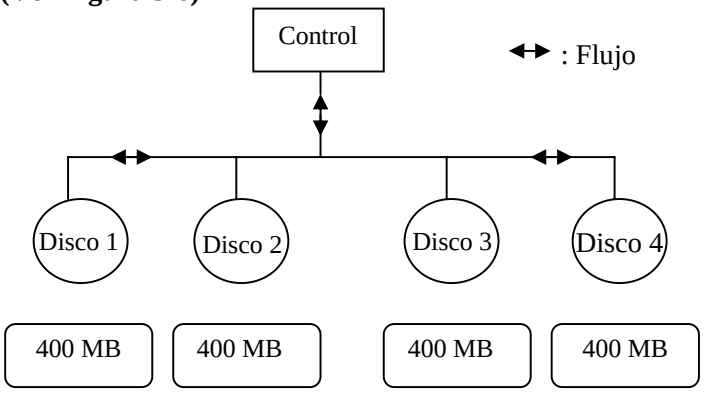


Figura 3-6. *Sistema Disk Spanning*

- Disk Mirroring. Los datos escritos en una unidad de disco son simultáneamente escritos en otra unidad; si un disco falla, el otro disco puede ser usado para comenzar

el sistema y reconstruir el disco dañado. Una de las ventajas más significativa en está técnica es el 100% de redundancia en datos, eliminando completamente la alternativa de perdida de información y la posibilidad de arrancar cualquier sistema operativo en caso de desastre. La posible desventaja que tiene esta configuración es su costo ya que se tendría que duplicar cada unidad de disco duro. **(Ver Figura 3-7)**

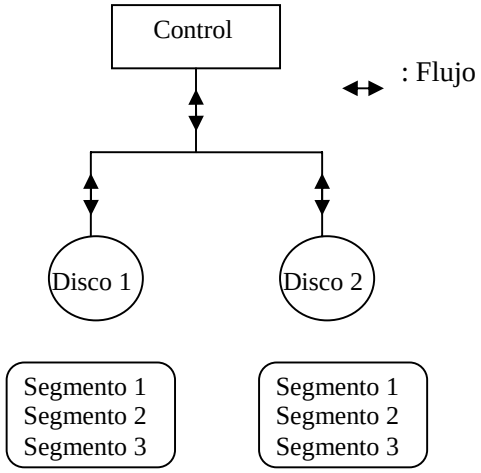


Figura 3-7. *Sistema Disk Mirroring*

- Paridad. Es la manera de generar redundancia en los datos de una base de información sin necesidad de duplicar completamente la información origen. Particularmente la paridad es aplicada a unidades de disco enteras o en su defecto a segmentos a través de todas las unidades de disco existentes.

  Los tipos de paridad son las siguientes:

  - *Dedicada*: La paridad de los datos es almacenada en un disco ajeno adicional.

  - *Distribuida*: La paridad de los datos es distribuida en todos los discos del sistema.

Si una unidad de disco falla, esta puede ser reconstruida desde la información de paridad respectiva. Por lo tanto la paridad proporciona redundancia en una falla de disco sin la necesidad de respaldar toda la unidad, sin embargo la generación de paridad puede decrementar el proceso de lectura.

El esquema de una paridad dedicada durante lectura - escritura es mostrado a continuación.**(Ver Figura 3-8)**

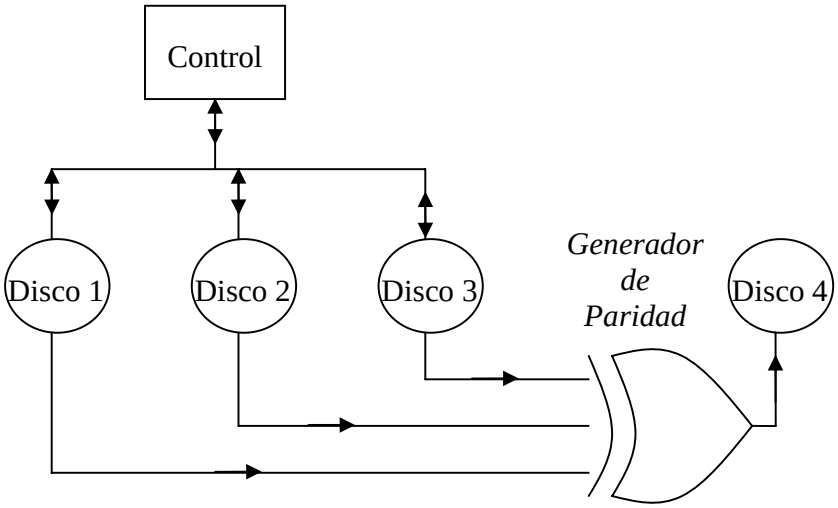


Figura 3-8. *Sistema en paridad dedicada.*

Los niveles RAID son modelos de arreglos de discos configurados para tolerancia a fallas e incremento de desempeño. Cada nivel tiene configurado características particulares que lo compensan con respecto a otros.

RAID 0

La información es dividida en bloques y distribuida secuencialmente en todos los discos, es íntegramente un sistema *striping*. Utilizado principalmente como una colección de datos de fuentes externas donde altas tasas de transferencia son alcanzadas; sin embargo la tolerancia a fallas no es contemplada ya que no hay redundancia de datos, para poder utilizar esta técnica es necesario como mínimo dos unidades para implementarlo.

RAID 1

La información escrita en un disco es duplicada en otro disco, habiendo siempre dos copias de los datos, cada copia en discos físicos separados. Esta técnica es la forma más simple contra fallas en discos físicos, es íntegramente un sistema *disk mirroring.* Está técnica puede ser considerada como una forma de respaldo ya que contiene una copia íntegra redundante de una partición en otro disco, es aplicado principalmente en sistemas donde la tolerancia a fallas es lo más importante. Se necesitan como mínimo dos unidades para implementarlo.

RAID 2

La información escrita es por medio de *disk striping* con la capacidad de comprobar fallas por un código *ECC (Error Correction Code)* que se intercala en todas las unidades de disco a nivel de bit; el método empleado para incluir dicho código y que actúa como corrector automático de errores es el *hamming* que básicamente por cada *n* bits de datos

se añaden *k* bits de paridad de tal forma que el carácter transmitido tiene una longitud de $n+k$ bits que ayudará a identificar bits de paridad y bits de datos con respecto a su posición. Actualmente su utilización no es contemplada ya que requiere características especiales inconvenientes tales como discos especiales.

RAID 3

La información escrita es por medio de *disk striping* con una unidad de disco dedicada para paridad. La recuperación de datos se realiza conforme al contenido de los otros discos, es capaz de soportar acceso a todos sus discos al mismo tiempo lo que hace que tenga una alta capacidad de respuesta, sin embargo no es aplicable en aplicaciones que procesan grandes archivos en forma secuencial, la disponibilidad y fiabilidad siempre son altas. Se necesitan como mínimo tres unidades de almacenamiento para su implementación.

RAID 4

Se utiliza la misma técnica de un RAID 3, el disco de paridad es construido con la información almacenada en los otros discos, con la única ventaja de poder acceder a los discos en forma individual. Es utilizado en el almacenamiento de información de gran tamaño, lo que lo hace ideal en aplicaciones gráficas. Se necesitan como mínimo tres unidades de almacenamiento para su implementación

RAID 5

Se utiliza la técnica *disk striping* pero la paridad existente será distribuida, su almacenamiento será por bloques en todos los discos duros, si alguna unidad falla se puede recuperar su información en tiempo real, mediante la operación lógica en la que se basa la paridad *XOR* sin que el servidor deje de funcionar. Para evitar problemas de saturación en los periféricos de entrada y salida (*cuellos de botella)* se asigna un bloque de paridad por cada disco, al distribuir la función de comprobación entre todos los discos se reducen estos efectos negativos. Por lo tanto este nivel de arreglo es aceptable para ser usado en sistemas operativos multiusuario. Se necesitan como mínimo tres unidades de almacenamiento para su implementación pero entre más unidades existan la relación costo- beneficio tendrá mejores resultados.

RAID 10

Este tipo de arreglo es una composición entre los niveles RAID 1 y RAID 0, por lo tanto se obtiene tanto capacidades redundancia a fallos de *mirroring* como de acceso eficaz de *striping*. Cada disco tendrá un duplicado, este sistema ofrece un 100% de redundancia. El costo de implementación es mayor ya que para dichas capacidades son necesarias mayor cantidad de unidades físicas. **(Ver Figura 3-9)**

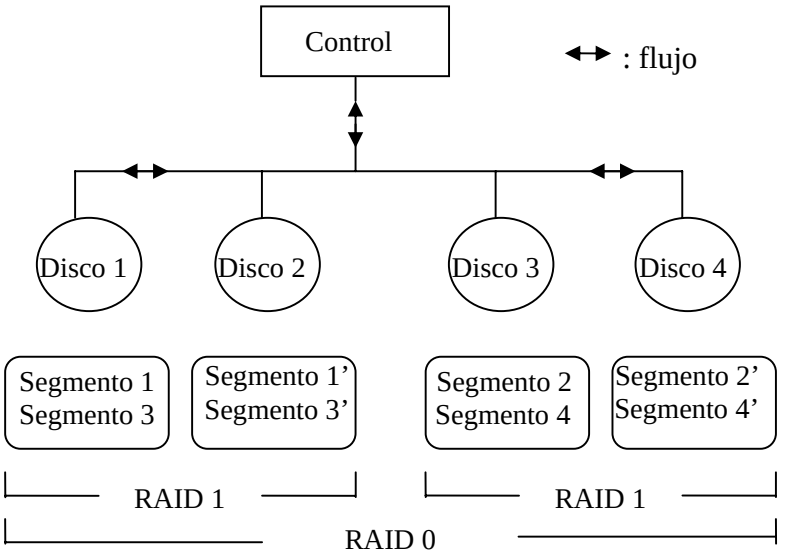


Figura 3-9. *Arreglo RAID 10*

RAID 30

Este tipo de arreglo es una composición entre los niveles RAID 3 y RAID 0, RAID 30 ofrece una alta velocidad y confiabilidad en la información.**(Ver Figura 3-10)**

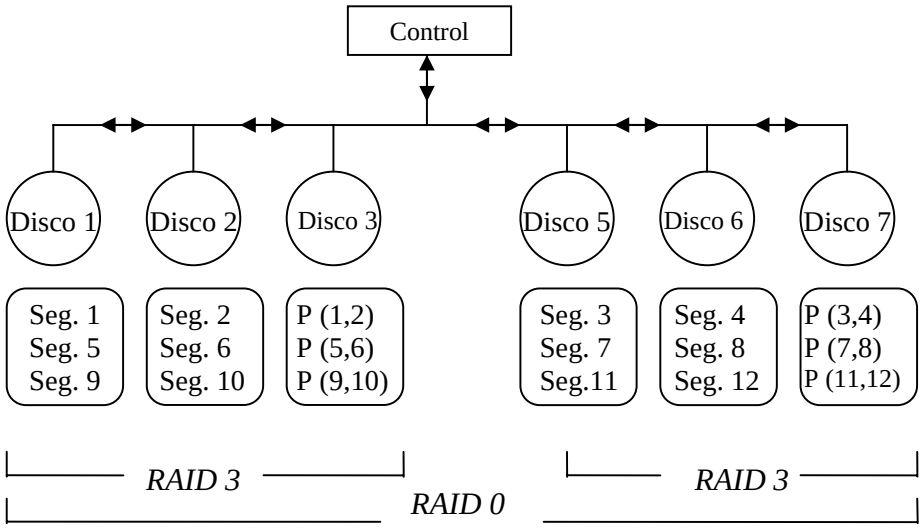


Figura 3-10. *Arreglo RAID 30*

RAID 50

Este tipo de arreglo es una composición entre los niveles RAID 5 y RAID 0, ofrece alta confiabilidad en los datos y buen desempeño de lectura y escritura. La paridad estará distribuida a través de todos los discos existentes en el arreglo. **(Ver Figura 3-11)**

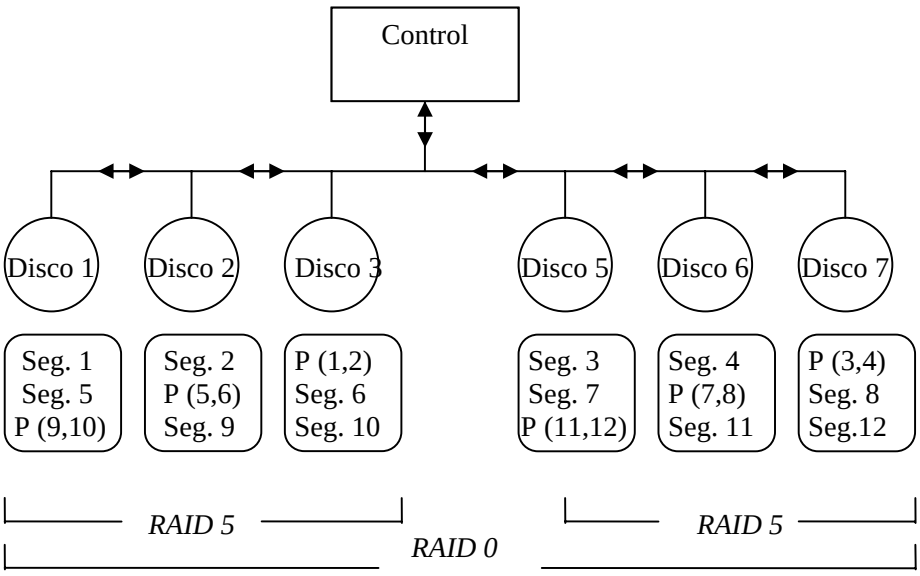


Figura 3-11. *Arreglo RAID 50*

El resguardo de la información en cualquier sistema es indispensable, la idea es guardar datos en medios confiables y seguros para poder tenerla siempre disponible en cualquier consulta. La integridad de la información se ve contemplada por la redundancia que ofrecen los sistemas RAID que garantizan que información crítica no se vea afectada en un desastre.

3.4 Dispositivos de Almacenamiento Digital.

En la actualidad las soluciones de grabación en infraestructuras de red están orientadas a medios de almacenamiento de gran capacidad los cuales permitan el resguardo y administración centralizada de eventos de video; para esto, el termino DVR (*Digital Video Recorder)* ha sido adoptado como término genérico para un dispositivo que hace la misma función que un VCR *(Video Cassette Recorder)* pero en el ámbito digital, donde los datos de video son almacenados en un disco duro en un formato de compresión tal como MPEG-4. Con esto se logra que un DVR tenga todas las funcionalidades que un VCR más la característica de acceder directamente a cualquier evento almacenado.

Un DVR está compuesto principalmente por 2 módulos:

El primer modulo contempla los elementos de hardware tales como discos duros, fuentes de poder, chasis, etc.

El segundo modulo considera al software en el cual está definido un pequeño sistema operativo que controla los dispositivos de entrada y salida, así como esta definido los algoritmos de compresión a utilizar en el almacenamiento.

Los DVR han sido categorizados por ser *basados en PC* y como *embebidos*. Un DVR basado en PC tiene una arquitectura clásica de una computadora personal con tarjetas de video especiales diseñadas para capturar imágenes de video; el tipo embebido es especialmente diseñado como un grabador de video digital con su propio sistema operativo y un software de aplicación contenido en una memoria de solo lectura o en un *firmware*[7]

Existen un gran número de fabricantes de DVR's los cuales contemplan algunas características similares pero no necesariamente las mismas:

En Hardware:

- Los DVR son comúnmente diseñados para ser ubicados en un Rack dentro de un site bajo características térmicas especificas.
- Múltiples entradas de video con conectores acordes tanto con video analógico como digital. (cable coaxial, par trenzado o fibra óptica). Las más comunes entradas son de 1, 4, 8,16 y 32 puertos.
- Salidas de video que son usadas para otros equipos tales como: multiplexores, monitores de video, etc.
- Indicadores e interruptores que permiten configurar e indicar el estado actual del medio.
- Conexiones para dispositivos de entrada tales como teclados o joysticks.
- Unidades de lectura y escritura de dispositivos ópticos que permitan realizar respaldos o extraer información relevante.
- Entradas para eventos de alarma para dispositivos externos de seguridad tales como: sensores y controles de acceso.
- Alarmas de salida para características de detección internas tales como detección de movimiento o fallas técnicas de cámaras.
- Comúnmente todos los DVR contienen un arreglo de discos duros que desechan la posibilidad de fallas en los medios, siendo el arreglo RAID 5 el más común siendo una característica importante ya incluida por cualquier DVR.

[7] Es software que se encuentra embebido en un dispositivo físico, es regularmente incluido en un archivo de imagen binario o memorias flash.

En Software:

- Se puede definir el número de tramas por minuto con la cual una cámara digital transmitirá las imágenes, pudiéndose configurar a que automáticamente se incremente ese valor en señales de entrada tales como detección de movimiento.
- La resolución de una imagen se puede definir a que sea ajustada en eventos de alarma específico, generando así una mejor calidad de imagen en sucesos importantes y trascendentes.
- Búsqueda de eventos almacenados por fecha y hora.
- Acceso remoto que permite por medio de un navegador de Internet conectarse al DVR y ver acontecimientos en tiempo real.

La solución basada en PC es una propuesta adecuada cuando se tiene una computadora con gran capacidad en hardware que permita eficientemente realizar tareas de administración sin perder nunca el estado activo de almacenamiento, en estos casos, el sistema operativo hace el proceso de comunicación directa con el disco duro que regularmente es configurado con algún tipo de distribución redundante que permita recuperar información en caso de fallos sin perder su funcionalidad. Cabe mencionar que actualmente se ha definido a un DVR que está dentro de una red de datos IP como NVR (*Network Video Recorder*) aquí las características son idénticas a un grabador digital común pero con las ventajas que una red de datos ofrece, tales como consulta de enlaces remotamente desde cualquier lugar del mundo por medio de Internet, señales de aviso a un correo electrónico, control del ancho de banda, etc.

En este capítulo se mencionaron las formas de almacenar información en una gran variedad de dispositivos. Primeramente se habló de medios de almacenamiento primarios que se utiliza para datos temporales principalmente y medios secundarios utilizados para almacenamiento definitivo. Dentro del almacenamiento secundario se encuentran tecnologías magnéticas y ópticas, las primeras son utilizadas para almacenar información muy grande y regularmente no son diseñados para ser portables, las ópticas son una alternativa reciente que permite grabar menor cantidad de datos pero con la posibilidad de poder ser transportados a cualquier parte. En segundo lugar se hablo un poco de las técnicas encaminadas a la seguridad de la información por medio de arreglos los cuales permiten el respaldo e integridad de los datos en caso de perdidas o daños físicos de los medios de almacenamiento, la tecnología de resguardo redundante se ha ido enriqueciendo por medio de técnicas cada vez mas avanzadas y versiones mucho mas eficientes de recuperación de información.

Finalmente se mencionó el tipo de almacenamiento en sistemas de seguridad, particularmente hablando en video, existen dos grandes alternativas, una de ellas es un servidor dedicado para almacenamiento con grandes características físicas que garanticen la integridad de la información o un grabador de video digital el cual lleva implícito la disponibilidad de cualquier información almacenada en él.

Capitulo 4

Infraestructura del Instituto de Ingeniería

Como parte de un análisis de seguridad global, siempre es necesario considerar y analizar todos los activos de una organización como preámbulo de un análisis de riesgos, debido a que la omisión de información podría generar fallas de seguridad que permitirían a amenazas ser potencialmente posibles. Por esta razón en este capítulo se realiza la identificación y descripción de cuatro elementos indispensables para el funcionamiento del Instituto de Ingeniería: *construcciones, equipamiento, personal e infraestructura de red.* Este capítulo permitirá identificar los procesos que se realizan dentro del Instituto de Ingeniería para tener un diseño que contemple sus zonas prioritarias a vigilar y así también permitirá conocer las capacidades con las que cuenta su infraestructura de red de datos.

4.1 Ubicación Geográfica

El Instituto de Ingeniería es una entidad académica dedicada a la investigación en diversos ámbitos de la ingeniería, sus instalaciones están ubicadas al sur de la Ciudad de México dentro de la Universidad Nacional Autónoma de México en su campus de Ciudad Universitaria. En Ciudad Universitaria, los edificios que componen al Instituto se encuentran distribuidos, ya que nuevas estructuras han sido construidas durante los cincuenta años que lleva de existencia esta entidad. El área geográfica que abarca es de alrededor de 20,000 m^2 en instalaciones generales. **(Ver Figura 4-1)**

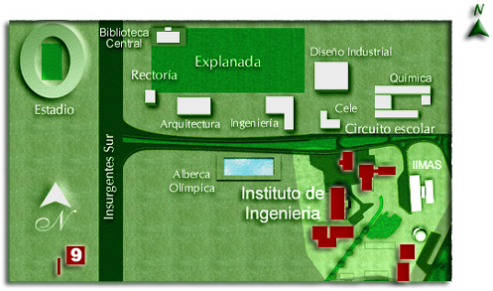


Figura 4-1. *Ubicación Geográfica*
(Fuente: www.iingen.unam.mx)

El Instituto de Ingeniería está conformado por catorce edificios, en los cuales se llevan a cabo labores de investigación de una gran variedad problemas actuales de ingeniería a nivel nacional así también en diecisiete laboratorios de investigación. **(Ver Figura 4-2)**

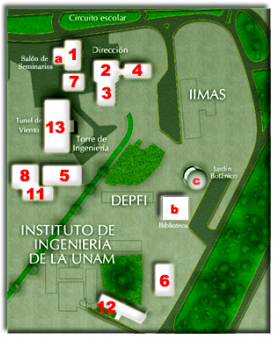


Figura 4-2. *Edificios del Instituto de Ingeniería.*
(Fuente: www.iingen.unam.mx)

El Instituto de Ingeniería no solamente esta conformado por inmuebles destinados a funcionar como oficinas, actualmente existen construcciones tales como laboratorios, talleres, centros de modelado donde también se realizan actividades científicas que permiten un estudio formal de fenómenos físicos, así como simulaciones de sucesos naturales; investigaciones y proyectos de interés social en los campos de: energía, transporte, medio ambiente, recursos hídricos, cómputo y comunicaciones.

4.2 Construcciones

Por la gran variedad de actividades de investigación realizadas en el Instituto de Ingeniería, cada uno de sus edificios tiene características particulares en diseño y arquitectura. Cada edificio alberga una gran cantidad de recursos humanos y materiales indispensables para la realización de actividades administrativas, científicas y técnicas. Como parte del proceso de identificación de elementos existentes dentro de ellos, se hace un mayor énfasis en aquellos aspectos referentes a seguridad física tales como: cantidad de accesos, salidas de emergencia, estacionamientos, número de niveles, complejidad y actividades realizas. Esta actividad permitirá dimensionar de mejor manera el sistema de videovigilancia pensado.

A grandes rasgos, las áreas implicadas en este reconocimiento son cerradas y abiertas. Como parte de espacios abiertos se agrupan a estacionamientos, áreas comunes de esparcimiento y laboratorios abiertos. Para espacios cerrados se clasifican oficinas, talleres, y laboratorios especializados para modelados.

A continuación se describen cada uno de los edificios del Instituto de Ingeniería junto con las actividades ahí realizadas:

EDIFICIO 1

Este edificio es donde se llevan a cabo principalmente actividades directivas, administrativas y de planeación acerca de las actividades académicas dentro del Instituto, aquí se lleva el control de todo el personal, siendo un edificio clave para el correcto desempeño de otras áreas, cabe mencionar que aquí se toman decisiones definitivas sobre planes de trabajo, aprobación de proyectos, etc.

Las áreas alojadas en esta edificación son:

- Dirección.
- Secretarías
- Unidad de Contratos y Convenios
- Coordinación de Sismología e Instrumentación Sísmica.

Este edificio es de tres niveles para los cuales se tiene una salida de emergencia. El estacionamiento de este edificio es compartido con el personal de la Torre de Ingeniería por lo tanto la afluencia de automóviles es continua.

EDIFICIO 2

En este inmueble se localiza la *Subdirección de Estructuras* la cual controla tres de sus coordinaciones. Aquí se realizan estudios de diseño de estructuras bajo efectos naturales tales como sismos y viento. Así también, análisis del comportamiento de los suelos y algunos otros criterios en la construcción de carreteras. Las coordinaciones que se ubican aquí son:

- Coordinación de Estructuras y Materiales
- Coordinación de Mecánica Aplicada
- Coordinación de Ingeniería Sismológica

Este edificio es de dos niveles y el estacionamiento es común para otros edificios (4, 3 y 2), esta edificación tiene la característica de ser la entrada general para los edificios 4, 2 y 3 por lo tanto la afluencia de movimiento es considerable.

EDIFICIO 3 (Raúl Sandoval Candazur)

En este edificio se encuentra la Coordinación de Mecánica Aplicada, así como uno de los laboratorios en los cuales se hace el estudio del comportamiento de estructuras y materiales ante diversas situaciones a las que se ven sometidos.

- Laboratorio de Estructuras
- Coordinación de Mecánica Aplicada

La mayor parte de esta construcción es abarcada por su laboratorio, solamente alberga algunos cubículos en los cuales se coordina las labores realizadas en el laboratorio. Este edificio es de un solo nivel con una puerta de carga y descarga de materiales.

EDIFICIO 4 (Raúl J Marsal Córdoba)

En las instalaciones del Edificio 4 se encuentran algunas otras áreas de la Subdirección de Estructuras, así como una coordinación y un laboratorio.

- Coordinación de Geotécnica
- Laboratorio de Mecánica de Suelos “Guillermo Hiriart Molinar”

Dentro de este edificio existen cubículos y módulos de estudio donde becarios, técnicos académicos e investigadores documentan la información recaba en prácticas de campo. El acceso principal es a través del Edificio 2 y tiene 1 puerta de emergencia utilizada usualmente para el acceso de materiales al laboratorio ahí encontrado.

EDIFICIO 5

En este edificio se localiza la S*ubdirección de Hidráulica y Ambiental* la cual estudia el aprovechamiento y control del agua, así como el diseño de estructuras hidráulicas,

ingeniería marítima, ingeniería en termo-fluidos, etc. Además de esta subdirección algunas de sus coordinaciones se pueden encontrar:

- Subdirección de Hidráulica y Ambiental
- Coordinación de Bioprocesos Ambientales
- Coordinación de Hidráulica
- Coordinación de Ingeniería Ambiental
- Laboratorio de Ingeniería Ambiental

EDIFICIO 6 (*Fernando Espinosa Gutiérrez)*

Aquí se puede encontrar la Coordinación de Vías Terrestres de la Subdirección de Estructuras, los estudios realizados en su laboratorio son a escala natural en tramos de pavimentos de prueba, así como en carreteras típicas, tanto en México como en el extranjero. Las áreas que se localizan aquí son:

- Coordinación de Vías Terrestres
- Laboratorio de Vías Terrestres

Este edificio tiene la menor cantidad de usuarios por lo que solo contempla un nivel; no existe un área formal para el estacionamiento de vehículos, la construcción más grande es del laboratorio y en general los recursos físicos existentes son maquinaría pesada y una gran variedad de componentes de suelos.

EDIFICIO 7 (*Nabor Carrillo)*

Esta área para el estudio del suelo es parte fundamental de la Coordinación de Geotecnia, aquí se lleva un análisis detallado y especializado en el tema de enrocamientos de cualquier índole. Por lo tanto aquí podemos encontrar:

- Mecánica de Rocas
- Laboratorio de Enrocamientos

La afluencia es mínima en este edificio, no existe un estacionamiento destinado para las personas que trabajan aquí, por lo tanto se toma como estacionamiento los lugares comunes para la Torre de Ingeniería y el Edificio 2. Tiene dos niveles comúnmente utilizados como oficinas.

EDIFICIO 8

Esta construcción contempla solamente un solo laboratorio de investigación en el cual trabajan investigadores de las coordinaciones de Hidráulica, Mecánica, Fluidos y Térmica.

En este edificio se construyen modelos físicos que permitan estudiar y analizar comportamientos del agua en estructuras hidráulicas y ríos.

- Laboratorio de Hidromecánica

Este laboratorio contempla dos niveles destinados para análisis y oficinas. Tienen un acceso de emergencia que como para los demás edificios, es utilizado para el ingreso de materiales ahí utilizados. Este edificio no tiene un estacionamiento propio.

EDIFICIO 9

Este edificio es el más apartado, se encuentra cerca del Jardín Botánico, forma parte de la Subdirección de Estructuras y Materiales, aquí se simulan movimientos sísmicos de cualquier tipo para probar diseños de estructuras.

- Laboratorio de la Mesa Vibradora

Ya que este edificio se encuentra aislado, no hay un control definido del personal, sin embargo, la zona de estacionamiento es exclusiva y la afluencia de automóviles es moderada. Aquí se realizan otras actividades de investigación para la Coordinación de Ingeniería Ambiental así como la Planta Solar.

EDIFICIO 11

Como parte de la Subdirección de Hidráulica, se encuentra un laboratorio en la cual se realizan estudios de sedimentos y su afectación por fenómenos fluviales y los efectos que estos provocan.

- Laboratorio de Modelos Fluviales

Este laboratorio es ubicado en un espacio abierto, su acceso es controlado y no hay acceso vehicular hacía él.

EDIFICIO 12 ***(Bernardo Quintana Arrioja)***

Aquí se encuentra la *Subdirección de Electromecánica*, y sus coordinaciones. Aquí se llevan estudios para el desarrollo de sistemas para la automatización de procesos, telecomunicaciones, aprovechamiento de la energía solar, análisis de regímenes transitorios, etc.

Las Coordinaciones y Laboratorios que aquí se encuentran son:

- Coordinación de Sistemas de Cómputo

- Coordinación de Instrumentación
- Coordinación de Automatización
- Coordinación de Ingeniería en Sistemas
- Coordinación de Ingeniería Mecánica, Térmica y de Fluidos.
- Laboratorio Óptica Solar
- Laboratorio de Doble Altura
- Taller Mecánico

En este edificio se controla toda la infraestructura de cómputo y telecomunicaciones del Instituto de Ingeniería. Este edificio consta de tres niveles que tienen 3 salidas de emergencia, su espacio de estacionamiento es reducido pero exclusivo para su personal.

EDIFICIO 13

Esta construcción realizada por el Instituto, también es conocida como la *Torre de Ingeniería*, alberga una gran cantidad de áreas de todas las subdirecciones, las cuales ocupan casi en su totalidad todas las instalaciones. Aquí se encuentran:

- Auditorio “José Luis Sánchez Bribiesca”
- Coordinación de Ingeniería de Procesos Industriales y Ambientales.
- Coordinación de Ingeniería Sismológica
- Coordinación de Ingeniería de Sistemas
- Coordinación de Geotecnia
- Laboratorio de Geoinformática
- Coordinación de Estructuras y Materiales
- Coordinación de Mecánica Aplicada
- Laboratorio del Túnel del Viento
- Coordinación de Ingeniería Mecánica, Térmica y de Fluidos
- Coordinación de Hidráulica.
- Facultad de Ingeniería
- Facultad de Química

EDIFICIO 18

Edificio más reciente para el Instituto de Ingeniería, parte de la Subdirección de Electromecánica en el cual existen aulas, laboratorios y cubículos. El acceso es realizado por medio del Edificio 12 sin tener definido un estacionamiento propio. Existen 4 salidas de emergencia a pesar de ser una construcción de un solo nivel.

Finalmente, la ubicación y distribución de los edificios permite definir al Instituto como un lugar inseguro debido al gran número de personas ajenas que utilizan las áreas comunes para trasladarse hacía otras facultades o Institutos dentro de Ciudad Universitaria.

4.3 Equipamiento

Como ya se mencionó con anterioridad, dentro del Instituto de Ingeniería existen una gran cantidad de laboratorios base de pruebas experimentales y análisis, por está razón, las herramientas y equipo ahí existente toma mucha importancia para continuar con los objetivos planteados por este órgano de investigación

A continuación se da una visión general de algunos de los laboratorios y del tipo de equipamiento existente:

Subdirección de Ingeniería Ambiental.

Esta subdirección tiene a su cargo dos laboratorios de ingeniería ambiental, Laboratorio de Bioprocesos e Ingeniería Ambiental y Laboratorio de Hidráulica. El espacio destinado para estos laboratorios es de 570m^2 c/u. Algunos equipos existentes en este tipo de laboratorios son balanzas, potenciómetros, medidores, etc.

Subdirección de Electromecánica

Esta subdirección contempla 4 laboratorios de gran valor (*Laboratorio de doble altura, Laboratorio de Hidromecánica, Laboratorio de Óptica Solar y Sistemas de Cómputo).* El equipo existente son motores eléctricos, osciloscopios, medidores, filtros solares, etc. En la parte de cómputo, existen todos los elementos de comunicaciones, sustento de la red de datos del Instituto de Ingeniería.

Subdirección de Estructuras y Materiales

Esta subdirección contempla 3 laboratorios en análisis de estructuras (*Laboratorio de Estructuras y Materiales, Laboratorio de Geotecnia y Laboratorio de Vías Terrestres)*. Los equipos que ahí se encuentran son de gran magnitud algunos otros elementos de menor dimensión son: actuadores, gatos hidráulicos, instrumentos para pruebas de resistencia y fatiga de especímenes.

Definitivamente, la instrumentación que se maneja en laboratorios es de suma importancia, por ello el efecto que tendría su ausencia sería verdaderamente perjudicial para el funcionamiento de recintos de investigación. La parte de equipamiento es un tema bastante delicado, por ser información de uso interno para Instituto de Ingeniería y por seguridad de sus laboratorios, la totalidad de los equipos existentes no ha sido mencionada en este documento.

4.4 Personal

El factor humano es uno de los eslabones más débiles en la cadena de la seguridad, la afectación del recurso humano puede afectar irremediablemente los objetivos propuestos así como los planes de trabajo. El Instituto de Ingeniería esta conformado por un gran número de personas a cargo de diferentes tareas que permiten el correcto funcionamiento y realización de metas planteadas en el Instituto.

Formalmente, el personal se integra por seis grupos generales que realizan funciones específicas:

1) Personal Académico
2) Personal Administrativo
   - Directivo
   - Operativo
3) Honorarios
4) Personal de Base
5) Profesores e Investigadores visitantes
6) Estudiantes

El *personal académico* son los encargados de realizar tareas de investigación de acuerdo a proyectos definidos, aquí se encuentra los elementos con mayor grado de estudios del Instituto. Investigadores y Técnicos Académicos participan constantemente en nuevos desarrollos de investigación los cuales se difunden a nivel nacional e internacional a favor del país.

El *personal administrativo* son los encargados de realizar tareas administrativas del Instituto, estos son parte importante para el abastecimiento de recursos a todas las subdirecciones y coordinaciones.

El *personal de base* contempla al personal encargado de servicios generales referentes a la seguridad y disponibilidad de los inmuebles, así como el mantenimiento y vigilancia de los edificios. Cabe mencionar que servicios de mensajería es abarcado por este tipo de personal.

Finalmente los *estudiantes* que complementan sus estudios por medio de la realización de trabajos de tesis que documentan técnicamente las actividades realizadas junto a investigadores, por tanto, son elementos de apoyo en el desarrollo de proyectos. Dentro de este tipo de personal se pueden encontrar estudiantes laborando como prestadores de servicio social, becarios y tesistas, a nivel licenciatura, maestría y doctorado.

El personal externo es un grupo no considerado como parte del Instituto debido a las actividades temporales que realizan, estas personas son requeridas en algunas

circunstancias por investigadores o personal administrativo por un tiempo muy definido para tareas particulares en muchas ocasiones fuera de las instalaciones.

Como se ha percibido, el personal del Instituto de Ingeniería es el recurso que permite que el desarrollo de la investigación exista, por ello, es importante ofrecer instalaciones seguras y confiables para que el desenvolvimiento de su trabajo no se vea interrumpido por factores ajenos como la inseguridad. La cantidad de personal que se encuentra en los edificios es tal que la búsqueda de una solución de seguridad debe afectar de manera positiva a toda la comunidad sin excepción alguna.

4.5 Red del Instituto de Ingeniería

4.5.1 Red de Datos

La red de datos del Instituto de Ingeniería tiene como principio establecer una comunicación eficiente entre su comunidad para que las actividades científicas que ahí se realizan sean desarrolladas fácilmente y con mayor eficacia. Esta red de datos ha sido sujeta a diversos cambios a través del tiempo ya que el adelanto tecnológico en este ámbito de las comunicaciones ha estado en constante desarrollo.

Buscando que su infraestructura esté siempre apegada a las últimas actualizaciones tecnológicas disponibles, hoy en día se ha logrado tener una red con alta disponibilidad y escalabilidad, donde voz y datos interactúan eficazmente en un mismo entorno dando la pauta a que nuevos elementos tales como video o audio sean contemplados como una posibilidad real de inclusión, buscando que nuevas capacidades sean utilizadas por la comunidad y que los alcances que se pudieran llegar a lograr sean siempre en beneficio de todo el personal que conforma a este órgano de investigación.

La red de datos del Instituto de Ingeniería es solamente un elemento de comunicación dentro de una red global conocida como RedUNAM; por lo tanto la comunicación hacía redes exteriores dependen directamente de la comunicación existente en este importante enlace. La característica principal que se ha buscado para la red del II es la adopción de tecnologías acordes con las existentes en RedUNAM. Actualmente en la red de datos del Instituto de Ingeniería existe una gran variedad de servicios que conviven bajo un mismo entorno: telefonía, correo electrónico, aplicaciones, sistemas de videoconferencia, etc., son realizadas en conjunto debido a las capacidades alcanzadas a través de los años.

Esta red une a todos los edificios que conforman al II por medio de enlaces subterráneos que permiten una comunicación transparente para el usuario que intenta conectarse a otro recurso sin importar que se encuentre dentro o fuera del Instituto. Dichos enlaces se han mejorado con el tiempo ya que las necesidades han ido en aumento y la cantidad de información que se maneja también crece aceleradamente.

Cabe mencionar que la forma de comunicar a los usuarios en cada edificio tiene la misma estructura, primeramente se toma en cuenta el número de usuarios a comunicar por piso, con base en esta información, se colocan los elementos de comunicación correspondientes que abarquen a esa cantidad de personas, tomando siempre en consideración, la posibilidad de aumento en los elementos a comunicar a futuro.

Existen una gran variedad de enlaces dentro de la red, el más importante es el que conecta al Instituto de Ingeniería con RedUNAM ya que este permite comunicación con el exterior, este enlace actualmente utiliza la arquitectura GigaEthernet la cual ofrece un flujo de la información de hasta 1Gbps por medio de fibra óptica, lo que permite tener un vínculo de gran capacidad para todo el tráfico que se podría generar dentro de la red del II. Existe otro enlace hacia RedUNAM y es por medio de la Torre de Ingeniería, este enlace fue considerado ya que el diseño de la Torre fue hecho para que tuviera la capacidad de tener un vínculo directo e independiente y buscando igualmente que existiera un balanceo de carga con enlaces ya existentes.

Los equipos principales que son la base de toda la estructura de red se encuentran localizados en el edificio 12 dentro de la Coordinación de Sistemas de Cómputo, ahí se localizan dos LAN Switches Core XRN que operan con la tecnología Expandable Resilient Networking de 3com permitiendo tener una red altamente flexible y siempre con un gran rendimiento. Así también tienen la funcionalidad de incluir LAG (Link Agregation) que es una característica que contempla una comunicación doble con cada uno de los switches Core XRN, con esto cualquier enlace creado en un switch también se conectará al otro switch; todo esto permite tener tiempos de respuesta inmediatos ante fallos y una posibilidad de crecimiento según las necesidades. Finalmente también existe redundancia entre ambos Switches Core XRN (nivel 1), definiendo un escenario respaldado para cualquier contingencia.

El resto de los enlaces están dirigidos hacía cada uno de los edificios del Instituto de Ingeniería, en cada edificio se ha establecido una sección principal que permitirá el alojamiento de otros modelos de switches (nivel 2) que están conectados directamente con el backbone principal, estos switches por edificio pueden ser vistos como el backbone de cada edificio ya que a estos se conectarán switches colocados en cada piso por edificio.

Finalmente los switches ubicados en cada piso (nivel 3) serán los que ofrecerán la conexión con las computadoras existentes por cada coordinación, como ya se menciono el número de switches dependerá de la cantidad de usuarios existentes por piso, por lo tanto la escalabilidad siempre debe ser considerada ya que la cantidad de personal que se incorpora al Instituto siempre está en aumento.

Como parte de una administración centralizada, cada uno de los puertos que conforman a los switches están identificados, esto permite llevar un monitoreo eficaz del estado de conexión para cada computadora y así identificar rápidamente la existencia de problemas de comunicación. Así también el enlace existente entre los switches principales y los de cada edificio contemplan también un LAG previniendo completamente fallas en cualquier

parte de la red de datos. El esquema general que se sigue por cada edificio es el mismo, salvo algunas excepciones donde el medio de comunicación es a través de UTP Cat. 6 1000Base-T y en otros Fibra óptica 1000Base-SX

Para los Switches Centrales se tiene la característica de controlar y soportar flujo de datos y de voz al mismo tiempo por medio de puertos Gigabit Ethernet que permitan transferencias de grandes cantidades de información hasta el backbone de cada uno de los edificios. Así también poder utilizar Redes Privadas Virtuales[1]

4.5.2 Red Telefónica

La red telefónica actual del Instituto de Ingeniería esta integrada en la red de datos existente ya que se busco reducir costos y la carga administrativa que implica dos redes independientes. Una vez logrado la integración de voz y datos en un mismo medio se han alcanzando los beneficios que la tecnología sobre IP ofrece y se han adoptado las nuevas características que la comunicación analógica no ofrecía.

La tecnología utilizada para integrar la funcionalidad de voz en la red de cableado estructurado es por medio de la plataforma 3Com Superstack 3 NBX® que se conforma principalmente de dos módulos de operación denominados NBX Gateway y NBX Call Processor los cuales son los elementos principales para el funcionamiento de la red. El primer elemento realiza el enlace directo con los switches para realizar el ruteo de llamadas a sus respectivos destinatarios. El NBX Call Processor es un módulo único que tiene por función principal administrar todo el tráfico de llamadas que se generan en la red.

Existe una comunicación redundante (E1 de Fibra óptica) entre el sistema de telefonía del II con la RED Telefónica de la UNAM, este enlace permite la comunicación con el resto de las entidades de la Universidad y fuera de esta. Cabe mencionar que la Torre de Ingeniería también contempla un enlace similar de un sistema NBX con la red telefónica, por lo tanto existen dos conexiones de telefonía hacía el exterior con lo cual se puede considerar un flujo equilibrado de enlaces de voz hacía redes externas.

Un aspecto a contemplar fue la integración de una red telefónica a prueba de fallas eléctricas, en otras palabras, que la posibilidad de comunicarse fiablemente aun en casos de falta de energía eléctrica siempre estuviera vigente; para esto a los switches que conforman a la red de datos se les anexaron Ethernet Power Supplies (EPS) los cuales ofrecen en un mismo enlace energía eléctrica y datos. Así entonces, un EPS permite generar en sus puertos de salida datos y suministró de energía por medio de cables de LAN 10/100Mbps, por lo tanto estos puertos de salida son conectados directamente a cada aparato telefónico permitiendo la utilización del teléfono.

[1] Virtual LANs son un grupo de dispositivos conectados en segmentos físicos diferentes con la capacidad de comunicarse entre ellos como si estuvieran en una misma LAN.

Para que la funcionalidad de voz sobre el protocolo IP se logre, los enlaces de la red de datos tuvieron que ser actualizados, se necesitaban por lo menos enlaces FastEthernet (100Mbps) a nivel general para lograr una comunicación eficiente, por lo tanto los enlaces antiguos que no ofrecían estas características tuvieron que ser removidos y remplazados.

Muchas funcionalidades fueron adquiridas y operan hoy en día en la red telefónica:

- Para los administradores de la red es posible realizar estas tareas unificadamente, es decir, pueden monitorear tanto paquetes de datos como voz desde un mismo punto.
- Funciones de control de llamadas de larga distancia y teléfonos celulares pueden ser restringidas únicamente al personal autorizado.
- La supervisión y administración del flujo de llamadas es realizada por medio de un registro que permite controlar su realización.
- La capacidad de mensajería unificada es utilizada para que mensajes de voz y de e-mail puedan ser consultados en un solo buzón de voz.
- El software de los aparatos telefónicos puede ser actualizado de acuerdo a los estándares existentes hasta ese momento.
- Las conexiones analógicas también siguen siendo consideradas dejando activa la posibilidad de integrar comunicación analógica y digital al mismo tiempo.

Existen más características disponibles que aun no han sido integradas, pero el objetivo es que las ventajas que este tipo de tecnología ofrecen sean utilizadas al máximo.

4.5.3 Red Inalámbrica

Es la red de datos más reciente instalada en el Instituto de Ingeniería, la tecnología inalámbrica ha sido considerada como una opción de comunicación real que permite participar a cualquier usuario con la red de datos existente sin necesidad de estar sujeto a un cable físico, logrando así enlaces casi tan eficientes como los obtenidos por una red estructurada basada en enlaces físicos.

Las redes inalámbricas locales están basadas fundamentalmente en las normas IEEE[2] 802.11 (*Wireless Fidelity*). Las variantes de estas normas son:

- **802.11a**. Fue la primera norma de comunicación de los enlaces inalámbricos y se alcanzan velocidades de hasta 54Mbps, con desdoblamiento de velocidad hasta 72 y 108 Mbps. Esta variante opera dentro del rango de los 5GHz a través de doce canales en un radio de cobertura máximo de 50m.

- **802.11b.** Es la segunda norma del estándar, alcanza velocidades de 11Mbps, con desdoblamiento hasta 22Mbps; opera dentro del rango de los 2.4 GHz por medio de tres canales en un radio de cobertura máximo de 50m.

[2] Organismo de estandarización internacional.

- 802.11g. Es la tercera norma de comunicación, ofreciendo velocidades de hasta 54Mbps, tiene la característica de tener compatibilidad con los dispositivos **802.11b,** funciona dentro de la frecuencia de los 2.4GHz por medio de tres canales con una cobertura máxima de 100m.

Los enlaces inalámbricos son efectuados a través de *puntos de acceso*[3] 3Com Mod. 8750® los cuales se localizan distribuidos en todos los edificios del Instituto de Ingeniería. Este modelo tiene la característica de manejar dos estándares de comunicación **802.11b** y **802.11g** que por consecuencia permite hacer enlaces de 11 y 54 Mbps a frecuencias de 5Ghz y 2.4Ghz; con esto se logra tener mayor cobertura de usuarios en una misma área. El número máximo de usuarios soportados por un solo dispositivo es de 253 a velocidades de hasta 54Mbps a distancias no mayores de 100m.

Las velocidades de conexión se establecen en forma automática ya que el estado de la conexión depende de la ubicación del usuario dentro del radio de cobertura. Otra característica importante es la capacidad de poder alimentar de energía eléctrica a los puntos de acceso por medio de su cable de par trenzado (*PoE*) conectado a ellos lo que facilita la instalación de puntos de acceso a un solo cable.

Por parte de la seguridad, las conexiones inalámbricas se realizan por medio de un código de cifrado de emisión/ recepción llamado WEP (*Wired Equivalent Privacy*) el cual permite cifrar a un nivel de 128 o 154 bits y WPA (*Wi-Fi Protected Access*) que permite un nivel de protección más alto ya que utiliza el cifrado de datos a un nivel de 256 bits y también TKIP (*Temporal Key Integrity Protocol*) que son claves de sesión dinámica por usuario.

La red inalámbrica privada en el Instituto es controlada por medio de reservaciones hechas por un servidor DHCP que asigna direcciones IP no homologadas a los equipos; cabe mencionar que los puntos de acceso son conectados a los switches existentes y separados virtualmente de la comunicación, es decir, el tráfico existente dentro de la red inalámbrica se encuentra aislado por medio de VLANs, las cuales ofrecen segmentar el tráfico y dirigirlo a través de los canales de comunicación más convenientes.

Para que no exista interferencia con la información que procesan, los puntos de acceso son configurados escalonadamente, es decir, deben existir 4 o 5 canales de separación entre cada uno de ellos para lograr enlaces adecuados. Para una configuración con disponibilidad de 11 canales (802.11a), se configurarían tres puntos de acceso en los canales 1,6 y 11 con lo cual se logran velocidades afines pero en canales totalmente separados; la información procesada es dirigida por enlaces troncales hasta llegar hasta un destino de la misma red inalámbrica o de la red cableada.

No existe un lineamiento de ubicación de puntos de acceso por edificio ya que un estudio detallado de alcances en comunicación inalámbrica, arrojo que algunos edificios contienen

[3] Aparato que permite comunicar dispositivos inalámbricos para formar una red inalámbrica, comúnmente es utilizado como un puente entre redes WiFi y Ethernet.

estructuras más complejas en las cuales se tienen que hacer otro tipo de consideraciones para abarcar lugares de difícil acceso para señales de radio frecuencia.

La red inalámbrica se encuentra conectada a un Firewall que garantiza la integridad y disponibilidad de los enlaces inalámbricos existentes, peticiones identificadas como perjudiciales para la red inalámbrica, son detenidas y eliminadas para evitar algún tipo de ataque.

Actualmente está red opera eficientemente dando servicio a cerca de 50 usuarios los cuales siguen en aumento buscando migrar a una comunicación sin cables. Los resultados obtenidos hasta hoy han sido notorios ya que el costo que implica un cableado estructurado ha disminuido considerablemente.

Por otro lado, como parte de la infraestructura tecnológica del Instituto de Ingeniería, se encontraron sistemas de videovigilancia activos que realizan tareas de seguridad en dos edificios. Estos sistemas son tecnologías analógicas bajo esquemas de grabación continuos. Un análisis y estudio de estas tecnologías, se realizará en capítulos posteriores para identificar su posibilidad de convivencia con la red datos del Instituto y su integración con el nuevo sistema IP actualmente en desarrollo.

En este capitulo se ha mencionado la estructura general del Instituto de Ingeniería. Primeramente se identificaron los edificios que lo contemplan así como su ubicación geográfica dentro de ciudad universitaria, así mismo, se menciono el tipo de personal que se localiza dentro de cada una de sus instalaciones y el material de apoyo que utilizan para sus labores de investigación y análisis. Finalmente como parte importante se dio un esquema general de la infraestructura de red existente y las tecnologías que se utilizan en la comunicación de información tales como: voz, datos y video dentro del Instituto que permiten concluir la real posibilidad de adoptar un nuevo sistema basado en video en la estructura de red convergente existente hoy en día.

Capítulo 5

Análisis de Seguridad

Los incidentes de seguridad afectan los activos de empresas así como al personal que labora en ellas; por esta razón, el diseño e integración de estrategias de seguridad se ha vuelto importante para evitar o minimizar consecuencias no deseadas que puedan afectar los escenarios de trabajo existentes.

Un riesgo es la exposición a situaciones negativas que puedan afectar el funcionamiento directo o el resultado de actividades comunes, siendo el impedimento para conseguir objetivos. Para que un entorno pueda considerarse seguro debe cumplir con características idóneas donde se puedan realizar plenamente actividades. Los riesgos siempre existirán en cualquier ámbito de trabajo y más aquellos que afectan la integridad y seguridad física de del personal tales como robos y asaltos, por esto, la administración de este tipo de riesgos es fundamental para poder reaccionar ante algún evento en particular bajo un método establecido acorde a la situación.

Este capítulo tiene por objetivo exponer un análisis de seguridad basado en requerimientos del personal del Instituto de Ingeniería así como sus autoridades que permitirá identificar las áreas de mayor importancia del Instituto para definir la ubicación idónea de aquellos puntos de vigilancia del sistema.

5.1 Consideraciones

La acción ante un riesgo puede ser reactiva o proactiva siendo cada una ellas una respuesta valida a situaciones que expongan las vulnerabilidades de cualquier entidad.

Primeramente ser *reactivos* significa actuar ante circunstancias ya suscitadas que permitirán establecer un plan de reacción de eventos en particular, esta es una solución eficaz cuando el impacto no es de carácter crítico y los procesos pueden seguir su cause. La forma *proactiva* busca estructurar de manera concreta la posibilidad de riesgos con todo lo que ello implica, primeramente se realiza una *identificación* la cual ofrecerá información que permitirá ubicar riesgos principales antes de que estos se vean afectados. Posteriormente la *declaración* del riesgo define las condiciones de situaciones no deseadas y las consecuencias de dichas situaciones directa o indirectamente en la estabilidad de los procesos.

Dentro de un buen estudio de riesgos existen tres factores importantes que deben ser considerados: *la probabilidad de ocurrencia*, *el impacto dentro de la organización* y la *exposición al riesgo*. El primero es simplemente identificar cada uno de los riesgos y asignarles un valor representativo, dependiendo a la información recolectada, cualquier riesgo sin probabilidad implica un suceso sin posibilidad de ocurrencia. Posteriormente el *impacto* es un valor que cuantifica el nivel de severidad de cualquier riesgo, hay ocasiones en que se presentan eventos dañinos que no afectan el correcto funcionamiento de un proceso u objetivo, por lo tanto deben ser categorizados de última prioridad para que no retrasen los tiempos de respuesta de otros de carácter crítico. Finalmente se tiene que contemplar cuales factores son los más *expuestos* es decir los de probabilidad e impactos altos para colocarlos como punto de inicio de cualquier diseño sobre seguridad.

Dentro de la administración de los riesgos para un proyecto de seguridad física el factor humano es el riesgo que debe ser considerado de más alta prioridad; un estudio de seguridad en el que se busque identificar y cuantificar la importancia del personal no es viable ya que el objetivo es ofrecer condiciones apropiadas a toda persona sin excepción.

Como parte de una actividad de identificación de riesgos a lo que respecta a **activos**, los elementos a tomar en cuenta son los siguientes:

Identificación del riesgo. Aquí se define lo que es aceptado como un riesgo, el cual será contemplado y considerado para futuras recomendaciones de seguridad.

Condición del riesgo. Las circunstancias que se deben presentar para que este riesgo se origine, desde este momento se pueden considerar soluciones basadas en prevención logrando así controlar riesgos de carácter sencillo.

Probabilidad del riesgo. Es importante cuantificar la posibilidad de presencia de riesgos, con base en experiencias y riesgos eventualmente posibles, un valor porcentual entre cero y 100 ofrecerá una perspectiva más clara de los eventos más comúnmente suscitados que puedan afectar a los activos.

Consecuencia de riesgo. La posibilidad de que ocurra un evento perjudicial nunca podrá ser nulificado por tanto considerar las consecuencias que genera un suceso de este tipo es fundamental para tener un plan de reacción.

Impacto del Riesgo. Para este caso también es importante cuantificar que tanto puede dañar una consecuencia, pudiendo considerar un valor numérico que represente la magnitud relativa del hecho que cuantifique el impacto.

Tipo de impacto. Es importante considerar de que manera el impacto puede afectar la organización: monetariamente, técnicamente, legalmente, moralmente, físicamente, etc.

Riesgos consecuentes. En muchas ocasiones cabe la posibilidad de que un riesgo genere más riesgos, por esto considerar cómo se vería afectado todo el entorno es importante para identificar riesgos secundarios también administrables.

Finalmente con una administración adecuada se busca reducir la probabilidad de ocurrencia de un suceso, minimizar la magnitud de una pérdida o reducir aceptablemente las consecuencias que un riesgo delictivo pueda provocar. Ya que existe una declaración que define los tipos de riesgo a los que se es vulnerable se debe hacer una documentación que implica una conversión de los datos de un riesgo a información para tomar decisiones sobre ellos.

Dentro del Instituto de Ingeniería se han presentado eventos perjudiciales; se ha visto amenazado y perturbado por situaciones las cuales han afectado el buen funcionamiento de

las actividades que ahí se realizan, donde los activos y pertenencias de particulares han sido el objetivo principal de ataque, perdiendo así los objetivos definidos y la confiabilidad de espacios seguros para desarrollar investigación.

Por la inmensa diversidad de actividades que se realizan dentro del Instituto de Ingeniería en cada uno de sus edificios, la cantidad de riesgos a los que su personal está expuesto es siempre latente, tan es así, que hechos delictivos han afectado a investigadores, técnicos académicos, estudiantes y trabajadores, generando que su rendimiento laboral no sea el óptimo. Los riesgos mas importantes serán los que afectan a las personas que laboran en el Instituto; la seguridad de activos son el segundo punto clave para este sistema de seguridad basado en video. Algunos riesgos delictivos que pueden afectar directamente a las personas pueden ser los siguientes:

Robos o atracos
Asaltos
Hurtos
Amenazas
Espionaje
Actos vandálicos
Perdida de información

El desarrollo y estudio de cada una de los espacios críticos, está basado en planteamientos hechos por la propia comunidad del Instituto desde estudiantes hasta autoridades que en conjunto brindaron el conocimiento que servirá como referencia para la ubicación de la tecnología de videovigilancia. Es importante mencionar que actualmente no existe un registro completo referente a delitos durante los cincuenta años de vida del Instituto de Ingeniería. No obstante, se presentan solamente algunos ejemplos que han ocurrido en los últimos años como apoyo en el diseño de la solución en la distribución del sistema.

Un análisis de riegos físico pretende identificar la estructura física del ambiente en el que los activos se encuentran, vulnerabilidades que puedan traer daños a la información y a todos los demás activos. Un análisis de riesgos de esta naturaleza, será el que provee el soporte físico al entorno en que está siendo manipulada la información e implica la identificación de posibles fallas en la localización física de los activos, la evaluación del impacto de accesos indebidos a las áreas donde se encuentran los activos y hasta la evaluación del impacto en desastres ambientales en la infraestructura de todo el Instituto de Ingeniería

Como se puede apreciar, un análisis tan extenso implicaría una gran cantidad de tiempo; todas las partes implicadas deberían ser participes por medio de encuestas y/o entrevistas que permitan identificar a detalle, aquello con lo que se cuenta y se quiere proteger. Por lo tanto, un análisis de seguridad para una organización de tales dimensiones sale del objeto de estudio de este tema de tesis y de los objetivos planteados al principio de este trabajo de investigación.

Con base en peticiones y registros, se identificaron los riegos para interiores en edificios y laboratorios, la información arrojó detalles importantes que permiten identificar los lugares más sensibles y de mayor valor para la comunidad.

Por lo tanto, se puede definir que las áreas más críticas a tomar en cuenta son las siguientes:

Edificio 1: Caja y Laboratorio de Sismex
Edificio 3: Laboratorio de Estructuras y Materiales
Edificio 5: Laboratorio de Bioprocesos e Ingeniería Ambiental
Edificio 8: Laboratorio de Oleaje y Laboratorio de Hidromecánica
Edificio 9: Mesa Vibradora
Edificio 11: Laboratorio de Hidráulica y Mesa de Arena
Edificio 12: Laboratorio de Doble Altura y Sistemas de Cómputo

En el resto de las zonas con menor factor de riesgo se contemplarán como campo de acción para el sistema de videovigilancia. Finalmente podemos mencionar que existen tres objetivos primordiales en la administración de riesgos de los cuales se busca alcanzar:

1. Reducir la probabilidad de ocurrencia. Un sistema de seguridad de video no garantiza que eventos negativos sean nulificados, sin embargo es una buena herramienta que permite reducir el número de crímenes.
2. Reducir la magnitud de perdida. Un sistema de seguridad de video permitirá disminuir la cantidad de perdidas ya que la identificación de autores de un robo o de conductas indebidas puedes ser sancionados para no reincidir en el mismo delito.
3. Modificar las consecuencias del riesgo. Para abarcar este objetivo en su totalidad, es importante tener una planificación integra de seguridad, es decir, no basta con tener la mejor de las tecnologías sin la existencia de una estrategia de reacción ante eventos.

Por lo tanto una persona necesita conocer los lugares y las situaciones donde pueden producirse ataques con el fin de evitarlos y si no pueden ser evitados, por lo menos buscar que herramientas de seguridad sean adoptadas para reducir eventos negativos en torno a estos espacios.

5.2 Índice Delictivo

El Instituto de Ingeniería se ha visto envuelto en situaciones desafortunadas que han afectado de manera considerable a un gran número de personas; la extracción de activos han causado perdidas económicas considerables que han ocasionado la perdida de confianza y tranquilidad para realizar actividades en forma segura.

La información que a continuación se presenta es un elemento importante en el diseño del sistema de seguridad y base para identificar tendencias delictivas en diferentes zonas. Se

podrán definir mejores esquemas seguros en aquellos lugares identificados como vulnerables y con mayor reincidencia delictiva.

5.2.1 Relación de Delitos dentro del Instituto de Ingeniería

Exteriores

Fecha	Hora	Delito	Ubicación	Zona
12/07/2002	19:30	Robo de autoparte	Estacionamiento Edificio 5	I
19/11/2002	14:00	Incendio	Laboratorio de Ingeniería Ambiental	X
06/09/2002	14:30	Asalto a becario	Estacionamiento Edificio 2	F
18/09/2002	15:05	Robo de autoparte	Estacionamiento Edificio 1	A
05/10/2007	20:30	Robo de autoparte	Estacionamiento Edificio 1	A

Interiores

Fecha	Hora	Delito	Ubicación
15/09/2002	14:00	Robo de instrumento de medición	Edificio 12, Automatización
08/11/2002	10:15	Disputa	Edificio 5, Planta Baja,
14/05/2003	17:00	Robo de documentación	Edificio 1
15/05/2003	09:00	Robo de herramienta	Edificio 8, Taller Mecánico
23/05/2003	12:00	Robo de equipo portátil	Edificio 2, Piso 1
11/04/2004	11:00	Robo de cámaras digitales	Edificio 3, Segundo Nivel
15/04/2004	14:00	Robo de objetos personales	Edificio 12, Piso 2
11/04/2007	15:32	Robo de objetos personales	Edificio 1
12/04/2007	12:00	Robo de Material Eléctrico	Almacén General
24/10/2007	13:30	Robo de proyector	Edificio 12, Piso 2
29/10/2007	11:00	Robo de Laptop	Edificio 5, Piso 2

Como se puede apreciar, la mayor cantidad de eventos se suscitan en horarios vespertinos, donde el flujo de gente ya no es tan continuo. El tipo de robo es en general de objetos de dimensiones pequeñas lo que permite su fácil extracción aún con los elementos de seguridad ubicados en los accesos de cada uno de los edificios. La *información* es otro activo de gran importancia para investigadores debido a que implican grandes inversiones en tiempo, dinero y esfuerzo que también se ha visto afectado considerablemente.

Nota: La información anteriormente mencionada es representativa. Algunos de los eventos presentados en las instalaciones fueron omitidos por motivos de seguridad.

5.3 Zonas de Vigilancia

Una zona de riesgo es considerada como aquel espacio donde un siniestro puede presentarse por características desfavorables del lugar mismo; espacios solitarios, áreas comunes sin vigilancia y la no concientizacion de personas sobre medidas básicas de seguridad pueden ser algunos factores generadores de eventos desafortunados que afectan directamente los objetivos de la organización.

En esta sección se buscará identificar los espacios externos en los cuales hay una mayor probabilidad que se presente un incidente perjudicial; considerando la distribución no uniforme en edificios y su ubicación dentro de un campus universitario, los espacios comunes son mayoría y el contacto directo con otras dependencias de la Universidad evita poder controlar las personas que transitan alrededor de las instalaciones por medio de herramientas de seguridad física como controles de acceso, sensores y alarmas; se partirá de la propuesta de que los espacios de más riesgo son aquellos no vigilados, donde la visualización no es clara y de más fácil acceso.

Las zonas que a continuación se mencionan han sido consideradas como las más vulnerables dentro del área que abarca el Instituto de Ingeniería con apoyo en el análisis de seguridad realizado hasta este momento:

Zona A
Primera sección del estacionamiento del Edificio 1, aquí se localizan un gran número de automóviles particulares los cuales en su mayoría corresponden al personal administrativo de este edificio, por las actividades que ahí se realizan, el personal administrativo abandona el edificio a altas horas de la noche, lo que permite que la posibilidad de un incidente delictivo sea latente.

Zona B
Segunda sección del estacionamiento del Edificio 1, esta parte del estacionamiento es importante ya que aquí se encuentran los automóviles del personal que labora en la Torre de Ingeniería, de igual manera, esta sección es acceso único hacía estacionamientos pertenecientes a otros edificios. La posibilidad de un incidente delictivo por las actividades realizadas hasta altas horas de la noche es también latente.

Zona C
Tercera sección del estacionamiento y única salida para automóviles provenientes de edificios contiguos, lo que lo hace una sección de gran flujo vehicular; aquí se encuentra un acceso peatonal proveniente del circuito universitario que facilita el acceso de personas ajenas a las áreas comunes de estacionamientos.

Zona D
Primera sección del estacionamiento perteneciente al Edificio 2, 3 y 4, aquí se encuentran automóviles particulares correspondientes a personal de tres edificios, lo que lo hace un

estacionamiento con bastante actividad y carga. A este estacionamiento se puede acceder por varias alternativas, una de ellas es un acceso peatonal proveniente del circuito universitario, así como accesos por áreas comunes de ciudad universitaria lo que facilita el contacto directo con los automóviles y personas en cualquier momento.

Zona E
Segunda sección del estacionamiento perteneciente a los Edificio 2, 3 y 4, aquí se ubican el resto de los automóviles pertenecientes al personal de 3 edificios, esta sección del estacionamiento también tiene un acceso directo a zonas comunes y áreas de esparcimiento para universitarios, llegar a estas zonas sin vigilancia dedicada realmente es sencillo.

Zona F
Sección ubicada a un costado del Edificio 1, esta zona fue acondicionada como estacionamiento por la saturación en los estacionamientos principales, por aquí se vuelve único el ingreso a las zonas E, F y D, así también existen una zona de descanso y esparcimiento donde parte de la comunidad convive; Por la gran diversidad de actividades ahí realizadas, los riesgos aumentan considerablemente.

Zona G
Esta zona se vuelve importante ya que es el único paso hacía el estacionamiento del Edificio 5, de igual manera esta zona contempla el acceso hacía el sótano de la Torre de Ingeniería donde hay flujo vehicular hacía el almacén general.

Zona H
Sección ubicada a un costado del Edificio 3 la cual tiene un gran flujo peatonal por ser la ruta de acceso más rápida hacia los Edificios 2,3 y 4; a pesar de ser un camino relativamente corto(35m aproximadamente), esta sección carece de buena iluminación por las noches.

Zona I
Sección única de estacionamiento para el Edificio 5, esta zona contempla un espacio para tránsito de equipo pesado perteneciente a los laboratorios encontrados en el Edificio 3. Por su pequeñas dimensiones, en está sección existe un gran flujo vehicular por la saturación de espacios durante todo el día. La posibilidad de robo de auto partes o de vehículos es factible.

Zona J
Sección ubicada a un costado del Edificio 6, abarca tanto un acceso común para el personal del mismo edificio y un laboratorio del Edificio 12, por su gran extensión es también utilizado como estacionamiento, el flujo de tránsito no es tan constante, sin embargo es un punto frágil de seguridad ya que no hay control de acceso vehicular hacía esta zona.

Zona K
Lugar utilizado por el Edificio 18, contemplando su estructura de un nivel y su diseño arquitectónico, esta zona es ocupada como explanada.

Zona L
Sección en proceso de construcción, con base en modelos, será un área de esparcimiento la cual debe ser observada en su totalidad.

Zona M
Sección destinada a estacionamiento de automóviles del Edificio 12, por encontrarse dentro de un área restringida, la posibilidad de que automóviles ajenos se infiltren es poco probable, sin embargo el acceso peatonal es libre, lo que permite que personas tengan a su alcance los automóviles ahí localizados.

Zona N
Acceso único para estacionamientos pertenecientes a la Facultad de Ingeniería y Posgrado de Ingeniería, no obstante la saturación de las áreas destinadas para estacionar automóviles han provocado que este espacio sea utilizado por algunos personas del Instituto y otras dependencias como estacionamiento, lo que origina que su integridad sean contempladas en el diseño.

Zona O
Sección ubicada frente al Edificio 5, aquí se localiza un constante movimiento de personal que ingresa a este edificio ya que es la estructura con mayor población estudiantil. La escasa iluminación así como la gran cantidad de vegetación convierten a esta zona un área desprotegida, así se buscará visualizar el trayecto desde el acceso del edificio hasta su respectiva zona de estacionamiento.

Zonas P y Q
Estas zonas son importantes pero no criticas ya que cualquier tránsito en estas, tendrían que implicar un acceso por zona O ya contemplada.

Zona R
En esta sección existe un acceso controlado que es utilizado para ingreso de material a laboratorios, su salida es hacía circuito universitario lo que permitiría accesos no autorizados a los laboratorios más próximos.

Algunos edificios del Instituto se encuentran apartados de las edificaciones principales, por las tareas de investigación que ahí se realizan y la importancia de los activos que allá se encuentran, se han identificado las zonas potencialmente vulnerables las cuales pueden ser aprovechadas por amenazas que afecten objetivos, se identificaron cuatro zonas críticas conforme a la importancia de los activos y los procesos ahí realizados:

Zona S
Sección más amplia donde se pueden englobar el helipuerto de la universidad y una sección de estacionamiento para el personal que realiza investigación en los laboratorios que ahí se encuentran; el acceso está controlado pero los muros existentes no son lo suficientemente

altos para evitar un acceso indebido; es importante mencionar que en este tipo de zonas, al aire libre, es difícil considerar todas las posibilidades de acceso ya que una intrusión puede darse por cualquier punto.

Zona T
Esta sección es comúnmente utilizada por personal para dirigirse hacía otros laboratorios, la sección es solitaria y de gran vegetación, lo que la hace una sección crítica que pudiera ser aprovechada para llevar a cabo un delito.

Zona U
En esta sección se encuentra un planta solar de grandes dimensiones, la altura de los sensores solares llegan cerca de los 3 metros, lo que origina que la visibilidad en esta zona (aproximadamente 500m^2) no sea clara, la posibilidad de un incidente perjudicial es latente.

Zona V
Acceso vehicular principal al Edificio 9 y a su laboratorio, formalmente este acceso no es controlado, un automóvil ajeno fácilmente podría ingresar, esta zona es importante porque es utilizada para estacionamiento de vehículos los cuales se encuentran apartados y expuestos a daños.

En la siguiente figura se identifican las zonas críticas externas **(Ver Figura 5-1)**

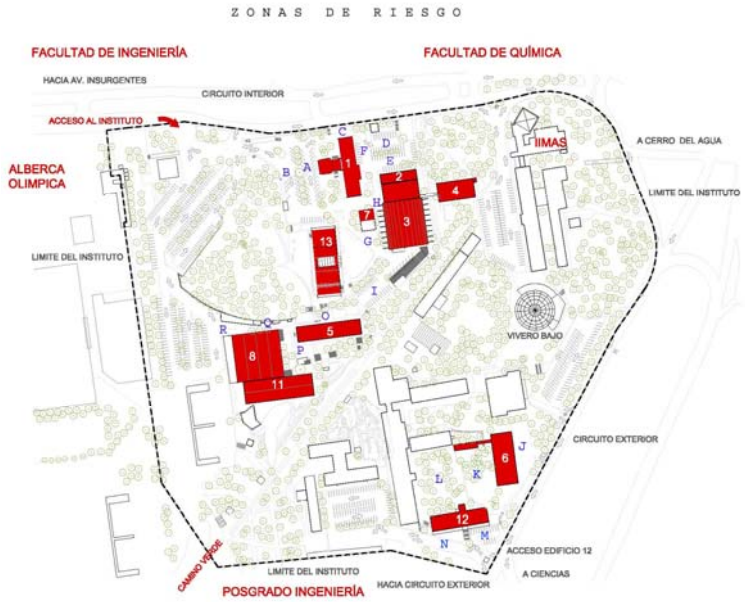


Figura 5-1. *Zonas de Riesgo en el Instituto de Ingeniería.*
(Fuente: www.iingen.unam.mx)

Se han presentado en este capitulo, 22 zonas las cuales han sido consideradas como críticas por diversos factores. La seguridad física se vuelve prioridad cuando las posibilidades de incidentes simplemente existen; por la distribución del Instituto en sus edificios, las zonas de flujo vehicular así como peatonal son muchas, es por ello que un buen análisis de

seguridad, permitirá priorizar las acciones de seguridad en esas áreas estratégicas. Para las zonas experimentales que se caracterizan por estar rodeadas de vegetación y espacios no urbanizados se buscó tener un cuidado especial por medio de un análisis *costo-beneficio* que permita definir lo primordial a vigilar.

5.4 Repercusiones en el Instituto de Ingeniería

Desde tiempo atrás el Instituto ha desarrollado actividades de investigación científica aplicada sobre problemas específicos de nuestro país y así brindar asesorías en diversas áreas de la ingeniería. Los resultados obtenidos han sido aportaciones significativas en el desarrollo experimental a nivel nacional e internacional con lo cual se coloca como un organismo de gran credibilidad ante el mundo.

El Instituto de Ingeniería, proporciona servicios de ingeniería a diversos sectores de la sociedad así como la formación de recursos humanos que son base de las futuras generaciones de investigadores que contribuyan con el desarrollo del país y el bienestar de la sociedad. Este centro de investigación es una comunidad integrada por una gran cantidad de elementos (humanos, físicos, tecnológicos) los cuales en su conjunto forman la base elemental para procesos realizados. Por las dimensiones que abarca este órgano de investigación y la variedad de actividades que se realizan, el valor de sus activos son indispensables para la continuidad de las actividades realizadas.

Como se mencionó anteriormente, el Instituto de Ingeniería se ha visto perturbado por acontecimientos delictivos que han afectado en la realización de actividades laborales.

Las repercusiones más evidentes e inmediatas en los que se ha implicado el Instituto son de carácter *económico*, el robo de activos ha ocasionado una pérdida monetaria para el Instituto ya que el reemplazo del material robado, debe hacerse de manera inmediata. Así también robo a particulares ha generado que los estudios de investigación no se hagan en las mejores condiciones por el ambiente de desconfianza que se origina en un entorno sin seguridad. A pesar de que los incidentes que se han presentado dentro de las instalaciones del Instituto son activos, los desastres intangibles pueden ser aun más perjudiciales que los que se pueden cuantificar. Por ejemplo sería muy perjudicial para el Instituto de Ingeniería tener una mala imagen que evitara asignación de futuros proyectos de gran inversión debido a perdidas de confianza de entidades externas.

De igual manera por ser una institución dedicada a la investigación, la *información* se vuelve un ámbito de prioridad, la mayoría de la documentación existente es lograda a través de años de estudio que por su importancia se vuelve confidencial y de gran valor. Por esto, la integridad y el manejo de la información es razón suficiente para considerar todas las posibilidades necesarias que la protejan. La cuantificación de repercusiones ayudará a entender las consecuencias que podrían existir en ambientes inseguros, los principales criterios a considerar son los siguientes:

Impacto en Investigación

Bajo	*Produce un impacto reducido en los procesos analíticos, la continuidad se normaliza cuando se recupera o remplaza el faltante*
Medio	*Produce un impacto que puede ocasionar la reasignación del análisis hacía otras entidades solamente de forma transitoria en estudios particularmente sensibles*
Alto	*Imposibilidad de realizar investigación en alguna de las áreas.*
Catastrófico	*Imposibilidad de realizar estudios especializados cual sea que estos fuesen*

.

Impacto Operacional

Bajo	*Produce retraso en procesos no sensibles*
Medio	*Produce retraso en procesos importantes, ocasionando demoras en los tiempos de entrega de soluciones.*
Alto	*Origina retrasos graves en procesos primordiales*
Catastrófico	*Cuando las actividades y procesos se ven interrumpidas indefinidamente.*

Impacto en la Imagen

Bajo	*Situación conocida solamente por el personal interno*
Medio	*Se presenta cuando existe perdida de confianza y de seriedad en un área en específico.*
Alto	*Se presenta cuando existe perdida de confianza en muchas áreas de investigación.*
Catastrófico	*Se presenta cuando hay un desprestigio general de toda la entidad, lo que origina la imposibilidad de sustento de la organización*

Se han mencionado solo algunas repercusiones en las que podría verse implicado el Instituto de Ingeniería ante amenazas potenciales. La diversidad de actividades que se realizan (administrativas, académicas, técnicas) obliga a considerar todos los ámbitos al momento de elegir un sistema de videovigilancia. Con base en el anterior estudio, se pueden definir la mejor ubicación y número de cámaras de video a utilizar en el proyecto.

Hasta este punto, sabemos que el sistema propuesto servirá primeramente como herramienta disuasiva, así como un sistema de consulta de eventos suscitados y finalmente como una herramienta para constante monitoreo. Así que, toca el turno de estudiar las tecnologías existentes en el mercado actual referentes a vigilancia en video para buscar la solución más adecuada y aquella que se ajuste de mejor manera a la estructura tecnológica y laboral existente en el Instituto de Ingeniería.

Capítulo 6
Evaluación de Tecnologías

Los sistemas de videovigilancia han existido de tiempo atrás y debido a sus grandes resultados, los requerimientos han aumentado día a día. El proceso de digitalización ha beneficiado a la industria de la seguridad y actualmente ofrece un mejor funcionamiento en equipos de videovigilancia. Las mejoras en este tipo de sistemas es constante y nuevas alternativas han surgido bajo un concepto totalmente IP.

Los sistemas de videovigilancia actuales han evolucionado a través de los años a razón de cuatro etapas donde los componentes básicos de un sistema CCTV (cámara, medio de transmisión, grabador y monitor) han sido digitalizados.

La primera generación de los sistemas CCTV se caracterizó por la digitalización de la cámara de video. Las cámaras digitales basadas en sensores CCD reemplazaron a cámaras analógicas. El sensor utilizado era completamente digital, sin embargo, se continuaba usando medios de transmisión analógicos como el cable coaxial y las grabaciones eran realizadas en VCRs.

La segunda generación se caracterizó por la digitalización del grabador del video. Hubo buenos beneficios con esta medida como: la no necesidad de cambiar cintas, mejor calidad de grabación y herramientas especializadas de búsqueda de eventos. En este momento se le denomino al equipo de almacenamiento de video como DVR con entradas y salidas analógicas para cámaras y monitores, por lo tanto, era un sistema hibrido.

La tercera generación fue una mejora al sistema basado en DVR pero con la cualidad de poder monitorear en lugares remotos por medio de la utilización de una PC con un software de administración de video dedicado.

La última generación y actualmente vigente fue la digitalización del medio de transmisión. Cámaras IP y servidores de video han terminado con el uso de equipos analógicos buscando utilizar un medio digital como las redes de datos utilizadas en cómputo.[10]

De acuerdo con la etapa actualmente vigente, este capítulo contempla algunas soluciones interesantes referentes a sistemas de videovigilancia basadas en el protocolo de comunicación IP. Cabe mencionar que las soluciones aquí presentadas tienen registro y son propiedad de fabricantes especializados en el área.

Dentro del ámbito de sistemas CCTV existen cientos de soluciones, esta sección permitirá analizar y seleccionar aquella más afín a las necesidades propias del Instituto de Ingeniería.

Existen un gran número de medios que permiten el transporte de datos de manera eficiente, en particular siempre hay consideraciones a tomar en cuenta en el manejo de video las cuales darán la pauta a tomar la mejor opción

Las posibilidades para transmisión de video son variadas, sin embargo, se delimitará el estudio a las alternativas existentes dentro del Instituto y que permitan ser utilizadas dentro del esquema de generación - transmisión –almacenamiento de video digital.

El medio de transmisión utilizado debe ser capaz de administrar la gran cantidad de información que puede llegar al orden de los GBytes; considerando que dicha información en ocasiones es necesario difundirla hasta dispositivos de monitoreo y unidades de respaldo remotas, las cualidades del enlace deben ser óptimas.

Existen muchos escenarios que podrían satisfacer esta necesidad, por ejemplo, plantear una solución basada en distribución de señales por medio de *radio frecuencia*[1], para la cual se necesitaría un sistema de transmisión acorde con las dimensiones del Instituto con repetidores y transmisores distribuidos, sin embargo este tipo de soluciones está sujeto a costos excesivos de implantación y mantenimiento. Así también, la transmisión de video por medio de un cable dedicado permitiría confiabilidad en el medio, pero el costo y complejidad de instalación aumentarían considerablemente por las características del Instituto.

Ante este panorama, se buscarán integrar señales de video digital a la red de datos existente actualmente en el Instituto de Ingeniería, para la distribución de información que generará este sistema de videovigilancia.

6.1 Medios de Transmisión de Video

Los sistemas analógicos de seguridad fueron la primera alternativa de videovigilancia utilizada por grandes empresas y organizaciones que buscaban la integridad de sus activos y la seguridad de sus ámbitos de trabajo. Las primeras soluciones se basaban en cámaras analógicas conectadas a una grabadora de cassettes (VCR) donde las cintas que almacenan la información eran similares a las utilizadas en el hogar. Paulatinamente las soluciones se fueron digitalizando hasta llegar a sistemas que utilizan cámaras y computadoras para la gestión del video. Actualmente buscando aprovechar las mejores características de cada una de estas dos tecnologías, existen soluciones mixtas donde componentes digitales y analógicos conviven bajo un mismo entorno.

El sistema analógico más simple es el conocido como *circuito cerrado de televisión* (CCTV) el cual utiliza un VCR para almacenar el video proveniente de las cámaras conectadas al VCR por medio de un cable coaxial. En estos sistemas el video no se comprime, lo que ocasiona que las cintas de grabación puedan contener información en promedio de 8 horas. En soluciones donde se tienen más fuentes de video, es necesaria la existencia de multiplexores que permiten grabar el video proveniente de varias cámaras en una sola VCR y para vigilar es necesario colocar un monitor analógico directamente a la salida del componente de multiplexado.**(Ver Figura 6-1)**

[1] También denominado espectro de radiofrecuencia (RF), sección del espectro electromagnético en el que se pueden generar ondas electromagnéticas aplicando corriente alterna a una antena.

Figura 6-1. *Circuito cerrado de televisión*

Este tipo de sistemas CCTV ofrecen algunas ventajas con respecto a los sistemas digitales, debido a la inexistencia de compresión de video, las imágenes obtenidas son de mejor calidad así también el gasto en almacenamiento depende únicamente de la cantidad de cassettes necesitados. Las desventajas sobresalen al tener dificultades en la administración del video, costo de cableado del cable coaxial, grabación de eventos innecesarios, etc.

Otra alternativa de CCTV es aquel que utiliza un *grabador de video digital (DVR)* como medio de almacenamiento. En este tipo de sistemas las cintas de grabación utilizadas por el VCR serán reemplazadas por unidades de discos duros que almacenarán video digitalizado y comprimido, lo que ocasiona tener una unidad de almacenamiento robusta. La mayoría de los DVR ya incluyen de forma nativa multiplexores para integrar varias señales de video. **(Ver Figura 6-2)**

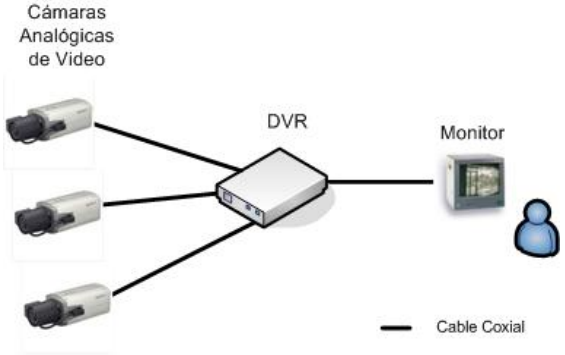


Figura 6-2. *CCTV con DVR analógico*

Una variación de la solución anterior es un CCTV utilizando un DVR IP. En esta solución las tareas de digitalización y compresión de imágenes son realizadas por el DVR, y el tipo de información obtenida de estos procesos puede ser transmitida a través de una red de datos IP para que se administre la información en una terminal remota. Este tipo de sistemas permiten disminuir el tiempo dedicado a las tareas de administración y configuración ya que evita realizar traslados al lugar donde se encuentra el DVR. **(Ver Figura 6-3)**

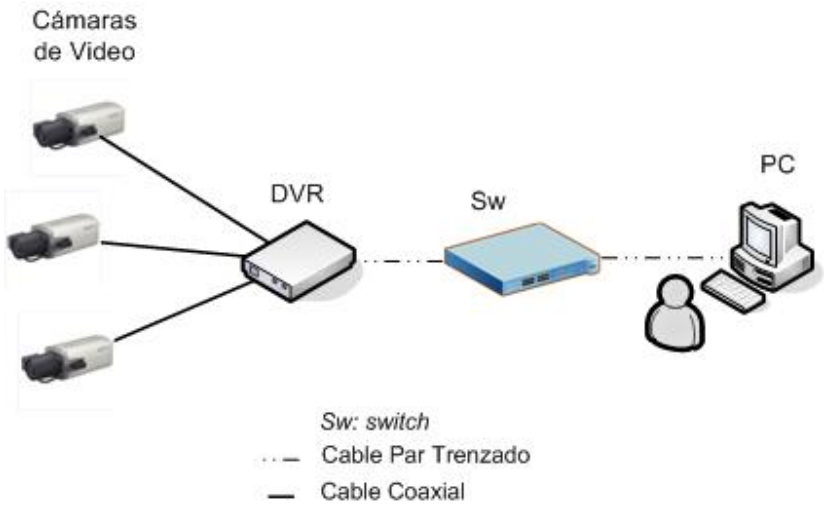


Figura 6-3. *CCTV con DVR IP*

Existen sistemas diseñados para la integración de tecnologías analógicas a los medios de transmisión utilizados en redes de datos, cámaras analógicas pueden ser aprovechadas en soluciones basadas en IP. Un módulo de codificado debe ser integrado al sistema que permita ofrecer nuevas funcionalidades al equipo analógico acordes a sistemas digitales. Ya digitalizada la señal, el módulo es conectado a la red en la cual se transmitirá el video para almacenamiento, monitoreo, administración, etc. A pesar de ser un sistema compuesto por cámaras analógicas, es considerado como un verdadero sistema de video IP ya que toda la estructura de comunicación y transporte se hace en ambientes IP. **(Ver Figura 6-4)**

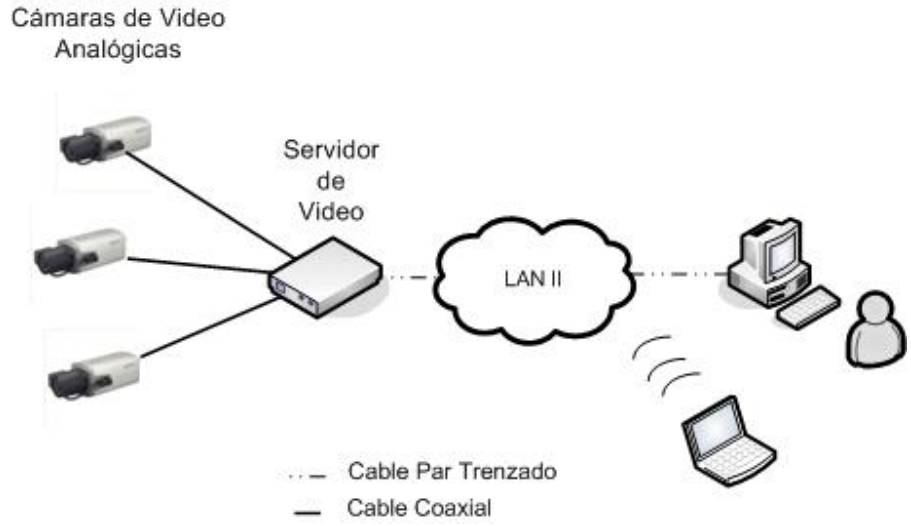


Figura 6-4. *Integración a la red de datos con un Servidor de Video*

Finalmente se tienen los sistemas puramente IP, en los cuales todos sus elementos son conectados a una red de datos, aquí las cámaras utilizadas son controladas por un software de gestión de video. Las ventajas ofrecidas por esta tecnología reciente son:

- Cámaras de alta resolución (del orden de megapixeles).
- Alimentación eléctrica de cámaras por medio del cable de comunicación, funcionalidad inalámbrica.
- Entradas y salidas digitales a través de IP junto con el video.
- Calidad de imagen constante.
- Funciones de Pan, Tilt y Zoom.
- Consulta y administración desde cualquier punto de la red o Internet.
  (Ver Figura 6-5)

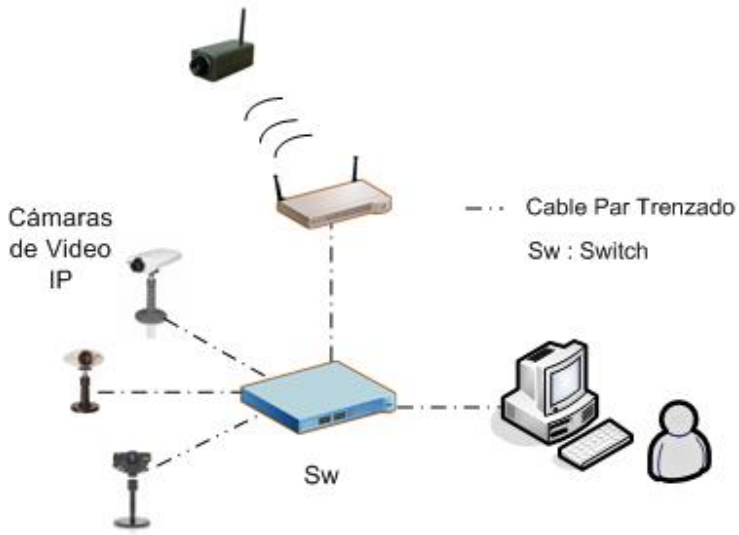


Figura 6-5. *Sistema de videovigilancia IP*

Hoy en día el protocolo de Internet IP es el protocolo de comunicación más utilizado en servicios multimedia; su utilización ha ido aumentando por la escalabilidad y flexibilidad que ofrece, es utilizado en soluciones de cualquier dimensión dejando siempre abierta la posibilidad de crecimiento de nuevos elementos. El video IP es una solución que permite a los usuarios administrar, controlar y grabar video a través de una red IP.

Los sistemas de video tradicionales basados en cable coaxial son limitados en muchos sentidos. El precio de instalación y mantenimiento en superficies grandes se vuelve alto así como el numero de estaciones de control ya que su crecimiento también implica aumento de costos por la necesidad de adquirir toda una estructura de monitoreo. La central de monitoreo o matriz también se ve afectada por sus limitantes de crecimiento dependientes de equipo nuevo. Por un momento, las soluciones basadas en DVR mejoraron la capacidad de almacenamiento pero con limitaciones, los equipos de grabación debían estar cerca de la central de monitoreo, a menudo las tasas de transmisión y la calidad de la imagen se veían afectados. La idea de una única solución integral que se pueda ampliar libremente y que ofrezca video de alta calidad en diversos lugares lo proporciona el video IP.

En general, para video IP no es necesario preocuparse por el crecimiento ya que los elementos que lo hacen posible (cámaras, PC's, servidores, etc.) pueden incorporarse a cualquier punto de red en cualquier momento. Así también el video IP puede ser manipulado por diferentes tecnologías de compresión y cifrado para la optimización del almacenamiento y el cifrado de la información; la vigilancia IP es una tecnología con la cual se puede obtener toda la funcionalidad de un sistema analógico y además de otras funcionalidades.

Gracias a los avances en manejo de video, hoy en día no hay dependencia de un medio único de transmisión, el transporte de las señales se realizan sobre redes típicas LAN y WAN sin perder capacidades de administración utilizadas con las antiguas soluciones analógicas basadas en enlaces dedicados. Actualmente, existe toda una gama de tecnologías que soportan el transporte video en pequeñas y grandes distancias (SONET/SDH, CableModem, DSL, ATM, MPLS/GMPL, RPR, Wireless, Ethernet), sin embargo, se buscará encaminar la transmisión de video a través de los enlaces que conforman la estructura de comunicación para voz y datos, con esta nueva adopción, por todos los tipos de señales que se transmiten, la convergencia definirá a la red como del tipo multimedia.

Como ya se mencionó, existen dos alternativas para transportar video dentro de las instalaciones del Instituto de Ingeniería: *red inalámbrica* y *red alámbrica*.

La red inalámbrica provee las mismas funcionalidades que el cableado fisco pero sin la necesidad de cables entre los dispositivos de comunicación; basada en el conjunto de protocolos TCP/IP esta tecnología ofrece ventajas cuando de video se trata. Si hablamos de un gran número de dispositivos de seguridad y monitoreo (cámaras, PDA, laptops, etc.), una comunicación inalámbrica permitiría una mayor flexibilidad en reubicación o portabilidad de dispositivos, limitando la administración del sistema a espacios donde exista cobertura del servicio. No obstante, los enlaces inalámbricos no son el medio ideal para transmitir video de *alta calidad* ya que la interferencia de señales en este tipo de medios es difícil de controlar; la interferencia en un enlace inalámbrico puede ocasionar errores en la información tales como: perdida de imágenes, distorsión, etc., que en cierto momento pueden ser de carácter crítico para la calidad del video.

Como ya se mencionó, la comunicación entre dispositivos inalámbricos (Standard 802.11), se realiza en las frecuencias de 2.5 GHz y 5GHz, estas bandas no están licenciadas formalmente en México, es decir, su utilización es libre, lo cual garantiza que otros usuarios utilicen las mismas frecuencias para satisfacer necesidades de comunicación, dando por resultando que la pequeñas variaciones en el ambiente local interfieran con el envío de señales.

Dentro del campo de la seguridad, la vigilancia IP inalámbrica es concretamente la unión de dos tecnologías independientes: videovigilancia en red y la transmisión inalámbrica de información, su unión permite ofrecer una solución alternativa de gran escalabilidad para integrar sistemas de seguridad y vigilancia. Las características que ofrece este tipo de

soluciones sin cables son su alto grado de disponibilidad, ahorro de instalación, operación y escalabilidad.

Cuando se presentan problemas de implantación, (costos elevados, problemas de instalación), la tecnología inalámbrica tiene algunas cualidades que le permiten ser considerada como una red de seguridad viable:

- **Instalación rápida**. La ubicación de cámaras puede ser prácticamente en cualquier sitio, siendo un proceso rápido comparado con los largos periodos de tiempo invertidos en una instalación de fibra óptica o cableado estructurado.
- **Costos.** Definitivamente los costos son muchos menores que una solución basada en fibra óptica, con la ventaja de poder llegar a lugares de difícil acceso para un medio físico.
- **Flexibilidad.** La movilidad de cámaras y dispositivos de monitoreo está comprobada ya que pueden ser reubicadas y estar reconectadas en un lapso de tiempo relativamente corto.
- **Alta capacidad.** Algunas redes manejan capacidades de ancho de banda suficientes para soportar video, asegurando la información necesaria para los sistemas de seguridad.

Una solución basada en videovigilancia IP y conexiones inalámbricas de transmisión permite la apertura a sistemas de seguridad que ya cuenten con cámaras analógicas, digitales o una combinación de estas, a través de elementos que ayudan a las tareas de procesamiento, de compresión, de ruteo, etc., por lo tanto no es necesario estar sujeto a las ultimas tecnologías por ser una solución relativamente nueva. [9]

Ante estas cualidades características de conexiones inalámbricas, podría ser una posibilidad inequívoca como medio de transmisión, no obstante, los resultados reales que ofrecen los enlaces inalámbricos no son tan acordes a los estándares ya que la inconsistencia de los medios es recurrente. Frente a estas circunstancias, algunas mejoras en las tecnologías inalámbricas han minimizado las debilidades de este tipo de enlaces. Primeramente diversos métodos de comprobación de errores permiten que información perdida o afectada en el proceso de envío sea retransmitida logrando que todas las imágenes lleguen al destino, como otra alternativa, la velocidad de envío se reduce buscando que tasas de transmisión bajas sean utilizadas para permitir el flujo confiable en el medio. Estas soluciones se vuelven eficientes en escenarios de datos donde la información puede ser reestructurada sin ser percibido por el usuario; sin embargo, cuando se hablan de soluciones basadas en video en tiempo real, la información debe ser continua y en tiempo, condición necesaria que no puede ser cumplida cuando se hacen reenvios de información. De igual manera, reduciendo considerablemente las tasas de transmisión, se perdería calidad del video por las necesidades propias de composición del video (secuencia de imágenes en tiempos definidos).

Sobre la seguridad de los datos, actualmente la vigilancia IP incluye medidas concretas de seguridad que permiten que la información no sea interceptada y visualizada en forma ilícita. Con la ayuda de firewalls y VPNs, la información que fluye a través de cualquier red es integra y el video nunca se ve afectado por factores externos ajenos al propio entrono de

seguridad. Otras medidas referentes al aseguramiento de los datos son: La autenticación que regularmente se hace en dos niveles, uno para el monitoreo y otro para tareas administrativas como configuración del sistema; La encriptación por medio del cifrado de la información, la mayoría de los fabricantes de componentes inalámbricos permiten transferir datos de forma segura, forzando a que solamente el destino pueda entender e interpretar la información.

El uso de la red inalámbrica como principal opción de transmisión de video debe ser considerado cuidadosamente para streams de video. El envío puede verse afectado por las variaciones en el ancho de banda disponible debido a interferencias comunes que se presentan en todo ambiente, las alternativas existen pero no son nada confiables. Naturalmente, las mejoras sobre estos detalles vendrán a futuro, pero hoy en día, no existe garantía en los enlaces inalámbricos que permitan considerarla como primera opción.

La otra alternativa del transito del video es a través de la red Ethernet de cableado estructurado la cual también utiliza el conjunto de protocolos TCP/IP como base del esquema de comunicación. Ya que los enlaces establecidos en redes IP han demostrado ser un medio eficaz para el envío y recepción de datos, se considera la mejor de las opciones cuando las cantidad de ancho de banda disponible es considerable y los dispositivos de red pueden tolerar métodos de transmisión de video IP. Con base en la tecnología Ethernet, la información referente a video se encuentra embebida dentro de paquetes IP, con lo cual se logra la transmisión de video a través de los mismos canales de comunicación por donde datos y voz coexisten. Sin embargo la convivencia no es tan simple como parece, ya que las posibilidades de saturación de ancho de banda o cuellos de botella se incrementan por la cantidad de información que contemplan las imágenes de video de alta calidad, a pesar de esto, Ethernet es una de las tecnologías para el transporte de paquetes IP en redes de área local que ha tenido un impacto positivo en soluciones de videovigilancia por los aspectos siguientes:

- Los sistemas de video IP pueden transmitir video sin la necesidad de una infraestructura propia y exclusiva. Aprovechan las redes IP locales e internet para transportar la información a cualquier lugar que así se necesite. Al añadir un sistema de video IP simplemente se aprovecha y se extiende la infraestructura de red para su funcionalidad con el video.
- En promedio una única cámara de video implica aproximadamente entre 0.2 y 2 Mbps de ancho de banda. Con base en esta idea, se puede considerar el número de cámaras a trabajar en un mismo enlace y de ser necesario, aprovechar los beneficios que una red de IP ofrece segmentando y separando a una red exclusiva para video en caso de utilizar un gran número de cámaras y codificadores. Para enlaces inalámbricos estas cantidades de información aun son excesivas de manejar por los estándares actualmente vigentes.
- Es posible enviar video en redes IP seguras con características de autentificación y encriptación, debido a que la información generada por un sistema de videovigilancia es crítico y de acceso restringido, este aspecto actualmente es utilizado en sistemas profesionales.

- La fiabilidad de los enlaces Ethernet la hace ser una tecnología disponible para transmisión de datos a pesar de que se trate de video. Realmente las fallas en funcionamiento son mínimas en periodos largos de tiempo, el enlace depende exclusivamente del estado físico de los enlaces y de configuraciones en los equipos de red.

La comparación directa entre un enlace inalámbrico y alambico no es una tarea fácil de definir debido a que en ambos existen ventajas y desventajas. No obstante, la elección del medio de transmisión se hará posteriormente y se basará en la experiencia adquirida en ambas redes del Instituto y de la integridad de sus enlaces.

6.1.1 Video en paquetes

Cualquier dato transmitido por medio de una red IP, necesita ser encapsulado en datagramas IP (paquetes IP). Por característica propia, los datagramas incluyen *encabezados* los cuales contienen información de control: direcciones IP origen y destino, TTL del paquete, prioridad del paquete y el protocolo que es usado para su transmisión. El rendimiento de las señales de video IP está relacionado directamente con el tamaño de los paquetes de video a enviar en la red. El tamaño del paquete dependerá del tipo de red utilizada (MTU[2]) y de los beneficios y desventajas que ofrece utilizar paquetes largos o cortos.

En paquetes largos como cortos, los encabezados son una parte esencial que no puede ser omitida, el utilizar paquetes cortos implicará que la información contenida tendrá que ser repetida en cada uno de estos paquetes, al contrario de un único paquete largo el cual contendrá una sola vez la información como parte de su encabezado, al final el ancho de banda puede ser aprovechado de mejor manera con mayor cantidad de streams de video. Otra ventaja es la disminución del procesado de cada uno de los paquetes. Cualquier paquete IP tiene que ser procesado por dispositivos de red para dirigirlos a los destinos correctos, este análisis se hace consultando la información de los encabezados, la carga en cada uno de estos dispositivos de enrutamiento se pueden amortiguar cuando la cantidad de paquetes se ve reducida, aunque actualmente los componentes de red tienen más poder de procesamiento, este beneficio no es completamente aprovechado en entornos de red donde existe una gran variedad de dispositivos de enlace. Una última ventaja es hacía el aprovechamiento de la utilización de la red. En muchas tecnologías de red tal como Ethernet, pequeños espacios son incluidos en cada envío de información, con paquetes grandes menor cantidad de espacios se generaran en el medio.

Una de las ventajas de utilizar paquetes pequeños es en la recuperación de paquetes perdidos, cuando se llega a ver afectado el encabezado del paquete, los streams de video son descartados y por lo tanto menor cantidad de información es perdida. Otra ventaja está en la reducción en tiempos de latencia. Un paquete no puede ser transmitido hasta que esté completamente integrado, con señales con muy poca cantidad de información, necesitarán mucho tiempo para conformar un paquete en su totalidad, provocando tiempos de espera

[2] *Maximun Transfer Unit* es la unidad máxima de transferencia que expresa el tamaño en bytes del datagrama más grande que puede pasar por una capa de un protocolo de comunicaciones. *Ejem* **Ethernet 1500bytes**

altos en todo el proceso de transmisión. Una última ventaja se da en la transmisión de los paquetes cuando se puede ver afectada su longitud. Cuando un paquete IP esta limitado a una longitud establecida por una máxima unidad de transferencia, existirá segmentación de paquetes lo que ocasionaría mayores cargas de trabajo para los dispositivos de red.

Por lo tanto, la longitud de los paquetes esta en función de varios aspectos, sin embargo se puede llegar a establecer un tamaño acorde a las características de la red sin que exista fragmentación de paquetes. Desafortunadamente algunos dispositivos IP no permiten la configuración directa de paquetes, en los sistemas de videovigilancia, el tamaño del stream depende de las cualidades definidas en las imágenes componentes del video, por ello es importante limitar la cantidad de información que la cámara de video enviará a través de la red de datos para minimizar consecuencias en su transporte.

6.1.2 Protocolos de Transporte de Video

Los protocolos de transporte son usados para controlar la transmisión de paquetes hacía destinos. El video en tiempo real se apoya en tres protocolos principalmente:

- **UDP** es de los protocolos más antiguos, es utilizado en aplicaciones de video donde la información es muy sensitiva al tiempo. Es un protocolo no orientado a conexión que puede soportar información transmitida a gran velocidad que es el caso para el video digital, sin embargo por ser un protocolo sin conexión implica un descontrol de envío entre el emisor y receptor, el envío se realiza por medio de una dirección IP y un puerto sin comprobar que la información fue recibida completamente y correctamente; por esta razón podría ser que UDP no fuera el protocolo adecuado para enviar video ya que la integridad del video puede verse afectada cuando el momento de desplegar las imágenes se presente. En el estándar NTSC, las imágenes deben ser presentadas cada 33ms (para PAL 40 ms), por lo tanto con la ausencia de datos de video el receptor necesitaría:

  1. Identificar el dato faltante.
  2. Notificar al emisor sobre el faltante para solicitar su retransmisión.
  3. Recibir y procesar el dato reenviado.
  4. Asegurarse de que la imagen sea presentada en su secuencia apropiada.

  Considerando que esto se debe realizar antes de 33ms, se ha buscado la manera de remediar este problema, enviar información antes de ser necesitada ha sido una alternativa para esta situación en particular; el video es acumulado en una unidad de almacenamiento momentánea (buffer) la cual permitirá recabar información temporalmente y darle la oportunidad al receptor de solicitar una retransmisión si así lo necesitara. No obstante, el uso de un buffer no es tan factible en situaciones donde los datos tan pronto como son originados deben ser presentados (videoconferencia) ya que existe un retraso de la señal cuando se lleva a cabo el almacenamiento temporal.

  Algunas de las ventajas y desventajas de utilizar UDP son:

· Ventajas
- Ya que UDP no ofrece confiabilidad ni estado en sus conexiones, los paquetes son más pequeños que TCP.
- Permite responder peticiones en forma rápida por su estado no definido de conexión. No es necesario esperar a establecer la conexión entre los dos puntos de comunicación, ni una notificación del receptor sobre la integridad de la información.
- Puede ser utilizado en aplicaciones multicasting porque no necesita establecer una comunicación entre dos puntos.

· Desventajas
- Este protocolo no tiene un mecanismo propio para retransmitir automáticamente datos dañados o perdidos en la transmisión, dejando la responsabilidad al receptor de adecuar los datos e interpretar errores.
- En la mayoría de los firewalls la transmisión por UDP no esta permitida, por la inseguridad que ofrece tratar con paquetes que no se sabe su origen.
- Es responsabilidad de la aplicación asegurarse que los datos no excedan la capacidad de flujo de datos del medio de transmisión.

Finalmente, cuando los formatos de video utilizados contienen su propia corrección de errores (MPEG con Reed-Solomon[3]), cuando los medios de transmisión no están saturados y los retrasos de comunicación se desean minimizar, UDP puede ser una elección viable para el transporte de video.

- **TCP**. Este protocolo es el más utilizado en la mayoría de redes de datos, incluso en Internet ha tenido un auge por el tipo de comunicación confiable que genera en sus conexiones. Una conexión orientada necesita establecer un enlace entre emisor y receptor antes que cualquier transmisión de datos se realice. Como parte de este tipo de conexión, continuos mensajes de estado (acknowledgment) deben ser intercambiados desde inicio hasta el final del envío para asegurar la integridad de la información. Una de las principales cualidades de TCP es su capacidad de recuperación ante errores. Los paquetes bajo este protocolo contienen información que los identifica dentro de toda una secuencia de presentación (Sequence Identifier). Cuando un paquete es perdido o llega al destino en orden equivocado, la continuidad de la información se ve interrumpida, por lo tanto el receptor realiza un reporte de notificación sobre el paquete perdido para su reenvío. De esta manera TCP asegura que todos los datos enviados sean recibidos permitiendo la confiabilidad e integridad de información como el video.

  TCP puede controlar el flujo de datos a través de una conexión con el uso de bits de estado y de un buffer receptor en el otro lado de la conexión. El receptor informa al emisor el tamaño de buffer utilizado, esta notificación permite al emisor controlar la cantidad de datos y la velocidad de envío tiene la responsabilidad de no sobrepasar el tamaño reportado. El flujo de información toma un rol muy importante porque el emisor debe actuar ante las notificaciones del receptor sobre que tan rápido pude aceptar y

[3] Código de corrección de errores que se incluye en los paquetes transmitidos, la longitud del código es de 16 a 20 bytes los cuales permiten al destinatario la posibilidad de rehacer datos erróneos.

procesar información, estas variaciones dependen directamente del estado de tránsito en la red por donde fluye la información o por otras diferentes tareas que en ese momento el receptor este realizando. Siempre que el emisor conoce un estado de saturación en el buffer destino, retardará el envío de nuevos datos hasta que los existentes hayan sido procesados y el receptor haya terminado sus funciones.

Ya que en una solución de video el arribo de video no solamente debe ser intacto sino a tiempo la transmisión por TCP puede interferir con el transporte de video. Por lo tanto un proceso que retransmite información puede ser perjudicial en tres maneras:

- Si un paquete es retransmitido demasiado tarde para su secuencia de utilización, el receptor puede verse ocupado innecesariamente analizando un paquete que no tendrá ya utilidad.
- Cuando los paquetes son retransmitidos, estos ocupan ancho de banda que podría ser utilizado por información útil.
- Como ya se señaló, las propias características de TCP pueden interferir en el transporte de video, la reducción en las tasas de envío pueden afectar el despliegue de video en tiempo real.

TCP puede ser una ventaja cuando el despliegue de video en múltiples destinos es necesario. Cualquier conexión en TCP debe establecerse a través de un *socket*, este par único permitirá realizar un sin numero de conexiones si y solo si este socket no es utilizado por alguna otra conexión en el mismo host, es decir, una conexión al socket 192.168.1.2:80 no puede duplicarse desde un mismo origen; una conexión al mismo socket puede hacerse desde otro origen distinto. Al contrario de UDP el cual combina todo un flujo de datos por un único puerto.

Algunas ventajas y desventajas de utilizar TCP son:

- Ventajas
  - Puede realizar retransmisión de datos en automático, sus propios mecanismos aseguran que cada byte de datos transmitidos por el emisor lleguen a su destino. Si algún dato se pierde o es corrompido en el trayecto, TCP retransmitirá el dato.
  - La secuencia numerada que cada uno de los paquetes permite determinar que datos son los ausentes o si llegan en forma diferente a como fueron enviados.
  - Conexiones simultaneas múltiples pueden ser realizadas por medio de un solo puerto, lo que permite a múltiples peticiones sean atendidas al mismo tiempo quitando carga a un servidor o la misma cámara.
  - La seguridad de integridad de cualquier dispositivo IP a cualquier red por medio de TCP.
  -
- Desventajas
  - El establecimiento de la conexión debe estar completada para el comienzo del envío de información, esto puede ser una desventaja cuando la confiabilidad no es total.

- Por sus propios mecanismos de control, TCP disminuirá las velocidades de flujo cuando errores se presenten. Si estas velocidades son menores a aquellas necesitadas por la señal de video, entonces los resultados se verán considerablemente afectados.
- TCP no soporta multicasting debido al *handshaking*[4], por lo tanto, una conexión separada necesita ser establecida por el emisor hacía cada uno de sus destinos.

TCP es un protocolo muy utilizado en la actualidad por una gran cantidad de servicios. Para aplicaciones que implican video, es una posibilidad que permite tener información completa e integra que para efectos de seguridad es de las características más importantes, la confiabilidad de la información se vuelve una razón de peso para cualquier sistema de videovigilancia.

- **RTP.** Este protocolo es utilizado en aplicaciones multimedia de tiempo real, tales como voz y video en Internet. En RTP el tiempo de transmisión es prioridad. Para aplicaciones de tiempo real, los tiempos de llegada de información es primordial a una perdida o a un retraso de datos, ya que si el periodo de entrega no es el adecuado no se puede tener una señal integra utilizable por el destino, así la perdida de paquetes puede ser de mejor manera tolerado que retrasos en la señal. RTP se basa en proveer señales de video y audio en tiempos exactos en redes IP. Los errores que se puedan presentar en el envío de datos o la perdida de información no son retransmitidos y el flujo de datos no es variable según la saturación del medio como TCP lo hace en redes congestionadas.

  Este protocolo no es exactamente un protocolo de transporte, como UDP o TCP, de hecho, RTP se ayuda de UDP como método de transporte. Los paquetes RTP se encapsulan en paquetes UDP para su transmisión. RTP permite la utilización de dispositivos llamados *mezcladores*. Un mezclador es un programa intermedio que con la ayuda de otro protocolo de control, recibe paquetes de uno o más orígenes para generar una sola señal RTP, en este proceso se realizan ajustes de secuencia, marcas de tiempo, etc.

  Como un componente de RTP, se encuentra RTCP (RTP Control Protocol), el cual es utilizado siempre que una conexión RTP es realizada. Esta conexión es realizada usando un puerto continuo al utilizado por RTP, es decir, si una conexión RTP utiliza el puerto 1380, entonces la conexión RTCP utilizará el puerto 1381. El protocolo RTCP realiza las siguientes funciones:

  - Permite la sincronización entre diferentes medios de audio y video. RTCP maneja indicadores de tiempo los cuales son usados para sincronizar cada stream RTP y formar una señal compuesta con audio y video.
  - Proporciona reportes de estado acerca de cómo los datos enviados por el emisor están siendo obtenidos por el receptor por medio de estadísticas. En estas se incluye información como el número de paquetes perdidos o el tiempo de llegada de paquetes,

[4] Proceso en el que la información se transmite entre los dispositivos de origen y destino para mantener y coordinar el flujo de datos entre ellos. Un handshaking apropiado asegura que el dispositivo de destino estará listo para aceptar datos antes de que el dispositivo origen transmita.

- simplemente con el objetivo de comunicar los retrasos de transmisión presentados en la red.
- En sesiones RTP, donde varios participantes interactúan, RTCP realiza la identificación de los implicados para determinar nuevos elementos para ingreso y contabilizar los receptores presentes.

Algunas ventajas y desventajas de utilizar RTP son:

· Ventajas
- RTP soporta diferentes formatos de audio y video lo que permite compartir fácilmente diferentes tipos de audio con una gran variedad de formatos de video.
- Los números identificadores de secuencia en paquetes permite al receptor identificar cuando hay paquetes faltantes. Estos números permiten restablecer el orden adecuado de los paquetes en caso de su arribo desordenado.
- Los streams RTP pueden ser distribuidos usando multicasting, así un solo origen puede proveer a muchos destinos simultáneamente.
- Los datos para control de sincronización permite a múltiples señales multimedia ser transmitidas separadamente y ser estructuras en su forma correcta según una misma secuencia de tiempo.
- El receptor puede optar por decodificar solo una parte de la señal multimedia, así dispositivos con conexiones lentas pueden escoger solo el audio para mejorar el desempeño.

· Desventajas
- Algunos firewalls bloquean tráfico RTP por estar contenidos en paquetes UDP.
- No hay un mecanismo para establecer prioridades en el tiempo de transporte propio de paquetes RTP. Diferentes técnicas deben ser utilizadas para que puedan fluir aceptablemente en redes congestionadas.

Finalmente RTP es un protocolo que complementa lo no deseado por el protocolo TCP. Por ejemplo, RTP no disminuye la velocidad de transmisión cuando el medio no es el adecuado sino que provee información a la aplicación que envía para conocer el estado de congestión. Con esto el emisor puede determinar que hacer para compensar el estado no propio del medio, por ejemplo, sacrificar calidad o ignorar los estados del reporte cuando los receptores son mínimos. Finalmente RTP soporta multicasting el cual puede ser una de las más notorias ventajas en redes donde se transporta video.

6.2 Selección del Método de Transmisión del Video

Hasta este momento se han estudiado todo un ambiente relacionado con el video, desde su origen hasta lo necesario para su transmisión. Sin embargo, formalmente no se han mencionado todos los beneficios que puede ofrecer un sistema de video IP con respecto a sistemas de circuitos cerrados de televisión analógicos.

En términos de **escalabilidad** se tienen las siguientes ventajas:

Primeramente, los sistemas tradicionales de video basados en cable coaxial son limitados en su crecimiento. Por la necesidad de tender cableado a cada una de las cámaras de monitoreo, el crecimiento se ve limitado con superficies grandes debido a la inversión requerida para hacer llegar las señales de cámaras a aquellos lugares donde quieran ser monitoreadas, considerado también que la calidad de la imagen está en función de la longitud del cable, en espacios demasiado amplios habrá que considerar elementos que permitan amplificar la señal para conservar la información.

En segundo lugar, el video IP puede crecer según las necesidades que se vayan presentando. A pesar de que la tecnología analógica adopto DVR's para mejorar sus capacidades de grabación, un sistema de este tipo normalmente permite un número específico de cámaras (4, 9, 16, 32). Si un sistema contempla 15 cámaras, basta con adquirir un grabador de 16 canales de entrada para satisfacer el requerimiento con una cámara a crecer, el problema existe cuando son necesarias 17 cámaras, se necesitaría adquirir otra unidad de grabación complementaria. Los sistemas basados en IP tratan a cámaras IP como dispositivos de red los cuales pueden ser adquiridos en incrementos unitarios. Como parte de esto, una solución basada en IP, puede controlar las capacidades de gestión de cámaras. Si se necesita tener un frame rate de 30 en cada una de las cámaras, entonces el número de cámaras a gestionar se ve reducida (probablemente 25), no obstante, si son suficientes 2fps para algunas cámaras se podrá administrar una mayor cantidad de ellas (por encima de 100), a reserva de lo que la aplicación de gestión de video indique.

Finalmente, cuando se necesiten administrar un mayor número de cámaras, por ser soluciones basadas en servidor como medio de control, a este se le pueden incorporar nuevas elementos de hardware (aumento de memoria, disco duro, etc.) para soportar la escalabilidad de la solución, al contrario de una solución basada en un grabador digital donde el dispositivo esta limitado a sus características de fábrica sin posibilidad de crecimiento.

En términos de **control de imágenes** se tienen las siguientes ventajas:

Un sistema IP permite el manejo de velocidad en imágenes, a diferencia del video analógico donde la transmisión de imagen es definida a un número constante de imágenes por segundo. La principal cualidad es la posibilidad de poder evitar la transmisión de video innecesario a través de la red. En una solución IP la transmisión puede ser ajustada para aumentar la velocidad del flujo de imágenes de acuerdo a un evento o en detección de actividad. Con esto se garantiza que el medio no este siendo saturado por información redundante y las unidades de almacenamiento se ven optimizadas con información solamente útil.

Diferentes velocidades de transmisión pueden ser adecuadas a la capacidad del enlace por el cual se establece una conexión. Un usuario remoto conectado por Internet puede solicitar envío de video a un frame rate mínimo y al mismo tiempo un usuario dentro de la red puede solicitar la misma información a un frame rate de 25 a 30 imágenes por segundo.

En términos de **disponibilidad** se tienen las siguientes ventajas:

Hoy en día servicios de voz, video y datos están convergiendo hacía una misma plataforma de IP por todas las razones ya mencionadas. Cuando se busca que información multimedia coexista bajo un mismo entorno, es necesario controlar la disponibilidad del medio de transmisión y satisfacer los requisitos de cada servicio.

Calidad de Servicio (QoS), hace referencia a diversas tecnologías que garantizan calidad a cada uno de los servicios de red existentes, donde distintas aplicaciones de red pueden coexistir en la misma red sin consumir ancho de banda de la otra. QoS ofrece:

- La posibilidad de priorizar el tráfico permitiendo que los flujos más importantes tengan preferencia con respecto a los de menor prioridad.
- La fiabilidad de la red es mayor ya que la cantidad de ancho de banda que se puede utilizar esta limitado a los requerimientos de la aplicación, permitiendo que cualquier tipo de información llegue a su destino según las necesidades propias.

Para lograr QoS es importante que tanto los dispositivos de red como los componentes de video IP lo soporten.

El termino *Clases de Servicio* esta ligado al concepto de QoS; las clases son utilizadas para brindar diferente nivel de servicio de acuerdo al tipo de dato. La asignación de prioridades esta en función del tipo de información a enviar; un correo electrónico se le puede asignar un QoS de mucho menor valor con respecto a mensajes de control y mantenimiento del estado de la red o una aplicación en tiempo real que se este ejecutando. El parámetro de asignación de servicio para el video depende directamente de la importancia que tenga la solución de videovigilancia con respecto a los otros servicios ofrecidos en la red.

Cuando se necesita que el video se presente adecuadamente a los usuarios en una concurrida red, es necesario asignar una clase de servicio de alta disponibilidad para el tráfico del video, configurando a los dispositivos de red a dar prioridad a aquellos paquetes referentes a video para que puedan presentarse en los lugares de consulta o almacenamiento. A continuación se explica como se establecen prioridades ante la presencia de diferentes datos:

Primeramente, cada vez que la salida está disponible, un paquete es seleccionado de una de las tres entradas, si ningún paquete está disponible entonces no se realiza el envío.

En segundo lugar, si un paquete de alta prioridad está disponible, entonces este es enviado inmediatamente.

Si un paquete de alta prioridad está disponible existiendo uno de mediana prioridad o de baja prioridad, el paquete con mayor prioridad sigue teniendo preferencia de envío.

Si no hay existencia de paquetes de alta prioridad y si los hay para mediana y baja prioridad, entonces los datos son enviados en una secuencia de tres paquetes de mediana prioridad con uno de baja prioridad.

Por un lado, asignar el video siempre como de prioridad mayor ocasionaría que otro tipo de paquetes dependieran de la existencia de paquetes de video para su transmisión que es retraso de la información. Por otro lado asignar una clase de servicio como de baja prioridad para el video provocaría perdida y retraso en los paquetes en redes saturadas, que va en contra de las solicitudes para tener video de calidad. Una prioridad media podría ser una buena opción para el video en un entorno IP junto con una prioridad baja a datos no referentes a video.

La asignación de clases de servicio es una buena opción para permitir el flujo confiable del video en una red IP, esta opción acompañada con redes privadas virtuales podría establecer un verdadero control cuando el transporte de video se realice.

En términos de **gestión y seguridad** se tienen las siguientes ventajas:

Una de las mejores características que ofrece una solución basada en IP es la posibilidad de acceso al video en vivo en cualquier momento y en cualquier lugar. Así también el video puede ser almacenado en ubicaciones remotas por razones de seguridad e integridad de la información y consultarla a distancia. La posibilidad de acceder a los datos de video se limita a una conexión de red y una computadora.

En el ámbito de la seguridad, la vigilancia en IP permite utilizar información para su transmisión segura a través de tres pasos: *Autenticación, Autorización y Privacidad.* Primeramente la autenticación permite realizar una identificación ante el sistema proporcionando credenciales de acceso que arrojaran la validación. Posteriormente en la etapa de autorización se coteja la identidad proporcionada con respecto a una base de datos de identidades la cual delimita las restricciones dentro del sistema, aquí el usuario ya se encuentra conectado y listo para hacer peticiones de información o configuración. Finalmente la confidencialidad se realiza en el nivel de privacidad donde los datos enviados entre la aplicación de administración y los dispositivos de monitoreo (cámaras, servidores de video) pueden ser encriptados para evitar que otras personas puedan usar o leer la información (VPN o SSL).

Una vez fundamentado el medio por el cual será enviada nuestra información generada por las cámaras de monitoreo, es importante mencionar la manera en que el video será enviado al software de gestión o a consolas de monitoreo, que son finalmente, las dos opciones en que se puede utilizar la información en video. Cuando se tratan de conexiones individuales, sin ninguna difusión masiva, es indispensable la utilización de enlaces unicasting que permitan realizar una conexión punto a punto permitiendo que los datos sean dirigidos solo a un destino y ningún otro elemento de comunicación necesitará procesar la información.

La posibilidad de utilizar un método de transmisión de multicasting se ve delimitada por muchos factores. En una solución de videovigilancia donde la información tiene un valor

critico y privado y no se busca llegar a una gran variedad de destinos, regularmente cámaras o codificadores reportan hacía una sola central donde se lleva su presentación y probablemente su almacenamiento. Comúnmente una aplicación basada en multicasting es indispensable cuando se desea llevar *streaming de video*, en este escenario la visualización necesita ser realizada en toda una comunidad haciendo inviable la opción de unicasting por las cantidades de información que tendrían que ser generadas por el servidor de streaming. Así también, los dispositivos de red deben soportar envíos multicasting cuando así se requiera, como este tipo de técnicas de transmisión genera una fuerte carga de trabajo en dichos elementos de red, predeterminadamente este beneficio no está a disposición de utilizarse en la mayoría de los dispositivos.

La última posibilidad y nunca utilizada en aplicaciones de video es broadcasting, con esta técnica, los medios de transmisión se saturarían con datos de video dirigidos a destinos sin solicitarlos, la información es enviada de un solo punto a todos los puntos en la red, lo que sería catastrófico aun para una red de alta disponibilidad. Regularmente esta práctica se realiza en segmentos de red determinados o hacía otro tipo de aplicaciones.

El protocolo utilizado para transportar el video dependerá de las cualidades propias de las cámaras. Actualmente los fabricantes permiten optimizar los envíos de video dependiendo del formato de compresión utilizado. Nativamente toda información generada será enviada por medio de TCP que es un protocolo eficaz y confiable, así también las soluciones tienden a utilizar los métodos de compresión más avanzados MPEG-4 junto con protocolos de transporte como RTP, con lo cual se logra controlar los dos puntos más críticos en una solución de video vigilancia: el ancho de banda y almacenamiento.

6.3 Elección del Formato de Video

La importancia de elección de un formato se vuelve de las partes más importantes en el diseño de un sistema de seguridad. Primeramente la elección afectará directamente al proceso de transmisión de video a través de la red, considerando que menores cantidades de información transitan en la red, mayor disponibilidad y eficiencia habrá en los enlaces. En segundo lugar está la calidad de la imagen que es evidentemente una característica primordial que habrá que preservar en sistemas de videovigilancia, seguridad y administración remota, en los cuales pueden estar en riesgo la integridad de personas y bienes. Finalmente está el factor almacenamiento el cual puede disparar los costos de la solución por ser la parte más sensible económicamente hablando.

El formato de video está directamente relacionado con la manera en que se guardan los datos en el fichero y la compresión algorítmica utilizada para comprimir dichos datos. Para sistemas seguridad, el transporte de video se basa en dos tipos de compresión principalmente M-JPEG y MPEG-4. Estos métodos ofrecen una relación de calidad y compresión aceptable que permite atenuar la saturación de los medios que origina el video.

Primeramente se encuentra el formato M-JPEG que interpreta al video como una secuencia de imágenes, actualmente es el estándar más utilizado en sistemas de video IP. Una cámara IP realiza captura de imágenes individuales y las comprime en formato JPEG, al capturar una gran secuencia de imágenes en tiempos reducidos (30fps) y enviarlas hasta un lugar de visualización, la percepción será una imagen animada. Ya que cada imagen JPEG surgió de un mismo origen, la calidad y nivel de compresión será homogéneo en el video resultante.

Las principales ventajas de utilizar M-JPEG son la facilidad de comprimir imágenes por hardware y su capacidad de soportar cualquier tamaño de video para transmitir. Esto implica poder utilizar resoluciones QCIF hasta HDTV (1920 x 1080). La arquitectura M-JPEG utiliza imágenes normales JPEG sin información entre ellas, lo que implica que los errores de transmisión o perdidas de información solo afecta a una sola imagen. Cuando se presenta una perdida mayor, los usuarios podrán percibir retardos o degradación en la imagen. Dentro de las capacidades para M -JPEG

Sin embargo desventajas como interoperabilidad con tecnologías recientes y la carencia de productos que lo usan por la aparición de nuevos métodos para comprimir, han ocasionado que este formato sea una opción alternativa confiable pero no primordial. Para las cámaras de monitoreo de seguridad, esta solución es una verdadera opción para el envío de información por ser una tecnología no restringida para sus códecs. Es decir se puede realizar el envío de imágenes sin necesidad de instalar decodificadores propietarios que recuperen la información.

A partir de la creación de técnicas de compresión básicas como M-JPEG, Moving Pictures Experts Group desarrollo técnicas de compresión dirigidas completamente hacía video, llegado a ser MPEG, el método más frecuentemente utilizado en la actualidad por muchas aplicaciones. Este grupo desarrollo no solamente métodos de compresión para video (MPEG-1, MPEG-2, MPEG-4), sino también elaboró métodos de compresión para audio de gran capacidad. Hoy en día está asociación continua elaborando y mejorando los métodos de compresión hacía MPEG-7, MPEG-21 y Advance Video Coding (AVC) como una actualización del mismo MPEG-4.

Actualmente de toda la familia MPEG, MPEG-4 es el método de compresión más efectivo, base hoy de la mayoría de los esquemas de seguridad en transporte de video digital IP. Mucha de su tecnología de compresión fue desarrollada a partir de MPEG-2, donde se incluyeron nuevas formas de codificar no solamente video sino otro tipo de elementos que pueden ser utilizados tales como animaciones o texto. A pesar de incluir más tareas de codificación, los diseñadores han podido incrementar la calidad de imágenes en menores anchos de banda con respecto a los productos basados en MPEG-2.

Dentro de todas las mejoras que contiene MPEG-4, todas buscan converger hacía la mayor disponibilidad de los medios de transmisión. Primeramente los objetos componentes de una imagen pueden ser interpretados independientemente. En una secuencia de video cotidiana, MPEG-2 trataría los pixeles que conforman la imagen como parte de un todo y codificaría la imagen con base en los estándares de compresión existente DCT. Sin embargo, MPEG-4 puede manipular los objetos de la imagen como únicos, permitiendo así que en cierto

momento, el decodificador pueda recurrir al codificador en busca de información sobre la interpretación de las imágenes de la manera más simple. Otra de las ventajas es la utilización de macroblocks de tamaño variable, con esto, pequeños macroblocks pueden utilizarse en zonas finas de la imagen; permitiendo que mayores bloques sean usados y codificados con menor cantidad de bits si los pixeles en porciones de la imagen son similares. Así también la utilización de compresión fractal como una alternativa matemática a DCT y que los frames de tipo B puedan utilizar otros frames B para reducir la necesidad de frames P para reducir anchos de banda.

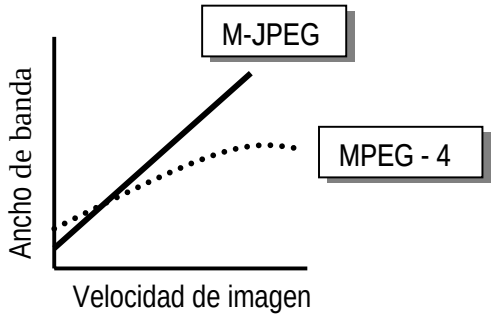
Una característica también muy importante es la posibilidad de formar una imagen con componentes de múltiples orígenes, lo que permite obtener video con muchas características como gráficos, comentarios, etc.

MPEG-4 (Parte 10) es la nueva técnica de compresión de video, o también conocido como AVC o H.264. Con este nuevo estándar se busca lograr tasas de compresión mucho más elevadas en tasas de bit menores. Aun no disponible para sistemas de videovigilancia.

6.1.3 Ventajas e Inconvenientes

M-JPEG es un estándar altamente utilizado en cámaras de monitoreo IP, por su simplicidad y la forma de tratar las imágenes individualmente. Es evidente que puede existir un retraso en el proceso de obtención de la imagen, codificación, compresión, transmisión, decodificación y representación pero sin afectar críticamente los tiempos de espera. Con todo esto se puede hacer notar que M-JPEG es una opción real para procesamiento de imágenes en detección de movimiento y seguimiento de un objeto. Así como para ser representada en cualquier resolución de imagen existente. Este estándar garantiza la calidad de la imagen sin importar las características existentes aunado a su flexibilidad para seleccionar la calidad de la imagen con el control del nivel de compresión. A pesar de esto, M-JPEG genera relativamente una gran cantidad de datos para hacer envíos en red en medios limitados.

Cuando se trata de enviar un volumen de datos menor por unidad de tiempo MPEG -4 es mucho más eficiente por su complejidad de codificación y decodificación. Sin embargo por esta misma característica los tiempos de espera son más elevados que M-JPEG. A continuación se hace una representación de la comparación en el uso de ancho de banda entre ambos estándares.



Como se puede observar en la gráfica anterior, donde el movimiento en la imagen no existe y la compresión MPEG -4 no puede utilizar similitudes entre imágenes, M-JPEG utiliza mejor el ancho de banda, no obstante a medida que el incremento de movimiento en la imagen aumenta MPEG-4 es más eficiente.

Actualmente algunos modelos de cámaras utilizan como método de compresión ambos estándares, buscando que el usuario final tenga opciones para obtener video. La siguiente tabla es un ejemplo ilustrativo acerca del envío de información desde una misma cámara origen hacía un destino utilizando los dos estándares.

El análisis se basó en calcular el tiempo que tarda un archivo de 8MB en ser saturado de información utilizando los dos métodos de compresión mencionados. Así también se busco identificar los protocolos de transmisión utilizados y el tipo de envío realizado.

Tipo de Formato	**MJPEG**
Tamaño del archivo **[MB]**	8
Duarción de la captura **[s]**	17
Total de Bytes	8,103,893
Total de Paquetes	7,903
Bytes por segundo	453,897
Paquetes por segundo	442
Porcentaje de utilización	3%
Ancho de banda disponible **[Mbps]**	100
Paquetes broadcast MAC	0
Paquetes multicast MAC	0
Paquetes IP	7,903
Bytes IP	8,103,893
Paquetes broadcast IP	0
Paquetes multicast IP	0
Paquetes TCP	7,903
Bytes TCP	8,103,893
Paquetes UDP	0
Bytes UDP	0

Tipo de Formato	**MPEG 4**
Tamaño del archivo **[MB]**	8
Duarción de la captura **[s]**	22
Total de Bytes	8,183,285
Total de Paquetes	5,690
Bytes por segundo	370,854
Paquetes por segundo	257
Porcentaje de utilización	3%
Ancho de banda disponible **[Mbps]**	100
Paquetes broadcast MAC	0
Paquetes multicast MAC	0
Paquetes IP	5,690
Bytes IP	8,183,285
Paquetes broadcast IP	0
Paquetes multicast IP	0
Paquetes TCP	3
Bytes TCP	381
Paquetes UDP	5,687
Bytes UDP	8,182,904

Como se puede apreciar, cuando se utiliza video en compresión M-JPEG la capacidad de almacenamiento se cubre de forma más rápida a través de paquetes TCP con un envío unicast. Por otro lado MPEG–4 tarda más en llegar a la cuota (5seg) utilizando envío de paquetes UDP con unicast.

Finalmente se pude mencionar que ambos tipos de compresión son útiles bajo ciertos escenarios, cuando exista un movimiento continuo de las imágenes, lo ideal es utilizar MPEG – 4 como estándar. Así también cuando se trate de imágenes fijas donde los cambios de imágenes no sean constantes (lugar apartado de movimiento vehicular o peatonal) lo más factible sería M–JPEG.

6.4 Evaluación de Cámaras IP de Video

Dentro de los sistemas de vigilancia en video existen una gran cantidad de opciones en cámaras IP para diversas necesidades. Como ya se ha mencionado, las cámaras analógicas están siendo desplazadas por cámaras IP por sus facilidades de integración en cualquier escenario de videovigilancia.

Existen una gran cantidad de fabricantes de cámaras de video que buscan desarrollar constantemente nuevas capacidades que permitan al usuario tener herramientas cada vez más eficientes con respecto al tratamiento del video. En general, la mayoría de los fabricantes clasifican las cámaras IP de acuerdo a sus características y propiedades existiendo los siguientes tipos:

- *Cámaras Fijas*. Este tipo de cámaras esta conformado por un cuerpo rígido que permite una configuración directa de la visión, este tipo de cámara es visible así como la posición a la que apunta por lo tanto puede ser una buena opción cuando se busca disuadir personas o monitorear un lugar fijo de suma importancia. La mayoría de estas cámaras permiten intercambiar su lente según las características del lugar a monitorear. Para protección propia de la cámara se le protege con carcasas diseñadas para exteriores o interiores (*housing*).según sea el caso.

- *Cámaras IP Domo Fijas.* Este tipo de cámara son conocidas como *mini domo* por su ubicación en una pequeña carcasa. La cámara permite enfocar a cualquier punto seleccionado. Su utilización está dirigido hacía aplicaciones donde la discreción es lo principal. Probablemente una de sus desventajas es el espacio tan reducido en el que se encuentran, lo que no permite intercambios en sus componentes según los requerimientos.

- *Cámaras IP PTZ.* Este tipo de cámaras también es conocido como *robóticas*, termino asignado por su capacidad de movimiento horizontal (pan), vertical (tilt) y acercamiento (zoom). Esta cámara es utilizada en regiones amplias donde es necesario seguir movimientos, sus capacidades actuales de zoom[5] (18x hasta 32x) permiten que los reconocimientos sean bastante rápidos y de gran calidad.

- *Cámaras IP domo.* Estas cámaras fueron diseñadas bajo la misma idea de las domo fijas: permitir la discreción y mesura en sistemas de grabación. Una cámara IP domo añade la ventaja de poder permitir una rotación de 360° horizontalmente, lo que permite sustituir a 10 cámaras fijas para realizar el mismo trabajo. Sin embargo una de sus desventajas es que solamente puede supervisar una ubicación al momento lo que la hace una cámara no confiable por los espacios críticos que puede dejar de cubrir.

[5] Actualmente las cámaras IP manejan dos tipos de zoom. En primer lugar se encuentra el zoom óptico, el cual permite hacer un acercamiento natural gracias a las capacidades ópticas del lente. En segundo lugar se encuentra el zoom digital, el cual es logrado por el software de gestión de video el cual utiliza una imagen y realiza el acercamiento electrónico.

· *Cámaras IP PTZ no Mecánicas*. Esta tecnología es la más reciente con respecto a cámaras IP de vigilancia. Esta cámara permite abarcar zonas entre 140° y 360° sin necesidad de realizar movimientos mecánicos, lo que se vuelve una ventaja por el no desgaste de piezas móviles. Este tipo de cámaras son de gran resolución (hasta 3 Mega píxeles) lo que permite tener imágenes completamente entendibles.

6.4.1 Componentes de las cámaras IP

Las cámaras de video se basan en los mismos componentes básicos que las cámaras analógicas o de fotografía, sus capacidades de interpretar imágenes y utilizarlas para su presentación son las mismas, sin embargo las tecnologías de codificación y compresión se le han asignado como tarea a la propia cámara lo que la hace un elemento mucho más complejo con módulos dedicados.

Hablando de lentes, existen dos categorías *C-Mount* y *CS-Mount* su composición es la misma pero su principal diferencia es la distancia que existe con el sensor de la cámara. Para CS-mount la distancia existente es de 12.5 mm. y para C-mount es 17.5 mm. Existen adaptadores que permiten convertir una lente C-mount a CS-mount. CS es una actualización de C que buscaba reducir los costos de fabricación y reducir el tamaño del sensor.

El sensor de la imagen es uno de los elementos más importantes cuando se trata de garantizar una buena calidad de imagen ya que este se encarga de transformar la luz en señales eléctricas. Esencialmente, existen dos tecnologías utilizadas para cámaras de videovigilancia: CCD y CMOS.

El sensor CCD es el elemento más utilizado por sus capacidades de interpretación de imágenes, su mayor sensibilidad a la luz permite que lugares con poca iluminación puedan ser interpretados eficazmente por el sensor, no obstante ante excesos de luz puede provocar perdidas en la imagen distorsionándola por completo. El sensor CMOS es una tecnología que busca integrarse a cámaras de video de tamaño reducido, su estructura permite tener cámaras de video muy pequeñas con resoluciones aceptables en lugares bien iluminados. Cuando la escasez de iluminación se presenta, sus carencias en percepción de detalles salen a relucir con imágenes oscuras granuladas.

Un sensor de imagen puede ser de diferentes tamaños (2/3”, 1/2”, 1/3” y 1/4"), el cual debe ser acorde al tipo de objetivo utilizado. Cabe mencionar que un objetivo para sensores de 1/2" permitirá adoptar sensores de la misma magnitud o más pequeños (1/3” y 1/4"). Es importante entender los efectos que tiene el utilizar sensores acordes a los objetivos para poder abarcar la mayor cantidad de información recabada de la imagen. Cuando el objetivo y el sensor son del mismo tamaño, la imagen interpretada es exactamente la misma que la percibida **(Figura 6-6a)**; cuando el sensor es mas pequeño que el diámetro del objetivo la información se perderá fuera del sensor **(Ver Figura 6-6b);** si el sensor es mayor que el diámetro del objetivo, existirán esquinas de color oscuro en la imagen. **(Ver Figura 6-6c)**

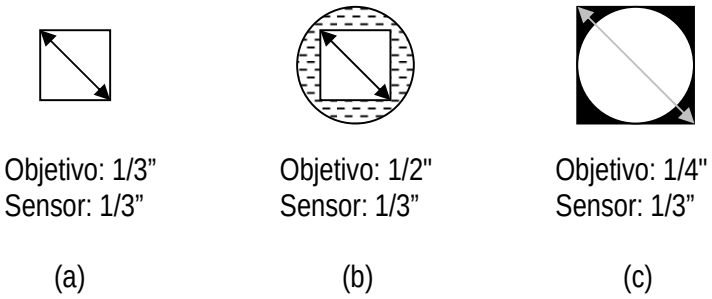


Figura 6-6. *Relación lente – sensor.*

La interpretación del video es parte importante de la cámara ya que depende directamente del lugar donde vaya a estar situada. El escaneo es la técnica utilizada para desplegar los pixeles interpretados por el sensor. El escaneo siempre se realiza de izquierda a derecha como una secuencia de líneas horizontales, una después de la otra. El tipo de escaneo puede ser de dos diferentes tipos: progresivo o entrelazado. En el escaneo progresivo, cada línea horizontal en la imagen es escaneada secuencialmente de arriba hacía abajo; es decir, la línea 1 será presentada primero, posteriormente la línea 2, 3,4,…. En el escaneo entrelazado, solamente las líneas impar de la imagen son escaneadas de arriba hacia abajo (campo 1) y posteriormente las líneas pares de la imagen (campo 2). El escaneo entrelazado es utilizado en monitores y pantallas que utilizan tubo de rayos catódicos, por su naturaleza propia, el video entrelazado no está dirigido en ambientes donde el movimiento es constante y la identificación de personas es lo primordial ya que sus dos campos componentes desplegaran dos diferentes ubicaciones ocasionando un efecto de distorsión (jagged) **(Ver Figura 6-7)**. La posibilidad de usar escaneo progresivo ayuda a eliminar este efecto permitiendo tener imágenes más claras sin efecto jagged. Sin embargo en soluciones de video bastantes robustas, el escaneo progresivo necesita un gran ancho de banda que permita interpretar la imagen completa en un único turno. **(Ver Figura 6-8).**

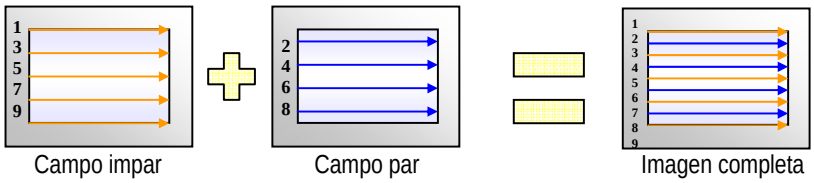


Figura 6-7. *Barrido Entrelazado*

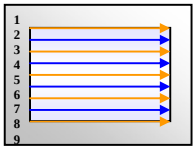


Imagen completa con un solo campo

Figura 6-8. *Barrido Progresivo*

Como ya se mencionó anteriormente, el *objetivo* es la parte de la cámara que contiene el lente y el iris de la cámara, por este elemento la luz se traslada para llegar al sensor de imagen. Existen 3 tipos de objetivos básicamente:

- Lente fija. El lente de este objetivo es fijo, no configurable, es necesario conocer la longitud focal del lente con anticipación para saber el campo de visualización horizontal
- Lente varifocal. Este lente permite el ajuste manual del campo de visualización. Cuando esta propiedad es cambiada, el enfoque debe adecuarse.
- Lente de zoom. Este lente es utilizado en cámaras PTZ, permite configurar la longitud focal en un rango relativamente amplio (6 a 48mm), sin afectar el enfoque. El objetivo regularmente es controlado de forma remota.

El *iris* es el elemento que controla la cantidad de luz que transitara hacía el sensor a través del objetivo. Para las cámaras IP esta propiedad ha sido adoptada por la necesidad de observar diferentes lugares con variadas fuentes de iluminación. Existen diferentes tipos de iris en los objetivos:

- Control de iris manual. Este modo permite solamente adaptarse a condiciones de luz específicas. Este iris no puede reaccionar ante cambios de iluminación drásticos; por esto, el iris se ajusta a un valor medio para condiciones de luz variable.
- Control de iris automático. Utilizado en cámaras de exteriores donde la iluminación de la escena está cambiando constantemente, la apertura del iris esta controlada por la propia cámara para mantener un nivel de luz óptimo para el sensor. Con este modo el sensor también se ve protegido ante excesos de luz.

Un diámetro de iris menor reduce la cantidad de luz permitida ofreciendo un mejor enfoque a mayor profundidad y un diámetro mayor ofrece mejores imágenes en situaciones de luz escasa por la mayor cantidad de luz aceptada.

En cámaras IP, existen otros elementos a parte de los anteriores que permiten el procesamiento, análisis y compresión del video hacía los destinos. **(Ver Figura 6-9)**

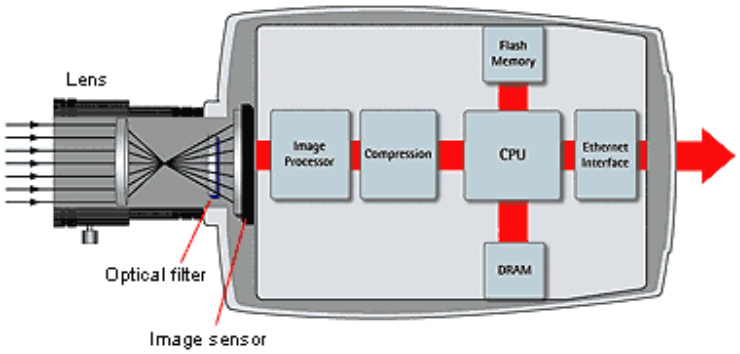


Figura 6-9. *Componentes de una cámara IP*
(Fuente: *Guía Técnica de video IP*, **Axis Communications,** Sección 18, Pág. 8)

6.4.2 Criterios de Evaluación para la Elección de Cámaras

Todos los fabricantes buscan ofrecer cámaras de video IP que permitan al usuario tener una buena calidad en imágenes y eficaces métodos de compresión de video que permitan disminuir la magnitud excesiva de información que implica. Ante estas características cada uno de los fabricantes intenta competir con mayor número de posibilidades cuando a propiedades en configuración se trata. Ante la gran similitud de capacidades existente entre fabricantes, se consideraron más factores (no propiamente de la cámara), que permitieron seleccionar la cámara más adecuada a las necesidades existentes.

La parte de *calidad de imagen* es un aspecto importante a considerar en el proceso de elección ya que se trata de un sistema que buscará evidenciar actos ilícitos de carácter crítico. Si la calidad de la imagen no es adecuada, los demás factores se vuelven intrascendentes. Con una buena calidad de imagen se abre la posibilidad de interpretar detalles y cambios en imágenes. Las evidencias serán de mayor exactitud aunando la posibilidad de tener mejor información de video con herramientas de alarma, detección de movimiento, etc.

La elección de *fabricantes reconocidos* permite estar cubierto en cuanto mantenimiento y garantías se refieren. En el ambiente de seguridad, existen una gran cantidad de integradores que ofrecen marcas no reconocidas que no garantizan una respuesta ante daños físicos, o si es conocida, los tiempos de respuesta se incrementan por la inexistencia de un representante en territorio nacional que remplace una pieza, convirtiéndose en procesos largos y contraproducentes para un sistema de seguridad que no puede estar detenido.

La utilización de cámaras IP con *facilidad de integración* a diferentes aplicaciones de administración de video. Esto permite tener una gama de oportunidades cuando de elección de software se trata. La oportunidad de tener cámaras IP con una interfaz abierta (API) permitirá realizar una integración hacía nuevas tendencias, garantizando que las cámaras puedan adaptarse a las nuevas tecnologías que se desarrollarán en un futuro como el análisis inteligente del video.

El factor *compresión* es una parte indispensable en el diseño del sistema, es importante tomar en cuenta las posibilidades que ofrece la propia cámara respecto a los estándares de compresión que puede manejar. Como ya se ha mencionado actualmente las cámaras IP manejan tres tipos de compresión en sus imágenes JPEG, M- JPEG ó MPEG-4, de lo cual sería importante utilizar más de uno de estos estándares para tener alternativas en el envío del video. A pesar de que MPEG-4 es un estándar, el licenciamiento del codec es llevado a cabo por cada fabricante lo que limita su utilización libre.

Las *funciones de red* de la cámara y los protocolos utilizados es una característica elemental a tomar en cuenta ya que es la manera en que la cámara puede ser parte de un entorno de red. Las velocidades de conexión, la comunicación entre cámara y el visor deben ser confiables y seguras que permitan autenticar y enviar información de manera cifrada para evitar fuga de información.

La forma de *energizar* la cámara es un aspecto que puede hacer que la solución sea mucho más costosa por la necesidad de llegar a cada una de las cámaras con una fuente de alimentación. En el caso de cámaras de movimiento, la necesidad de cableado es forzosa, sin embargo para cámaras fijas está característica será de las primeras en tomar en cuenta para la elección. Con esto se busca evitar costos de instalación de fuentes de alimentación para cada cámara, así como de sistemas de alimentación ininterrumpida (UPS) en caso de fallas eléctricas.

Video inteligente es el desarrollo para años venideros en sistemas de videovigilancia, este tipo de análisis requiere grandes cantidades de procesamiento, que no pueden ser llevadas a cabo por los servidores de gestión, por integridad propia. Para esto la cámara de video vigilancia debe permitir ejecutar análisis de modo que podrá elegir cuando enviar y procesar video. Considerando esta opción, permitirá mejorar la información en video recabada a solo grabaciones útiles e importantes.

Las *entradas* y *salidas digitales* que pueden manejar los dispositivos IP, pueden utilizarse para utilizar mecanismos que ayuden a evitar transferencias de video innecesarias. Ayudar al sistema de videovigilancia con dispositivos de alarma permitirá tener un sistema mucho más eficiente y completo.[5]

6.4.3 Evaluación de cámaras interiores y exteriores

Independientemente de la tecnología existente en cámaras IP, para el proyecto de videovigilancia se dividió el estudio hacía dos escenarios: espacios exteriores y espacios interiores. Haciendo esta distinción y tomando como base los criterios de evaluación anteriormente citados se evaluó una cantidad razonable de fabricantes líderes en el mercado de video IP. Los fabricantes considerados para el análisis de tecnologías en cámaras IP fueron: Canon, Axis, Bosch, Sony, Pelco, Toshiba, Samsung, Panasonic. Las cámaras analizadas fueron las de mejores cualidades, idóneas para los espacios existentes del Instituto de Ingeniería, según recomendación de expertos integradores y de los mismos fabricantes. En algunas ocasiones no fue posible contar con las cámaras físicamente por la disponibilidad del modelo, sin embargo se efectuaron visitas presénciales para observar su funcionalidad en ambientes reales de trabajo. El estudio se realizó en dos etapas:

Primeramente se efectuó un análisis de cámaras exteriores para las cuales se establecieron objetivos comunes, con esto se buscó ajustar la mejor configuración para la mejor de las percepciones, la base del estudio partió de los criterios de evaluación en función de los criterios mencionados. Para el caso de cámaras robóticas, la **Tabla 6-1** muestra un cuadro comparativo de las propiedades evaluadas. Posteriormente el análisis de cámaras interiores, **Tabla 6-2,** se realizó también bajo condiciones similares donde efectos de luminosidad, posición, conectividad fueron examinados. Cabe mencionar que el análisis no fue bajo condiciones ideales ya que diversos factores influyeron en el estudio tales como: disponibilidad de las cámaras, condiciones ambientales, la integridad de las propias cámaras.

Cámaras Exteriores					
	Sony SNC-RZ30N	**Canon VB-C50i**	**Axis 214**	**Toshiba DP20A**	**Panansonic WV-NS324**
Energía	12V DC	13V DC	12V DC	24V AC	24V AC
Sensor de Imagen	1/4" Sony ExView Had CCD, B.I.*	1/4" CCD, B.I.	¼" Sony ExView Had CCD, B.I.	1/4" CCD, B.I.	1/4" IT CCD, B.I.
Lente	25x zoom f = 2.4 - 60mm, F1.6 – F2.7	26x zoom f = 3.5 - 91mm,	18x zoom f = 4.1 - 73.8mm, F1.4	18x zoom, f = 4.1 - 73.8mm, F1.4 - F3.0	10x zoom, f = 4.2 - 42mm, F1.4
Rango Pan	340°,170/s	200°	340°, 100°/s	360°, 150°/s	360°, 100°/s
Rango Tilt	115°,77°/s	120°	120°,90°/s	0° - 92°, 45°/s	0° - 92°, 100°/s
Compresión	JPEG	MPEG,JPEG	M-JPEG,MPEG-4	Sin compresión	JPEG
Resolución	736x480, 640x480, 320x240,160x120	640x480,320x240 160x120	4CIF,2CIFExp, 2CIF,CIF,QCIF	720x480	640x480, 640x240, 320x240,160x120
Iluminación mínima	3.0 lux	1.0 lux 0 lux modo nocturno, luz infrarroja hasta 3m	0.005 lux	0.01 lux	1.0 lux
Conectores	Ethernet 10BaseT/100BaseTx, RJ45	Ethernet 10BaseT/100BaseTx, RJ45	Ethernet 10BaseT/100BaseTx, RJ45	Cable coaxial, RS-422	Ethernet 10BaseT/100BaseTx, RJ45
Protocolos	DHCP, TCP/IP, HTTP, ARP, FTP, SMTP, ICMP y SNMP	TCP/IP, HTTP, DHCP, FTP, NTP, DDNS, SMTP	IP, HTTP, HTTPS, SSL/TLS**, TCP, ICMP, SNMPv, RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS	Protocolo Toshiba P/D	TCP/IP, UDP/IP, HTTP, FTP, SMTP, DNS, DDNS, DHCP, NTP y BOOTP.

Tabla 6-1. *Especificaciones Técnicas de las Cámaras IP exteriores evaluadas*

Cámaras Interiores						
	Sony SNC-Z20N	**Axis 221**	**Toshiba IK-6400A**	**Panasonic WV-CW474**	**Panasonic BL-C10A**	**Bosch 445**
Energía	12V DC, PoE	7 - 22V DC, PoE	12V DC	24V AC	8.5V DC	12V DC, PoE
Sensor de Imagen	1/4" Sony ExView Had CCD,B.P.°	1/3" Sony CCD, B.P.	1/3" CCD, B.I.	1/3" CCD, B.I.	¼" CMOS, B.I.	1/3" CCD, B.I.
Lente	f = 4.1 - 76.8mm, F1.4 CS mount	f = 3.8 - 8mm F1.0 CS mount	No especificado CS mount	f = 3.8 - 8mm F1.0	F2.8 CS mount	No especificado
Compresión	JPEG	M-JPEG MPEG-4	Sin compresión	Sin compresión	M-JPEG	M-JPEG MPEG-4
Resolución	736 x 480, 640 x 480, 320 x 240, 160 x 120	4CIF,2CIFExp, 2CIF,CIF,QCIF	771 x 492	768 x 494	640 x 480, 320 x 240, 160 x 120	4CIF, 2CIF,CIF,QCIF
Iluminación mínima	0.7 lux modo color 0.01 lux modo B/N	0.65 lux modo color 0.08 lux modo B/N	0.2 lux	2.4 lux modo color 0.3 lux modo B/N	1.0 lux modo color	0.3 lux modo color 0.12 modo B/N
Conectores	Ethernet 10BaseT/100BaseTx,RJ45 Analógico compuesto RS-232	Ethernet 10BaseT/100BaseTx,RJ45 RS-232	Analógico Compuesto	Analógico compuesto Salida VGA	Ethernet 10BaseT/100BaseTx,RJ45	Ethernet 10BaseT/100BaseTx,RJ45 Analógico compuesto RS-232
Interfaces I/O	1/2	2/1	0/0	0/0	0/0	1/1
Protocolos	TCP/IP, ARP, ICMP, HTTP, FTP, SMTP, DHCP, DNS, NTP, y SNMP	IP, HTTP, HTTPS, SSL/TLS, TCP, RTSP, RTP, UDP, RTCP, SMTP, FTP, DHCP, , ARP, DNS.	No utilizados	No utilizados	HTTP, FTP, SMTP, TCP, UDP, IP, DHCP, DNS, ARP, ICMP, POP3	RTP, Telnet, UDP, TCP, IP, HTTP, IGMP, ICMP, SNMP

Tabla 6-2. *Especificaciones Técnicas de las cámaras IP interiores evaluadas*

Las cámaras robóticas están diseñadas para realizar seguimientos, su capacidad de cobertura no permite ser utilizadas en lugares donde es importante no perder detalle de lo que sucede. La seguridad de evidencia solamente es posible con cámaras dedicadas que permitan observar detenidamente hacía un punto de interés, por lo tanto en una solución de video seguridad adecuada, las cámaras robóticas tendrán una función de apoyo y complemento para la visualización de puntos críticos. Por otro lado, las cámaras fijas deberán tener una mejor visión de detalles, usualmente su mejor provecho es en lugares cerrados donde los cambios de imagen son frecuentes, en un ambiente abierto donde diferentes factores afectan la imagen (luminosidad, viento, lluvia), obstaculizan la utilización de este tipo de cámaras porque no existe un esquema definido de lo observado.

De acuerdo a lo anterior y al análisis técnico realizado se puede concluir que la mayoría de las cámaras analizadas tienen similitudes en características (resolución, protocolos de comunicación, sensor de imagen) sin embargo los tres aspectos principales tomados en cuenta para la elección son: compresión, interfaces i/o y alimentación eléctrica. Aunque estos aspectos sean los primordiales, la calidad de imagen siempre será una característica esencial a ser analizada cuando el préstamo de equipo sea posible.

Hasta este momento, en el Instituto de Ingeniería, se han utilizado en interiores cámaras Axis 221 con visión diurna y nocturna alimentadas a través de Ethernet, alojadas en carcasas GVI de para su mayor protección. Así mismo se han comenzado a utilizar cámaras fijas Axis 216 MFD con resolución de megapixeles lo que permite mejor identificación de objetos y personas. Para exteriores se utilizan cámaras Axis 214 PTZ con visión diurna y nocturna para seguimientos en áreas al aire libre, así como cámaras Axis 221 con carcasas para exteriores en aquellas zonas más sensibles donde se desea tener una visualización continua del lugar.

La elección de la marca Axis se debió a las ventajas ofrecidas con respecto a otros fabricantes tales como:

- Representación en territorio nacional en soporte y venta de equipo. Los componentes pueden ser reemplazados y los términos de garantía aplicados en tiempos de espera aceptables.
- Una gran variedad de equipos de videovigilancia, que permite elegir ante una gran variedad de situaciones el mejor producto.
- Calidad de imagen acorde a las situaciones establecidas. Axis permitió realizar demostraciones con sus productos para revisar sí sus equipos satisfacían las necesidades del Instituto de Ingeniería, obteniendo resultados positivos y acordes a los esperado.
- Compatibilidad con software de administración de terceros. Esto permite ampliar la posibilidad en elección de software de gestión de video y no estar atenidos a una sola solución en particular.
- Referencias técnicas y entrenamiento que ayudo a comprender la situación real de los sistemas de videovigilancia, sus beneficios y la manera de utilizar nuevas tecnologías basadas en IP.

- Soporte para la integración de sistemas CCTV de 1ª y 2ª generación, existentes en algunos edificios del Instituto de Ingeniería.
- Utilización de análisis avanzado de video. Esto permite explotar al máximo las cámaras de video Axis, debido a la posibilidad de realizar análisis de video directamente en la cámara sin necesidad de trasladar video innecesario hasta lugares remotos.
- Facilidad en la administración de los equipos, debido a sus intuitivas interfaces de gestión y herramientas de administración que permite llevar un mejor control y actualización de los equipos Axis.

Para la vigencia y estabilidad de un sistema de seguridad, sus componentes deben estar protegidos de los propios usuarios y de condiciones ambientales que puedan afectar su funcionalidad, para esta problemática existe una gran variedad de opciones que evitan que los equipos estén expuestos a agresiones y entornos hostiles. A pesar de que el Instituto de Ingeniería se encuentra en un campus universitario continuamente vigilado, es importante considerar sí los lugares de ubicación de cámaras estarán al alcance de las personas ya que al ser equipo costoso y con funciones tan importantes se vuelven blanco de ataques y agresiones en su contra en muchas ocasiones.

En cámaras de videovigilancia, la calidad del video obtenido depende de tres factores principalmente: el sensor de la cámara, la tecnología de compresión utilizada y el software de gestión del video. Sin un software de administración apropiado no se pueden abarcar todos los beneficios que la tecnología IP ofrece ya que de este depende la posibilidad de controlar, analizar y visualizar tanto las grabaciones en directo como el video grabado a través de la red IP. Así que, la eficiencia de una solución de videovigilancia IP no está en función de las capacidades propias de la cámara, sino de la capacidad del software de gestión para aprovechar toda la tecnología existente dentro ella. La elección del software de gestión se vuelve el elemento decisivo en el diseño del sistema de videovigilancia del Instituto de Ingeniería.

6.5 Evaluación de Software de Administración de Video

La eficiencia de un sistema de videovigilancia se puede corroborar por medio de las posibilidades que tenga para permitir la integración de dispositivos de seguridad tales como sensores, interruptores, controles de acceso, etc. Actualmente no basta con tener un resguardo de información en video de tiempos muy prolongados puesto que la mayoría de esta información es inservible y entorpece la búsqueda de sucesos específicos. Por esta razón, una buena herramienta de administración debe permitir, aparte de las funcionalidades básicas (controlar, analizar, consultar y almacenar video), realizar procesamiento en imágenes para identificar eventos (congestionamientos, objetos robados, identificación de sentidos, acumulación de personas, velocidades, etc.) y reducir la cantidad de información recabada que es el elemento del cual depende principalmente el costo de la solución en este tipo de tecnologías.

Para administrar video existen en disponibilidad dos alternativas principalmente. La primera de ellas es la plataforma basada en servidor PC y la plataforma basada en grabadores de video en red (***N**etwork **V**ideo **R**ecorder*).

Una plataforma basada en PC es un sistema que utiliza los componentes usualmente existentes en entornos de cliente-servidor, donde una máquina ofrece un servicio a una o muchas computadoras cliente. Con este tipo de esquema, el hardware utilizado por el servidor debe ser el óptimo para realizar grandes tareas de procesamiento. Además es posible aprovechar soluciones existentes en almacenamiento externo que garanticen la integridad de la información. Como parte de este esquema, la disponibilidad del equipo depende de la seguridad existente en su entorno ante ataques y códigos maliciosos.

La plataforma basada en NVR es una solución diseñada específicamente para video seguridad, un NVR es simplemente un equipo con la funcionalidad de administrar video por medio de una aplicación pre instalada donde elementos de monitoreo tendrán que conectarse para poder controlar dispositivos. Nativamente, es una aplicación instalada en un sistema operativo que realiza grabación, análisis y reproducción. La posibilidad de crecimiento dependerá de los límites de capacidad del diseño del grabador.

Nota. Algunos fabricantes manejan el término DVR (***D**igital **V**ideo **R**ecorder*) para hacer referencia a un grabador de video en red. Un DVR y un NVR poseen algunas similitudes pero no es la misma plataforma. El almacenamiento en ambos sistemas se realiza digitalmente (en disco duro), sin embargo, el DVR es un sistema híbrido al cual se conectan cámaras de video exclusivamente analógicas y el NVR es un verdadero sistema digital que recibe imágenes siempre de cámaras digitales.

La diversidad de opciones en el mercado es vasta en soluciones de videovigilancia, desde las más complejas como sistemas de monitoreo centralizado para miles de cámaras hasta un simple diseño de monitoreo que ofrece cualquier cámara IP por medio de su propio servidor web. Sin embargo en la búsqueda de la mejor solución, se presentaron alternativas interesantes las cuales fueron evaluadas bajo criterios técnicos y económicos.

6.5.1 Sistema Milestone Xprotect *(Milestone Corporation)*

Milestone Xprotect es un software de administración diseñado para soluciones de videovigilancia de gran magnitud para múltiples sitios. Su capacidad de controlar números ilimitados de cámaras en arquitecturas distribuidas, permite tener una gran escalabilidad para futuras expansiones.

La línea Milestone Xprotect ofrece cuatro distintas versiones de productos las cuales ofrecen diversas funcionalidades según las necesidades y las dimensiones de la solución. Las versiones disponibles son las siguientes:

1. *Xprotect Enterprise*. Permite controlar un número ilimitado de cámaras, múltiples servidores distribuidos y dos alternativas de monitoreo para usuario final.

2. *Xprotect Professional*. Permite hasta 36 cámaras, con dos alternativas de monitoreo para usuario final.
3. *Xprotect Basis+*. Destina para entornos mucho más reducidos, permite hasta 25 cámaras para su monitoreo en una arquitectura no distribuida.
4. *Xprotect Basis*. Opera hasta con 16 cámaras, destinada para hogares y negocios reducidos. Opera con una consola para monitoreo de usuario.

Por las dimensiones y características del Instituto de Ingeniería, la versión *Enterprise* permitiría obtener una infraestructura de videovigilancia no centralizada completamente escalable capaz de incorporar nuevas tecnologías sobre estudio y análisis del video digital.

Algunas de sus características más importantes de está versión se mencionan a continuación:

- Compatibilidad con cerca de 90 productos de video de fabricantes lideres en el mercado de la seguridad, abriendo la posibilidad de elegir el mejor equipo de acuerdo a las necesidades existentes.
- Acceso remoto que permite administrar y monitorear el sistema desde cualquier lugar donde exista conexión a Internet, usando una PC, laptop o PDA.
- Escalabilidad en su arquitectura por sus capacidades basadas en tecnología IP, permitiendo integrar elementos de seguridad según los requerimientos.
- Desarrollo constante de nuevas actualizaciones lo que permiten tener un producto moderno siempre protegido ante vulnerabilidades de seguridad que se pudieran presentar.
- Monitoreo de hasta 64 cámaras simultáneas por servidor de administración.

Especificaciones Técnicas

- Grabación, visualización y reproducción de video de manera simultanea.
- Soporte de compresión MPEG-4 y M-JPEG según marca y modelo del producto.
- Capacidades de almacenamiento ilimitadas por medio de múltiples resguardos de información al día.
- Detección de movimiento (VMD) ajustable a zonas exclusivas de la imagen.
- Frame Rate ajustable con respecto a movimiento detectado o en ocurrencia de eventos.
- Reporte de alarmas vía correo electrónico o mensajes SMS.
- Búsqueda inteligente por zonas o por objetos.
- Exportación de evidencia en formato JPEG o AVI, con la posibilidad de cifrado y protección de la información.
- Registros de actividad de usuarios remotos y configuraciones realizadas.
- Capacidad de configurar hasta 50 posiciones (presets) por cámara.
- Configuración de múltiples esquemas de monitoreo por día y hora.
- Soporte de Tecnología IPIX.
- Configuración en línea mientras el sistema está en operación
- Soporte DNS

- Integración con Active Directory de Microsoft.
- Aplicación con la posibilidad de funcionar como servicio de sistema, lo que permite ser ejecutado sin la necesidad de cuentas especificas.

A nivel usuario, Milestone permite tener una administración de los recursos a través de un cliente remoto (*smart client*) que permite la visualización y manejo de la información generada. Algunas de las características del cliente son las siguientes:

- Visualización de hasta 16 cámaras por usuario remoto.
- En un sistema distribuido, la capacidad de consultar grabaciones de diferentes servidores simultáneamente.
- Asignación de permisos a cada cuenta de usuario. El administrador del sistema define las posibilidades de monitoreo, consulta o configuración de las cámaras de acuerdo a sus funciones dentro del Instituto.
- Identificación de la ubicación de cada una de las cámaras por medio de referencias gráficas (mapas dinámicos) que permiten su identificación de forma más rápida.
- Manejo de cámaras robóticas remotamente.
- Opción de compresión configurable entre el servidor y cliente para controlar el uso de ancho de banda.
- Registros de actividad de los usuarios remotos en tiempo y acciones realizadas.
- Generación de archivos AVI y JPEG que permiten a un usuario exportar información si así lo necesitara.
- Visualización de video en MPEG-4 y M-JPEG simultáneamente.

Como una aplicación de administración de video, los requerimientos del servidor deben ser los suficientes para las tareas de codificación y decodificación que se realizarán, para el manejo de tráfico de red, manejo de cuentas de usuario y los servicios existentes que soportarán dichas tareas de gestión.

Sistema Operativo: Windows 2000 Professional, Windows Server 2000, Windows XP Professional, Windows Server 2003.
Procesador: Preferentemente Intel de doble núcleo o posterior.
RAM: 1GB como mínimo.
Network: Dos tarjetas de red de 1Gbps cada una; buscando aislar peticiones realizadas por clientes y el flujo de video hacía el servidor.
Tarjeta de Video: AGP, resolución mínima de 1024x768.
Disco Duro: Interfaz FastSCSI, 7200 rpm mínimo. El espacio de disco duro dependerá de la cantidad de video elegido para almacenar y los métodos de almacenamiento diseñados.

Una parte importante a mencionar es el licenciamiento y soporte técnico para la aplicación. El licenciamiento del producto se lleva a cabo por medio de una licencia base para el software Milestone (XPEBL) que permite la posibilidad de instalar el producto en un número indefinido de servidores de administración. Una segunda licencia es (XPECL) que implica el licenciamiento por cada uno de los elementos de video a gestionar a través del software. En el caso de dispositivos con capacidad para controlar más de una señal de video

(v*ideo server)*, el licenciamiento se realiza por señal de video, no por dispositivo. El soporte técnico al software depende directamente del sitio oficial del fabricante (www.milestonesys.com), donde una base de conocimientos está a disposición del usuario para resolver problemas o dudas que pudieran presentarse en la instalación, configuración y actualización del software. Aunado a esto, un representante del producto se encuentra en territorio nacional para aclarar dudas de cualquier índole y dar soporte técnico en forma presencial si así se requiere.

Nota. Existe un contrato de mantenimiento opcional ofrecido por Milestone (PMA). Este contrato permite acceder a actualizaciones y mejoras de software por un año, entre las ventajas más importantes, el mantenimiento ofrece la posibilidad de obtener una actualización de la versión del software sin cargos extras si así se publicará dentro del periodo de vigencia del PMA. El costo del PMA es por dispositivo o el 18% del costo de cada XPECL.

Milestone Xprotect Enterprise es una solución puramente IP, el cual permite aprovechar la red de datos existente en su totalidad, considerando las propias capacidades de dicha red, un esquema de monitoreo distribuido, y un manejo de almacenamiento bien estructurado, es factible tener información de video confiable y siempre disponible cuando así se requiera. El crecimiento de la solución esta garantizado y la posibilidad de integrar a un número ilimitado de consolas de monitoreo son un valor agregado de esta solución.

6.5.2 Endura Security System *(Pelco)*

Este sistema de seguridad está basado en una arquitectura distribuida de elementos que permiten lograr un sistema de alto desempeño y calidad en soluciones de video seguridad. Endura se integra a la infraestructura de red IP lo que representa disminución de costos de cableado, componentes e instalación. La plataforma Endura es un sistema completo de video digital compuesto por: codificadores, decodificadores, grabadores de video, estaciones de trabajo, consolas de monitoreo y medios de almacenamiento masivo.

Endura es un sistema hibrido que busca aprovechar los beneficios que existen en el video analógico y al mismo tiempo las ventajas que ofrece el video digital. Por un lado utiliza las imágenes generadas por cámaras analógicas de buena calidad para visualizar la mayor cantidad de detalles en espacios; por otro lado, utiliza el envío de video digital a través de una red de datos para el transporte de imágenes a consolas de monitoreo o unidades de almacenamiento.

Con estos dos principios abarca dos de los aspectos más importantes a considerar en un sistema de videovigilancia: calidad y transmisión de imágenes. Por ser un sistema robusto y complejo, los elementos implicados en este sistema son los siguientes:

Componente Endura	***Descripción***
Codificador NET5301T	*Este elemento codifica a MPEG-4, acepta señales analógicas de audio y video. Convierte estas señales a paquetes TCP/IP.*
Decodificador NET5301R	*Elemento de alto desempeño que convierte video digital y audio a señales analógicas del tipo S-Video o VGA.*
Estación de Trabajo WS5050	*Esta PC tiene instalado el sistema operativo, y es usado para visualización del video y configuración del sistema.*
Consola de monitoreo VCD5000	*Es una unidad decodificadora. Convierte múltiples streams MPEG-4 en señales de video para ser vistas en S-Video o VGA. Con la capacidad de añadir módulos de decodificación permitiría visualizar hasta 64 imágenes distintas. La consola de monitoreo permite controlar un ilimitado numero de decodificadores y VCD's.*
Servidor de administración SM5000	*Provee la administración de múltiples dispositivos, en este servidor también se administra la seguridad del sistema y la autenticación de usuarios y dispositivos.*
Servidor de almacenamiento NVR5100	*El grabador digital realiza el almacenamiento del video por medio de esquemas de grabación definidos. Con soluciones masivas de almacenamiento, se puede transportar la información a unidades de mayor capacidad (EnduraStor).*
Unidad de almacenamiento externo SEB50000	*SEB es un dispositivo de gran capacidad que permite almacenar hasta 3.9TB de información. Múltiples SEB's pueden ser adaptados a un solo NVR para lograr una solución escalable basada en red.*
Optimización de almacenamiento EnduraStor	*Esta opción permite reducir el frame rate del video ya almacenado. Cuando las capacidades de almacenamiento están por saturarse, se puede liberar espacio en disco.*

Para que la solución Endura pueda ser implementada exitosamente los requerimientos y necesidades son los siguientes:

- *Medios Físicos*
  - Enlaces con capacidad de 1000baseT.
  - Cableado estructurado Cat6 para enlaces Gigabit.
- *Protocolos de red*
  - Unicast: RIP, OSPF, Static Routing.
  - Multicast: PIM (DM o SM), DVRMP.
  - IGMP

La eficiencia del sistema Endura esta en función de las tecnologías de switcheo y ruteo utilizadas. Dentro de un sistema centralizado donde un equipo de red base (Core) es responsable de todas las decisiones, el control de tráfico se dificulta con la integración de Endura por las siguientes tareas que se originan:

- Realizar todas las decisiones de ruteo Unicast.
- Realizar todas las decisiones de ruteo Multicast.

- Administrar todo el tráfico de red Endura: video, audio, PTZ, UPnP.
- Administrar todo el resto de tráfico existente en la red.

Por lo tanto un sistema basado en un equipo Core no es el escenario recomendable para un ambiente Endura por la alta posibilidad que existe de que la capacidad de este equipo llegue a saturarse.

Un diseño alterno, ideal para el sistema es el denominado "*intelligent edge design*". Este diseño se basa en colocar switches distribuidos que realicen tareas de ruteo de datos para minimizar el impacto a un equipo Core único, permitiendo que los procesos de ruteo sean realizado por un grupo de elementos. Con este diseño se facilita el crecimiento del sistema ya que los switches pueden ser fácilmente incorporados a la red sin afectar a un simple y único Core. La estructura Endura basa su funcionamiento en *módulos* con funciones específicas que permiten tener un mejor control e identificación del tráfico para separase en VLAN's y ayudar a determinar requerimientos de red en particular.

Los cuatro módulos principales para comprender el funcionamiento de Endura son:

- Módulo A: Esta parte de la solución es la encargada de codificar, grabar, y almacenar los streams generados por las cámaras de video.
- Módulo B: Este módulo se encarga de decodificar y desplegar los streams de video así como de llevar la configuración de los componentes del sistema.
- Módulo Core: Es el elemento para la conectividad de los módulos, realiza las tareas de ruteo, autenticación y seguridad del sistema.
- Módulo C: Este bloque engloba a los tres anteriores: A, B y Core.

Módulo A
Este módulo es el más importante del diseño simplemente porque es donde se realiza la generación y transmisión de imágenes. El módulo A tiene por características:

- Puede soportar hasta 48 codificadores NET5301T y un NVR5100.
- Una VLAN debe ser asignada solamente a este módulo.
- El número de módulos A es ilimitado.

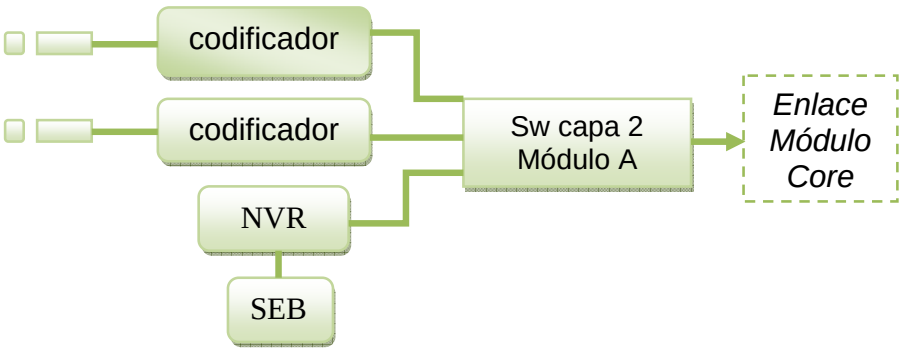


Figura 6-10. *Módulo A, Codificación y Grabación.*

Módulo B

El módulo B determina los requerimientos de ancho de banda para la red; es responsable de la decodificación y despliegue de video.

La funcionalidad del módulo B se limita a lo siguiente:

- Con base en permisos, puede ver y controlar cualquier cámara del sistema.
- Cada módulo B debe estar asignado a una VLAN específica.
- Este módulo puede existir cualquier número de veces (limitado solamente a la capacidad de la red)
- Los componentes que lo conforman son: NET5301R, VCD5000, WS5050.

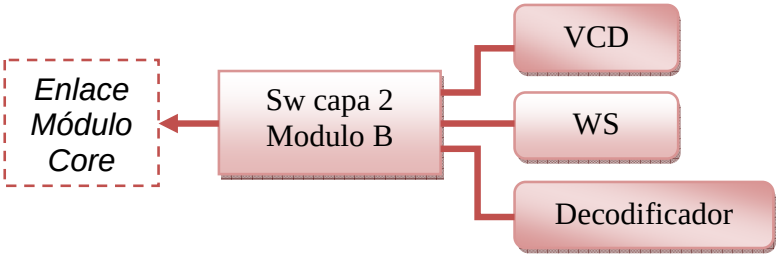


Figura 6-11. *Módulo B, Decodificación y visualización de video*

Las tareas de despliegue de video pueden realizarse en los tres componentes de este módulo (VCD, WS, decodificador) por esta razón es importante realizar una estimación de los anchos de banda requeridos en la red Endura tanto para monitoreo en vivo como en consulta de video. La cantidad de ancho de banda dependerá de la calidad de imagen deseada tanto para grabación como para reproducción.

Con base en las siguientes expresiones y valores de calidad de imagen se buscará la cantidad de ancho de banda para el peor de los casos en el módulo B:

$B_{wc} = B_w + O_H$

Donde:
B_w = Ancho de banda definido por la ecuación: $B_w = N_s - B_R$
O_H = Sobrepaso definido por la ecuación: $O_H = 25\%\ (B_w)$
N_s = Número de streams
B_R = Bit rate

Stream 1 (*consulta*)	Resolución	Bit Rate	Fps
Calidad baja	CIF	800kbps	15
Calidad media	2CIF	1.5Mbps	30
Calidad alta	4CIF	2Mbps	30

Stream 1 (*en vivo*)	Resolución	Bit Rate	Fps
Calidad baja	QCIF	600kbps	15
Calidad media	CIF	800kbps	15
Calidad alta	CIF	1Mbps	15

Valores calculados de ancho de banda para despliegue en *consulta:*

WS5050 (16 streams simultáneos):
$B_{wc} = (N_s)(B_R) + O_H = 32Mbps + 8Mbps = 40Mbps$
VCD5000 (64 streams simultáneos):
$B_{wc} = (N_s)(B_R) + O_H = 128Mbps + 32Mbps = 160Mbps$
NET5301R (4 streams simultáneos):
$B_{wc} = (N_s)(B_R) + O_H = 8Mbps + 2Mbps = 10Mbps$

Valores calculados de ancho de banda para despliegue *en vivo:*

WS5050 (16 streams simultáneos):
$B_{wc} = (N_s)(B_R) + O_H = 16Mbps + 4Mbps = 20Mbps$
VCD5000 (64 streams simultáneos):
$B_{wc} = (N_s)(B_R) + O_H = 64Mbps + 16Mbps = 80Mbps$
NET5301R (4 streams simultáneos):
$B_{wc} = (N_s)(B_R) + O_H = 4Mbps + 1Mbps = 5Mbps$

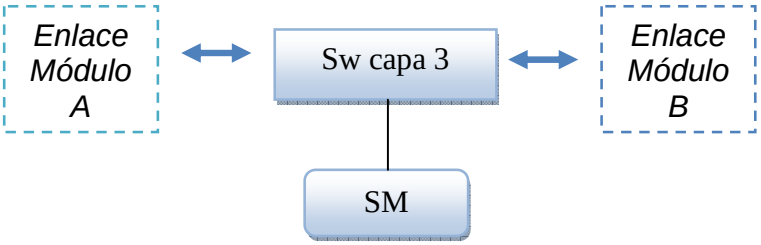
*Los cálculos anteriores fueron basados en información proporcionada por *PELCO* asumiendo que todo el video es reproducido a 4CIF (Mbps) a 30fps.

Con lo anterior se pude concluir que para el módulo B, las tareas de consulta de video ocupan más ancho de banda que la reproducción de video en vivo.

M ó d u l o C o r e

Este módulo es responsable de tareas de capa 3, realiza la autenticación y seguridad del sistema Endura y sirve de enlace entre los módulos A y B. La funcionalidad de este módulo es la siguiente:

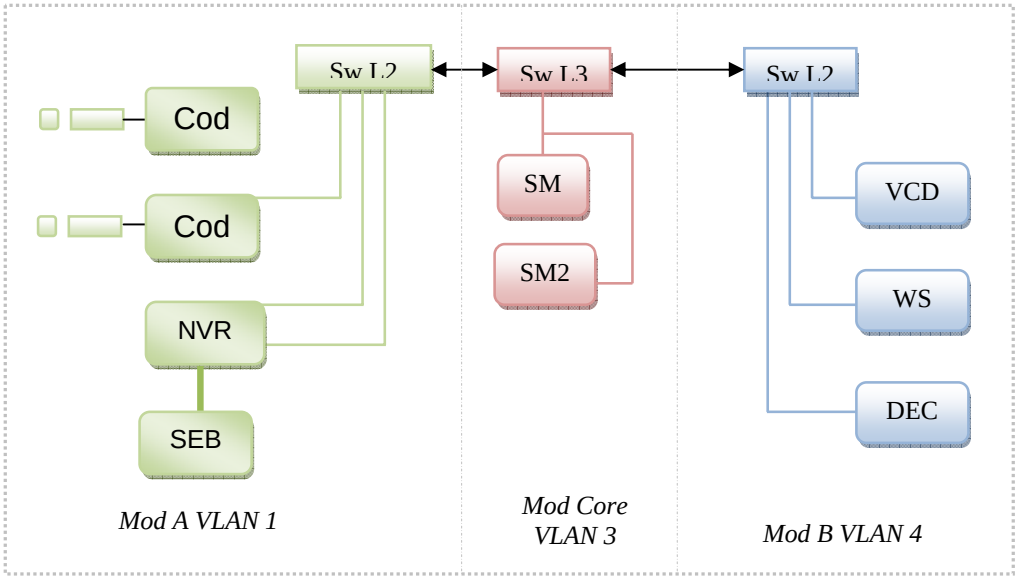
- Solamente existe un módulo de este tipo en toda la red Endura.
- El módulo Core contiene el servidor de administración (SM5000) encargado de autenticación y seguridad.
- El módulo Core utiliza una VLAN propia.
- Debe contener un switch de capa tres que una a los módulos A y B.



M ó d u l o C

El módulo C contempla toda la estructuras anteriores: A, B y Core. Implica todos los dispositivos utilizados en la solución.

Módulo C



Finalmente, Endura se puede resumir como un sistema diseñado para operar por medio de cuatro módulos los cuales permitirán la generación y almacenamiento de video en las cantidades que así se requieran.

Primeramente en el módulo A es donde todos los streams de video se generan e ingresan a la red tanto para visualización en vivo como para grabación. Para el caso de la visualización, el video tendrá que trasladarse hasta el módulo de visualización en una diferente VLAN. Cada módulo A puede tener hasta 48 codificadores y un NVR. Cada grabador digital grabará única y exclusivamente el video generado en su mismo módulo por lo tanto la cantidad de SEB's estará en función de la cantidad de cámaras y del tiempo de almacenamiento deseado.

En segundo lugar en el módulo B es donde las visualizaciones son realizadas. En Endura pueden existir múltiples módulos B como se deseen sin embargo es importante tomar en cuenta que este módulo usa la mayor cantidad de ancho de banda en la red.

Posteriormente el módulo Core realiza las tareas de administración del sistema e interconecta a los módulos de visualización y generación del video. Su único elemento que lo compone es una consola de administración y control que puede distribuir sus tareas con otro SM5000. El módulo Core provee la conectividad de red entre todos los componentes de Endura.

Finalmente el Módulo C hace referencia a toda la solución Endura, está compuesta por todos los módulos del sistema.

Endura es un sistema diseñado y planeado para abarcar necesidades de videovigilancia a gran escala. El crecimiento de la solución dependerá de la inclusión de nuevos componentes de la misma familia de los ya existentes. El incremento en las capacidades de almacenamiento dependerá de la conectividad de múltiples unidades de almacenamiento hacía las grabadoras digitales.

Para su correcta implementación y funcionamiento, Endura necesita grandes capacidades en la red de datos. La clasificación de la información generada permite tener una estabilidad en los medios y no saturar los canales de comunicación. Así también es un sistema capaz de ofrecer video de alta calidad en un entorno completamente distribuido donde los streams generados permanecerán en sus propios orígenes evitando así flujo innecesario de video en todas direcciones de la red. [4]

6.5.3 Surveillix Serie DVR *(Toshiba)*

Es la solución de seguridad más completa ofrecida por Toshiba, está basada en un diseño de almacenamiento centralizado de gran capacidad donde se administran todas las cámaras conectadas a esta unidad. Surveillix puede tener una grabadora digital de 4, 8, 16, 32 o 64 canales con discos duros de hasta 2TB de almacenamiento. El sistema Surveillix utiliza como plataforma Windows 2000 Server para su funcionamiento.

Surveillix permite la administración local y remota del grabador por medio de un software de gestión de video que controla cada una de las cámaras conectadas en forma individual. Hasta cinco usuarios simultáneos pueden administrar el grabador digital por medio de enlaces directos de red. Los perfiles de usuario se configuran con respecto a las capacidades que se necesiten: control pan/tilt, búsquedas, configuración, respaldo de información, etc.

Por ser un equipo de gran capacidad de almacenamiento, los discos duros son removibles lo que permite ser una solución escalable solamente insertando nuevos discos y en caso de falla poder remplazarse sin detener el funcionamiento del grabador digital. Así también, el DVR utiliza grabación redundante distribuida (RAID 5) para garantizar la integridad y disponibilidad de la información en video. Por las tareas de administración del video, el

DVR es un sistema que incluye sistemas de enfriamiento capaces de regular la temperatura del equipo permitiendo su estabilidad. Un DVR debe tener la capacidad de responder ante fallos de energía eléctrica, Surveillix utiliza fuentes de energía redundantes del tipo removible para poder ser sustituidas en caso de descomposturas, permitiendo la continuidad de operación del grabador digital.

Un DVR tienen la posibilidad de administrar cada uno de los dispositivos conectados a él de manera individualizada, cada cámara podrá tener configuraciones específicas de acuerdo con el escenario a visualizar. Para la captura de imágenes, existen cuatro diferentes tipos de grabación:

- *Calendario.* La grabación es realizada de manera planificada, se establece inicio – final de la grabación de cada cámara. Se puede establecer comportamientos especiales de grabación en días festivos.
- *Movimiento.* Permite establecer una grabación cuando exista movimiento frente a la cámara. Se puede establecer zonas rectangulares que permiten excluir secciones de la imagen sin importancia (movimiento de árboles, cambios de iluminación, etc.). La sensibilidad en la detección de movimiento es importante ya que se ajusta los cambios de imagen considerados como validos en movimiento.
- *Manual.* Cuando se necesita hacer una grabación rápida de algún evento, se realiza un doble click sobre la imagen, esta forma tiene prioridad sobre los tipos de grabaciones anteriores.
- *Entrada de Alarma*. Es el modo con máxima prioridad, cuando una alarma es activada, el video se puede grabar a una velocidad mayor a la establecida en frame rate, con esto se puede tener información de lo que sucedió con anterioridad hasta un minuto antes del evento.

La consulta del video almacenado es una característica importante cuando de administración se habla, ya que la búsqueda de sucesos particulares se complica cuando el video es demasiado y sin importancia. Surveillix utiliza cinco modos diferentes para la búsqueda de información:

- *Fecha.* Con un calendario se selecciona la fecha y hora del evento buscado. Técnica utilizada en todo software de administración de video.
- *Desglose.* Esta característica permite subdividir las imágenes contenidas en una selección de interés. Primeramente se muestran 24 fotos representes de las 24 horas del día, posteriormente se desglosan 6 fotos correspondientes a cada 10 minutos de esa hora seleccionada. Finalmente se publican 10 fotos correspondientes a cada minuto de ese segmento de 10 minutos escogido, así hasta llegar al evento exacto.
- *Índice.* Por medio de un registro se obtiene la fecha y la hora de las grabaciones realizadas sin importar el modo, la lista general permitirá ubicar el evento en específico de acuerdo al alarmado notificado.
- *Objetos.* Se selecciona un área en particular de interés para buscar movimiento. Los resultados de la búsqueda arrojan una lista de fecha y hora de movimiento en esa zona.
- *Gráfico.* Con renglones y columnas se representan las cámaras del sistema y las horas del día donde hubo grabación respectivamente.

Surveillix es una solución muy completa de administración del video, independientemente de sus características de visualización y consulta, ofrece herramientas útiles para control de la información que es base para considerar a un sistema como seguro. Algunas otras cualidades de este sistema son:

El software de emergencia permite desplegar la imagen donde haya una eventualidad prioritariamente a otras aplicaciones. Por medio de un sensor de alarma o botón de pánico, el DVR es configurado para que en caso de alarma se envíe automáticamente las imágenes a una computadora remota.

La administración remota permite llevar el control de las cámaras junto con su visualización en una PDA para realizar tareas de administración con conexiones inalámbricas.

El software API permite desarrollar aplicaciones especiales para integrar el DVR a sistemas de control de acceso o de monitoreo remoto para unificar a un solo sistema de seguridad. Pueden crearse paginas HTML para consulta y búsqueda de video al servicio de elementos de seguridad. El esquema de conectividad basado en Surveillix DVR tendría la siguiente distribución: **(Ver Figura 6-12)**

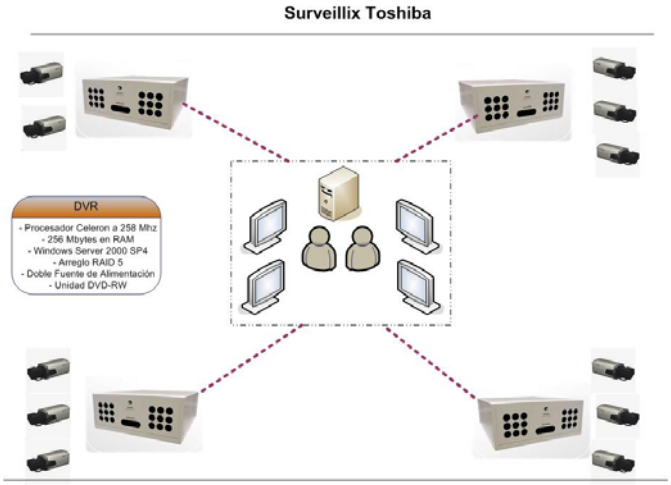


Figura 6-12. *Surveillix DVR Toshiba*

Los grabadores de video digitales realizan análisis inteligente del video (recuento de personas, obtención de matriculas, etc.) antes de codificar, comprimir y grabar. Un diseño de esta naturaleza es acorde en necesidades donde el número de cámaras no varía considerablemente ya que la capacidad del DVR está limitada a un número específico de cámaras.

Por cada una de las funciones que realiza un grabador de video digital, la implementación resulta altamente costosa, aunado a los gastos que se generarían si el crecimiento de la solución se presenta, por la necesidad de cablear cámaras hasta cada uno de los DVR's.

6.6 Selección del Sistema de Videovigilancia para el Instituto de Ingeniería

Hasta este momento se han analizado solo algunas soluciones existentes en lo que refiere a sistemas de seguridad de video en tecnologías analógica y digital. Como ya se mencionó, en el negocio de la videovigilancia cada fabricante ofrece soluciones a la medida bajo un mismo esquema: cámaras, software de administración y medios de almacenamiento masivo. Lo más importante en este momento es definir la tecnología con la cual el Instituto de Ingeniería basara su sistema de videovigilancia entre todo un mundo de soluciones existentes.

Por las dimensiones y características del Instituto, un sistema IP ofrecerá numerosas funcionalidades y más ventajas que un circuito analógico de video concretamente en los siguientes aspectos:

Un sistema basado en IP permitirá que cámaras, cableadas (*Ethernet)* o inalámbricas (*Wi-Fi*), puedan ser utilizadas sin importar su ubicación, tomado realmente a consideración los puntos mas sensibles a vigilar teniendo la entera seguridad que por medio de la red de datos o la red inalámbrica puede vigilarse esas zonas.

Una solución mucho más versátil de almacenamiento, la utilización del disco duro permitirá tener mejores velocidades de lectura y escritura con respecto a grabación en cintas magnéticas necesariamente utilizadas en CCTV, logrando un mejor manejo del video recabado con mayores capacidades de espacio, búsqueda y visualización de imágenes. Se podrá obtener video de más alta calidad en formatos utilizados hoy como AVI o en simples imágenes JPEG.

Tal vez uno de los aspectos más importantes es el factor económico, actualmente integrar un sistema de videovigilancia analógico implicaría una gran cantidad de gasto por ser un sistema aislado y dedicado. CCTV tiene como fundamento líneas de transmisión desde el origen del video hasta su lugar de monitoreo, por lo tanto para cada una de las cámaras componentes de la solución se necesitarían:

- Línea de transmisión dedicada para video (Cable coaxial RG59U a 75 Ω, 95% Blindaje en Cobre)
- Línea de transmisión independiente para control PTZ para cámaras del tipo domo; a su vez, receptores que conviertan las señales de movimiento en voltajes convenientes para los movimientos.
- Alimentación independiente hasta el punto de vigilancia para cada una de las cámaras que se necesiten controlar.

Como se puede apreciar, el cableado de líneas son costos considerables sin tomar en cuenta aquellos costos que implican cámaras, lentes y el centro de control en un diseño sencillo.

Dentro de los sistemas que basan su funcionamiento en video sobre IP, es importante identificar que solución ofrece la versatilidad de aprovechar las mejores características en generación, manejo y administración del video.

A través del tiempo la videovigilancia ha evolucionado para ofrecer sistemas eficientes a bajos costos. Después de la existencia de CCTV, la tecnología basada en DVR tomo una gran importancia por las posibilidades de grabación de video en forma digital, esta característica dio beneficios a los usuarios ya que evitaba la necesidad de cambiar cintas continuamente, lograba mejor calidad en grabaciones y la búsqueda de eventos se volvió más eficiente, sin embargo, el DVR continuaba recibiendo video del tipo analógico. Como parte de la innovación, se logro la integración de grabadores digitales a redes del tipo digital permitiendo la consulta de imágenes grabadas remotamente, por medio de un software de administración usando una computadora personal. Como última parte de la evolución, actualmente vigente se encuentra la vigilancia IP que logra que la línea de transmisión sea completamente digitalizada por medio del uso de redes locales, Internet y también redes inalámbricas.

Un DVR es un sistema hibrido ya que utiliza tanto señales analógicas como señales digitales para cumplir con sus funcionalidades, a grandes rasgos con un DVR, el proceso de digitalización y compresión ocurre en la unidad de grabación en contraste con video IP donde la mayor parte del trato del video se realiza directamente en la cámara permitiendo que soluciones más inteligentes recaigan en las propias cámaras, esta es la razón a la que se debe que una cámara IP sea claramente más costosa que una analógica.

El DVR y la videovigilancia IP comparten algunas características y funciones: grabación en discos duros, alta calidad en video, fácil consulta de video, grabación y transmisión de video sobre redes IP. No obstante, algunas ventajas demuestran la eficiencia de videovigilancia IP sobre un DVR:

- *Escalabilidad*. Videovigilancia IP permite el crecimiento de una a miles de cámaras en incrementos unitarios. No es necesario implementar por módulos de 16 cámaras como comúnmente una solución basada en DVR lo necesita. El crecimiento en almacenamiento se logra añadiendo servidores de almacenamiento a la red.
- *Reducción de costos en infraestructuras de red.* La mayoría de las entidades ya tienen un sistema de red basado en cableado estructurado así no es necesario cableado adicional y elementos muy costosos utilizados para conexiones hacía un DVR.
- *Integración de sistemas de seguridad electrónica y convergencia de red.* La videovigilancia IP es una plataforma de fácil integración para controles de acceso, sistemas de alarma, sensores de movimiento que pueden complementar la eficiencia del sistema.
- *Accesibilidad Remota.* Despliegue, consulta o manejo de configuración puede ser realizado desde cualquier parte del mundo por medio de Internet.
- *Inteligencia en cámara.* Detección de movimiento, manejo de eventos, interacción con salidas y entradas de alarma permiten a la cámara tomar decisiones inteligentes de notificación o inicio de actividades tales como grabación, cambio de frame rate, patrullaje, etc.

- *Confiabilidad del sistema.* Con medios de almacenamiento alterno utilizados en infraestructuras de red, puede integrase una solución confiable redundate que permite tener disponibilidad en la información.

Un buen sistema de videovigilancia debe tener la capacidad de adecuarse a nuevas tecnologías que continuamente se están desarrollando, Videovigilancia IP permitirá funcionalidades novedosas tales como:

- Incrementar las capacidades de análisis de video a nivel cámara, denominado como *Video Motion Detection (VMD), reconocimiento de patrones, seguimiento, detección de espacios, etc.*
- Mucho más resolución en imágenes que la ofrecida en el formato analógico NTSC (0.5 Mega pixeles), con resoluciones de hasta 3 Megapixeles.
- Cifrado de la información y autenticación del usuario a nivel cámara es un funcionalidad ya existente pero con las posibilidades de mejorar los algoritmos de cifrado.

EL DVR es una solución adecuada en soluciones de videovigilancia reducidas y donde la posibilidad de crecimiento no está considerada. El DVR fue un paso en el desarrollo de tecnologías de vigilancia en video. Actualmente todos los sistemas manejan cámaras, transmisión y grabación digital como tecnología más moderna y de mejores resultados.

Con base en el análisis realizado con anterioridad, Milestone Xprotect Enterprise es una plataforma abierta que permite aprovechar de mejor manera las funcionalidades que ofrece el video IP. Su esquema de licenciamiento permite crecer según las necesidades, así mismo permite la integración de una gran cantidad de fabricantes, lo cual es una ventaja ya que no se está sujeto a única marca y se puede aprovechar lo mejor de cada una de ellas.

Milestone Xprotect permitirá diseñar una solución completamente descentralizada que permita distribuir servidores de almacenamiento y gestión del video en todo el Instituto de Ingeniería siempre controlados por el administrador del sistema desde cualquier lugar en forma remota. Con esto se puede tener un mejor control en el flujo del video, evitando saturación de los medios de transmisión con el envío de la información a un único punto central.

Milestone Xprotect es la herramienta de mayor éxito para administración de sistema de videovigilancia IP en el mundo, sus funcionalidades son tan variadas y diseñadas específicamente para soluciones robustas de seguridad en video. La elección del software de administración es lo más importante, por ello se elige esté sistema como base del sistema de videovigilancia IP para el Instituto de Ingeniería.

Capítulo 7

Diseño del Sistema de Videovigilancia

Ha llegado el momento de definir la manera en que el Instituto de Ingeniería establecerá su sistema de seguridad en video. La distribución de la solución y la manera de utilizar las tecnologías son dos aspectos importantes que hacen la diferencia en soluciones de videovigilancia ya que cámaras mal ubicadas o esquemas de grabación mal planificados pueden ocasionar perdida de información relevante o almacenamiento equivoco de video.

Hasta este momento se ha seleccionado e identificado la solución de videovigilancia y las zonas más críticas para el Instituto, con base en las necesidades y el análisis ya realizado, se puede realizar un diseño que permita sacar el máximo partido del video IP en aquellas secciones de mayor impacto para la comunidad del Instituto.

7.1 Consideraciones para el Diseño del Sistema

El diseño de un sistema de videovigilancia no implica solamente la distribución de cámaras en todo el campus, es necesario identificar los factores que afectarán directamente a la eficiencia de la solución, por está razón, es importante considerar aspectos técnicos que influirán en el diseño.

- **Ancho de Banda.** El porcentaje de utilización del medio de transmisión está en función de la manera en que esté configurada la solución de videovigilancia, factores como: tamaño de imagen, frame rate y nivel de compresión de la imagen, afectarán de manera significativa el ancho de banda. Es importante definir las condiciones en las que se realizará la transmisión de video para apoyarse (si fuese necesario), de alarmas y sistemas inteligentes incorporados a las cámaras de red para reducir lo más posible la utilización de ancho de banda, sin perdida de información.

- **Almacenamiento.** Con este sistema, es necesario considerar grandes cantidades de información para su almacenamiento en disco duro; los factores que afectan las cantidades de almacenamiento y que deben tomarse en cuenta son: *número de cámaras, número de horas por día de grabación, tiempo de almacenamiento de información, esquemas de grabación y compresión de video.* Teniendo mucho más versatilidad en formatos de compresión, se puede aprovechar de mejor manera las capacidades de discos duros.

- **Redundancia.** Es necesario establecer respaldos de información para realizar recuperaciones de video en caso de fallas físicas. La replicación de la información ofrece una disponibilidad de la información y permite que el sistema sea confiable ante fallas comunes en soluciones basadas en redes de datos.

- **Escalabilidad del sistema.** Dentro del Instituto de Ingeniería se realizan nuevas tareas y se adquieren nuevas espacios de trabajo que necesitan ser resguardados, por está razón es importante identificar los métodos para la integración de nuevas tecnologías y la forma en que serán administrados estos nuevos elementos.

- **Velocidad de imagen.** Identificar el frame rate adecuado acorde al ancho de banda es parte importante del diseño. En los sistemas de video IP se define un frame rate adecuado a cada situación, esto evitará aprovechar los anchos de banda y los medios de almacenamiento establecidos .Así también será importante definir las velocidades de despliegue del video considerando que actualmente se pueden establecer diferentes frames rates hacia destinos distintos.
- **Seguridad.** Es importante tomar medidas de seguridad en diferentes ámbitos de la solución. Primeramente será importante considerar el tráfico de video como inaccesible por gente externa a su administración o utilización a través de enlaces lógicos independientes como VLAN´s debido a la importancia de la información que se manejará; sin embargo, como otra medida de seguridad que apoyará la integridad del sistema es un acceso controlado a nivel dispositivo donde cada elemento tendrá un control único y acorde a necesidades específicas del usuario. Para el almacenamiento, los servidores deberán estar aislados y fuera del alcance de los usuarios bajo condiciones ideales de temperatura.

Algunas características anteriormente mencionadas deberán ser consideradas en el proceso de instalación de los equipos. Factores de ancho de banda y velocidad de imagen están en función de la ubicación de cada una de las cámaras de video. Aspectos como escalabilidad, redundancia y almacenamiento son consideraciones ya realizadas en capítulos anteriores que serán retomadas como parte del diseño.

7.2 Ubicación de los puntos de vigilancia

Para identificar donde serán ubicadas cámaras de video, es importante recordar el objetivo primordial de un sistema de videovigilancia:

1. Ver remotamente uno o varios sitios de interés.
2. Verificar situaciones de excepción y dar apoyo a otros sistemas de seguridad electrónica (controles de acceso, alarmas, intrusión, etc.).
3. Registrar en un medio electrónico todos los acontecimientos.
4. Supervisar a personas y/o bienes materiales.
5. Prevención de delitos y/o accidentes.
6. Medio disuasivo de protección.
7. Toma de acciones en prevención de ilícitos y/o accidentes.
8. Seguridad Personal y patrimonial.
9. Análisis forense

El objetivo más importante a considerar es el factor *disuasión* ya que está característica es la parte principal que originará la reducción de ilícitos en el Instituto, por está razón, las cámaras de video deberán estar ubicadas en lugares visibles de tal manera que puedan generar un ambiente de tranquilidad y al mismo tiempo de incertidumbre por saber que están siendo observados.

Según cifras recabadas, en el Instituto la mayoría de los robos a bienes fueron realizados al interior de cubículos de trabajo y áreas de investigación, por estos hechos y con base en el análisis anterior las cámaras serán situadas de la siguiente manera:

Edificio 1

INTERIORES

# Cámara	*Ubicación*	*Objetivo*
1	Primer piso	Pasillo principal
2	Basamento	Pasillo principal
3	Basamento	Lab. de Sismología
4	Recepción	Vestíbulo
5	Recepción	Vestíbulo

EXTERIORES

# Cámara	*Ubicación*	*Objetivo*
6	Azotea	Zona A
7	Azotea	Zona C
8	Azotea	Zonas D y F
9	Acceso	Entrada Edificio

Edificio 2

INTERIORES

# Cámara	*Ubicación*	*Objetivo*
10	Planta Baja	Pasillo principal

EXTERIORES

# Cámara	*Ubicación*	*Objetivo*
11	Azotea	Zona E

Edificio 3

INTERIORES

# Cámara	Ubicación	Objetivo
12	Planta Baja	Pasillo principal
13	Primer Piso	Lab. de Estructuras

EXTERIORES

# Cámara	Ubicación	Objetivo
14	Azotea	Zona I

Edificio 4

INTERIORES

# Cámara	Ubicación	Objetivo
15	Planta Baja	Pasillo principal

Edificio 5

INTERIORES

# Cámara	Ubicación	Objetivo
16	1 nivel	Escaleras
17	2 nivel	Escaleras
18	3 nivel	Escaleras
19	Laboratorio Ingeniería Ambiental	Basculas de medición
20	Laboratorio Ingeniería Ambiental	Cámara de refrigeración
21	Laboratorio Ingeniería Ambiental	Basculas de medición

EXTERIORES

# Cámara	Ubicación	Objetivo
22	Azotea	Zona O

Edificio 6

INTERIORES

# Cámara	Ubicación	Objetivo
23	Planta Baja	Acceso Principal
24	Planta Baja	Lab. de Vías Terrestres

EXTERIORES

# Cámara	Ubicación	Objetivo
25	Azotea	Zona J

Edificio 7

INTERIORES

# Cámara	Ubicación	Objetivo
26	Primer Piso	Acceso principal

Edificio 8

INTERIORES

# Cámara	Ubicación	Objetivo
27	Planta Baja	Acceso principal
28	Planta Baja	Lab. de Hidromecánica
29	Planta Baja	Lab. de Olas

EXTERIORES

# Cámara	Ubicación	Objetivo
30	Azotea	Zona R

Edificio 9

INTERIORES

# Cámara	Ubicación	Objetivo
31	Planta Baja	Acceso principal
32	Primer Piso	Lab. Mesa Vibradora
33	Planta Baja	Acceso a Hangar
34	Planta Baja	Lab. Ingeniería Ambiental

EXTERIORES

# Cámara	Ubicación	Objetivo
35	Estacionamiento	Zona V
36	Azotea	Zona S y T

Edificio 11

INTERIORES

# Cámara	Ubicación	Objetivo
37	Primer Piso	Acceso Mesa de Arena

Edificio 12

INTERIORES

# Cámara	Ubicación	Objetivo
38	Sótano	Acceso a talleres
39	Sótano	Maquinaría
40	Sótano	Almacenes
41	Planta Baja	Acceso principal
42	Planta Baja	Acceso Sistemas de Cómputo
43	Primer Piso	Acceso Automatización
44	Segundo Piso	Acceso Mecánica Térmica y de Fluidos
45	Sótano	Lab. Doble Altura

EXTERIORES

# Cámara	Ubicación	Objetivo
46	Azotea	Zonas K y L
47	Azotea	Zona M
48	Azotea	Zona N

Edificio 13

INTERIORES

# Cámara	Ubicación	Objetivo
49	Sótano	Lab. Túnel del Viento
50	Sótano	Unidad de Servicios de Información
51	Sótano	Almacén general

EXTERIORES

# Cámara	Ubicación	Objetivo
52	Nivel 6, Ala Norte	Zona B
53	Área común	Zonas G y H
54	Área común	Acceso Estacionamiento
55	Área común	Salida Estacionamiento

Edificio 18

INTERIORES

# Cámara	Ubicación	Objetivo
56	Planta Baja	Acceso principal
57	Planta Baja	Vestíbulo
58	Planta Baja	Acceso laboratorios
59	Planta Baja	Pasillo principal

Hacía un proyecto completamente digitalizado, la consideración de 59 cámaras es prácticamente poco para las dimensiones y actividades realizadas dentro y fuera del Instituto; sin embargo su correcta selección, ubicación y configuración permitirá reducir el número total de elementos para videovigilancia, logrando beneficios de seguridad y registro tan fructíferos como soluciones de mayores dimensiones.

La distribución de las cámaras busca ser un modelo efectivo que tenga la posibilidad de aprovechar las mejores características del video digital a través de una red IP. Factores tales como rendimiento, interoperabilidad, escalabilidad, flexibilidad y funcionalidad son los elementos principales del diseño que permitirán tener una solución confiable y así mismo recomendable**.**

7.3 Sistema Distribuido

Las ventajas de un sistema de videovigilancia basado en IP son significativas, la distribución de la gestión y almacenamiento son características que permitirán tener un sistema seguro siempre disponible para la comunidad. Pensando en un sistema a prueba de fallas en un único punto, la distribución del video se realizará hacía diversos lugares del Instituto para lograr una funcionalidad independiente de los elementos de seguridad que conformen a cada uno de los edificios.

Basando la solución en un diseño de tres capas, arquitectura *esclavo – maestro* donde existe un servidor central como componente jerárquico principal, servidores secundarios realizarán el control de los dispositivos de seguridad en cada edificio, y podrán ser gestionados directamente a partir del servidor maestro en cualquiera de sus configuraciones. **(Ver Figura 7-1)**

Figura 7-1. *Estructura de 3 capas para el sistema de videovigilancia*

Buscando optimizar y asegurar la disponibilidad de los medios de transmisión, en cada servidor esclavo se incluirá un equipo redundante de almacenamiento que contendrá el video obtenido en esa ubicación en particular. Esta alternativa es la más rentable en un diseño distribuido que implica una gran cantidad de cámaras y por tanto gran cantidad de almacenamiento. Una única unidad de almacenamiento masivo podría ser una opción viable, sin embargo, es demasiado costoso. Una alternativa es la utilización de equipos de menores dimensiones que juntos ofrezcan la misma funcionalidad.

Así entonces, considerando un sistema basado en capas o niveles de funcionalidad y un monitoreo local para no perder efectos disuasivos, el sistema para el Instituto de Ingeniería se distribuye de acuerdo a la **Figura 7-2** presentada a continuación.

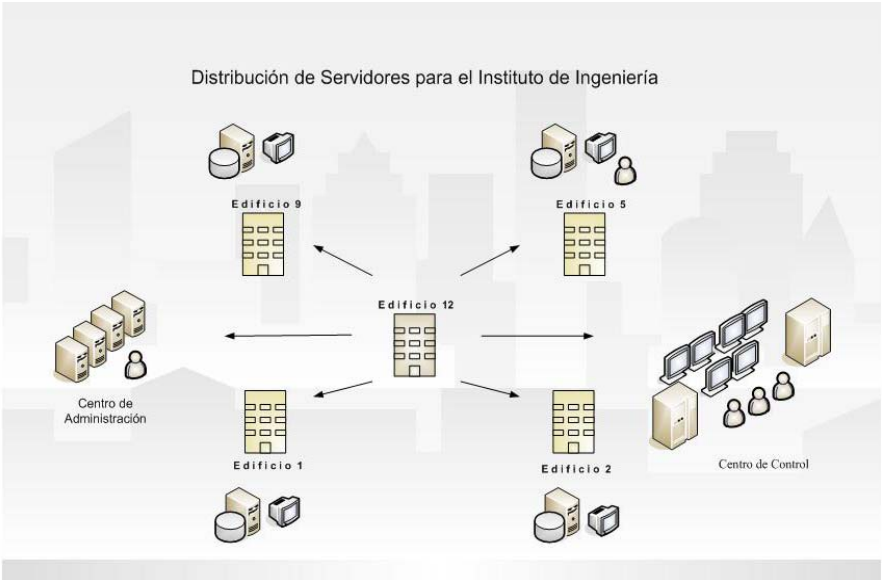


Figura 7-2. *Diseño distribuido Esclavo - Maestro*

Como se puede apreciar, el monitoreo y administración son dos actividades completamente diferentes. La configuración de esquemas de grabación y gestión de usuarios puede ser realizado desde cualquier edificio permitiendo el control total de la solución ante fallas o problemas. El personal encargado del monitoreo de cámaras debe ser diferente a aquel que realiza la administración del sistema debido a las características especificas de cada actividad. Su trabajo en conjunto ofrecerá mejores beneficios a la comunidad.

Existen algunas razones más que evidencian a un sistema distribuido como la mejor opción. Por las características del Instituto de ser un organismo compuesto por edificios y laboratorios distribuidos, la descentralización de servidores evitará tener video en tránsito por todos los edificios en los que se hayan contemplado cámaras de video, así también la infraestructura de red del Instituto brinda la flexibilidad necesaria para instalar y controlar cámaras de manera distribuida. Centralizar la grabación implicaría un consumo permanente de ancho de banda para las cámaras en actividad de 24 hrs. que puede afectar el desempeño de la red para otros servicios o aplicaciones. Finalmente, ofrece un sistema basado en subsistemas autónomos en los que se puede realizar monitoreo y administración sin verse afectado el sistema de manera global por fallas en el equipo o red, los daños y perdidas de comunicación que afectarán de manera modular a un edificio en específico.

Algunos aspectos implicados en la descentralización afectarán naturalmente a la solución. Al tener subsistemas descentralizados se incrementan las tareas de administración con respecto al mantenimiento y actualización de los equipos de cómputo. Probablemente las tareas de actualización y configuración de sistemas operativos y software de monitoreo aumenten así como su mantenimiento. Es importante considerar servidores acordes a las consideraciones de crecimiento y expansión deseadas, el idealizar servidores muy robustos, no permitirá tener beneficios monetarios convincentes para el diseño.

Finalmente, la estructura modular planteada permitirá mayor rapidez en la identificación de errores lo que reducirá los tiempos de respuesta ante fallas suscitadas y garantizará la funcionalidad del sistema.

.

7.4 La Migración al Video IP

El Instituto de Ingeniería cuenta con dos sistemas de CCTV independientes dentro de sus instalaciones. La iniciativa de los proyectos se creó por la necesidad de resguardar bienes específicos dentro de laboratorios y oficinas. Como parte de un sistema único de video seguridad, las consideraciones se ven modificadas por la necesidad de integrar estas tecnologías al diseño distribuido basado en video IP actualmente en desarrollo, reutilizando y aprovechando las inversiones realizadas hasta este momento en materia de CCTV.

La primera solución se basa en un sistema CCTV analógico de primera generación. Las imágenes son recabadas por 4 cámaras fijas conectadas a un multiplexor de señales para permitir grabar video procedente de todas las cámaras en la grabadora. El video se almacena en cassettes comunes con capacidad de hasta 8 horas de video. El medio de transmisión es el cable UTP el cual ofrece más facilidades de instalación y manejo, como parte de la evolución del CCTV analógico, el cable UTP permite enviar señales de video, alimentación de cámaras y controles PTZ por el mismo cable a distancias que van desde 300 hasta los 2400 metros.

Para poder enviar video analógico a través de cable par trenzado es necesario el balanceo de señales (acoplamiento de impedancias) a través de un elemento llamado *balum*[1] que permite adecuar las señales de video analógico (75 Ω) con el medio de cobre UTP (100 Ω). En la parte de imagen, las cámaras utilizan lentes varifocales y auto iris que permite tener un mejor control de la calidad del video controlando los cambios de iluminación. **(Ver Figura 7-3)**

[1] Cables bobinados alrededor de núcleos de ferrito con los que se logran emparejar impedancias.

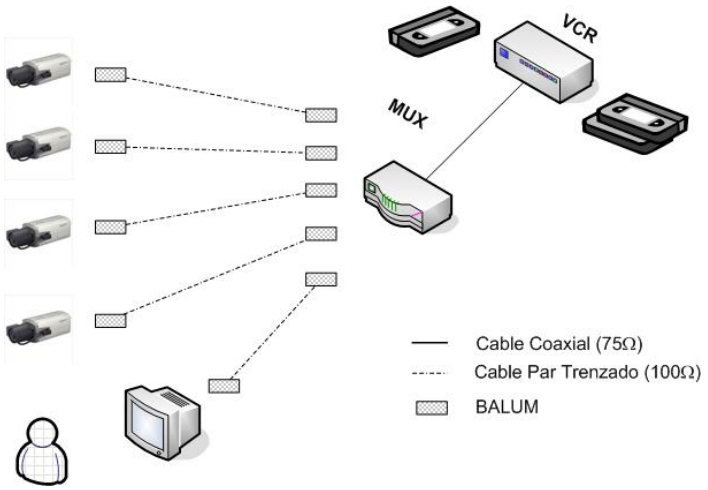


Figura 7-3. *Sistema CCTV con VCR en II.*

Un segundo sistema el video es almacenado digitalmente en un DVR. Este equipo tiene la posibilidad de administrar hasta 32 cámaras analógicas; el envío del video es a través de enlaces dedicados en cable coaxial hasta la unidad central de administración.

Se cuenta con dos cámaras fijas y una de movimiento lo que permite tener seguridad con las dos cámaras estáticas y seguimiento con la PTZ; el control de movimiento se realiza de manera serial hasta la unidad central con cable par trenzado, por lo tanto la estructura de cableado hacía cada una de las cámaras se compone de tres líneas completamente independientes (alimentación, transmisión del video y control de movimiento).

Los esquemas de grabación de esta solución es por eventos de movimiento detectados. En lo que respecta a almacenamiento, el DVR se compone de cuatro discos duros (160 GB c/u) los cuales están configurados en RAID 5 y un disco duro independiente donde se encuentra alojado el sistema operativo (Windows Server 2000 SP4) así como el software de administración del equipo (Surveillix Toshiba).

La gestión es realizada a través de la red por medio de clientes remotos que autentican a nivel DVR para realizar tareas de administración permitidas. **(Ver Figura 7-4)**

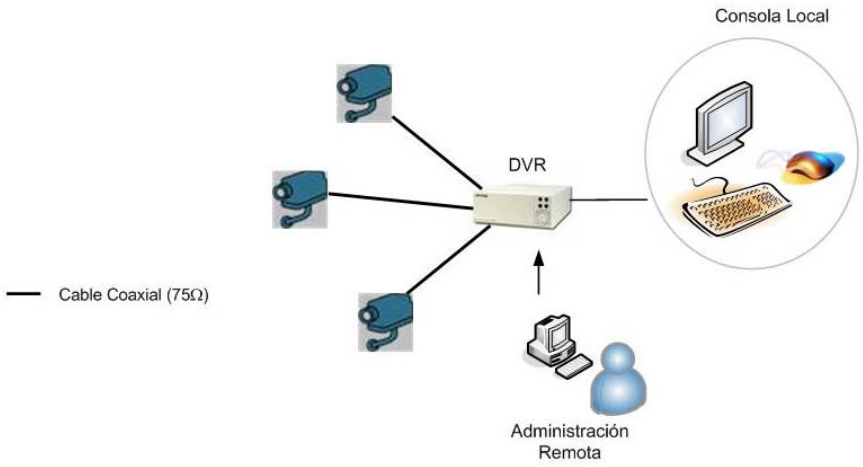


Figura 7-4. *Sistema CCTV con DVR en II*

Actualmente, las migraciones hacía tecnologías digitales son relativamente sencillas de realizar, el mercado de la seguridad electrónica ha puesto mucho interés en las soluciones IP por ser una tecnología rentable y flexible de eficiencia probada. Básicamente, la transición hacía sistemas digitales se basa en la digitalización de fuentes analógicas de video y la distribución de imágenes por medio de una red común no exclusiva. Como valor agregado, el video digital es comprimido para optimizar el uso de ancho de banda de los enlaces de comunicación por los que transitará el video. Los fabricantes ofrecen una gran cantidad de equipos que realizan codificación y compresión de señales analógicas para ser enviadas en una red de datos a diferentes destinos.

El proceso de migración se limita a elegir equipos de codificación conocidos en el medio como *servidores de video*. Un servidor de video transmite video, audio y datos digitales en estándares de compresión M-JPEG y MPEG-4 a través de la red IP lo cual permitirá ahorrar almacenamiento y ancho de banda del video convirtiendo a cámaras analógicas en cámaras en red. Concretamente el servidor de video ofrecerá las siguientes ventajas en la solución:

- Acceso remoto a cámaras analógicas a través de la red de datos, permitiendo que el control de la cámara se haga desde una computadora personal.
- Menor *Costo Total de Propiedad* logrando el aprovechamiento de la infraestructura analógica existente.
- Los beneficios del video digital ahora son aplicables en un sistema analógico.

Un servidor de video usualmente dispone de uno a cuatro puertos analógicos para conectar cámaras analógicas, así como un puerto Ethernet para conectarse a red. Así también dispone de un servidor web propio, un chip para compresión, una memoria flash

y RAM las cuales se encargan de almacenar el sistema operativo del codificador y almacenamiento temporal de instrucciones o información respectivamente.[12]
(Ver Figura 7-5)

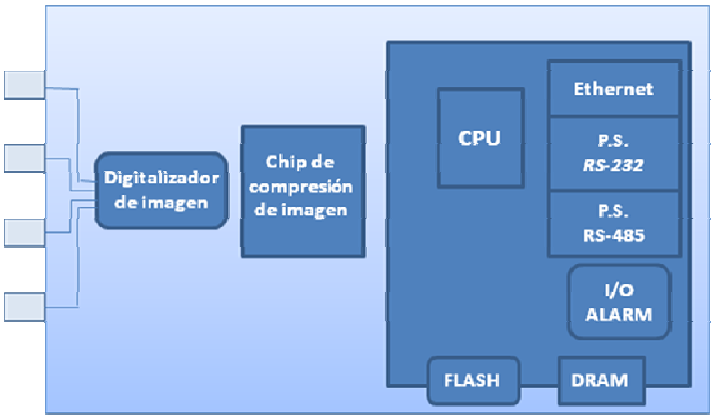


Figura 7-5. *Componentes de un servidor de video*
(Fuente: *¿Qué es un servidor de video?, White Paper,* **Axis Communications**, *Pág. 9)*

El servidor de video se conectará a la red del Instituto de Ingeniería por medio de su puerto Ethernet 10/100 Mbps, a él llegarán las cámaras analógicas deseadas, el resultado de la codificación será una imagen digitalizada y comprimida para ser visualizada en cualquier otro lugar con acceso a la red o directamente a través de su propio servidor web.

Por ser un dispositivo para integración de red, es necesaria la asignación de una dirección IP y la configuración de permisos adecuados para la visualización o administración del equipo. Para el sistema de videovigilancia del Instituto basado en el software de administración Milestone Xprotect, es posible la utilización de servidores de video para integrar las cámaras analógicas a la administración remota por IP; la integración de cámaras CCTV analógicas está restringida solamente por el licenciamiento de los puertos utilizados del codificador, un servidor de video necesitará una licencia por cada una de las cámaras conectadas a él.

Tomando en cuenta lo anterior, el planteamiento de la integración será el siguiente:

Para el sistema CCTV de primera generación se realizará una integración paulatina hacía video IP. Por los buenos resultados disuasivos que resulta el despliegue de video en tiempo real a la vista, se mantendrá el monitoreo continuo en manera local. Para obtener la misma señal de video en la red de datos, se colocará un servidor de video de cuatro canales a la solución analógica, con esto lograremos la visualización de las cámaras desde cualquier otro edificio o desde cualquier parte del mundo. **(Ver Figura 7-6)**

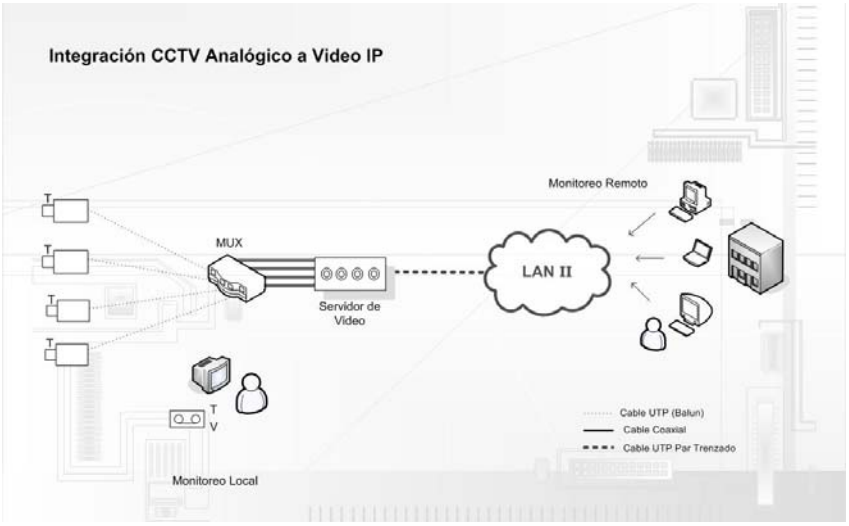


Figura 7-6. *Integración CCTV Edificio 5 a Red IP*

La utilización de señales balanceadas en este sistema CCTV no afectara la integración del servidor de video en la solución ya que el balanceo de la señal se hace en origen y destino se pueden obtener señales acordes a las necesidades del codificador para el monitoreo remoto. Para el sistema de CCTV basado en DVR, se efectuará la integración aprovechando la propia arquitectura del equipo. Como parte de su diseño, el grabador digital tiene salidas que permiten obtener alternativamente, video de cámaras analógicas conectadas al DVR (looping *outputs*), con esta característica, se simplifica la instalación del servidor de video a colocar cable coaxial como puentes a cada una de las entradas del codificador a partir de cada salida looping del grabador. Por el alto costo y capacidad de la solución, se realizarán tareas de administración por medio del equipo así como tareas de grabación para aprovechar su esquema redúndate de almacenamiento. **(Ver Figura 7-7)**

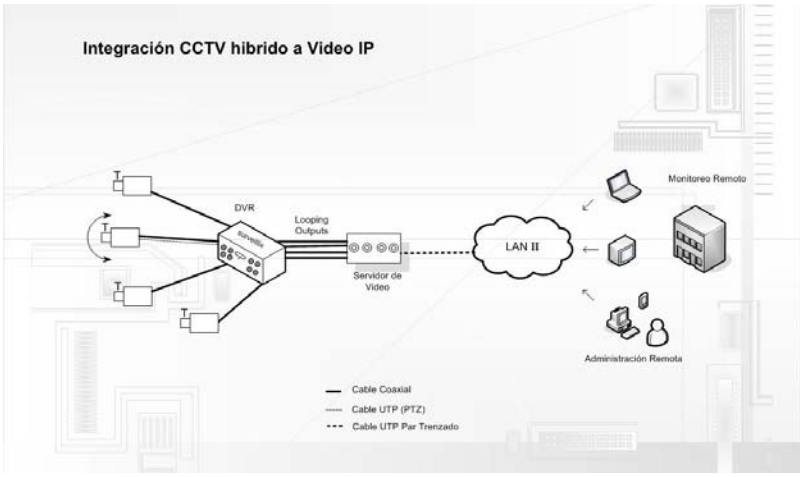


Figura 7-7. *Integración CCTV Edificio 1 a Red IP*

En ambos casos, la integración es realizada con un servidor de video de cuatro canales, suficiente para el número total de cámaras analógicas existentes. Es importante mencionar que cuando en una integración se utiliza looping output es necesario hacer la terminación de los canales (*alta impedancia*) con la finalidad de evitar imágenes distorsionadas no apreciables.[14]

En este capítulo se ha definido la distribución de las cámaras IP en las instalaciones del Instituto de Ingeniería. Tomando en cuenta las zonas más críticas y de mayor impacto de acuerdo al análisis de riesgos realizado en capítulos anteriores, se definió cada una de las posiciones las cuales fueron consideradas las mas viables y de mayor relevancia. Dentro del proceso de diseño, se presentó la problemática de integración de dos sistemas de CCTV de primera y segunda generación. La integración de los sistemas permitirá tener una solución unificada que permita ser controlada a través de la red de datos del propio Instituto. Ambos sistemas fueron integrados por medio de elementos de codificación de video que permitirán obtener imágenes digitales comprimidas hasta puntos de visualización y resguardo remotos.

Capítulo 8
Implantación

Para obtener los resultados estimados en el proceso de diseño es importante apegarse a medidas básicas que maximicen el rendimiento de un sistema de video IP. Existen factores que en la práctica serán importantes de considerar al momento de instalar una cámara que permitirán obtener buena calidad en imágenes, principio esencial para cualquier sistema dedicado a brindar seguridad por medio del video.

8.1 Instalación de las Cámaras de Video

La calidad de las imágenes que obtengan las cámaras de video está en función tanto de sus características como en la manera de realizar su instalación. Una cámara mal ubicada afectará su desempeño y evidenciará los defectos del sistema. La esencia de una buena imagen es la consideración temprana de factores existentes en medios naturales tales como:

a) Cantidades aceptables de luz permitirán video de buena calidad. Con poca luz, las imágenes se vuelven borrosas y granulares. Comúnmente la unidad utilizada para medir la cantidad de luz en escena es el *lux,* de los cuales se necesitan 200 para lograr imágenes de buena calidad. Actualmente las cámaras IP tienen buenos niveles de apreciación a un nivel bajo de iluminación ($\approx 1\ lux$). Existe también una medida denominada *lambert* que expresa la cantidad de luz que llega estrictamente a la cámara, por lo tanto, entre más clara sea una superficie en el entorno, más reflejante es y mayor cantidad de lamberts llegan al lente.

b) Evitar la contraluz permitirá tener imágenes claras y entendibles. Las imágenes pueden sobreexponerse con fuentes excesivas de luz, ocasionando que los objetos sean demasiado oscuros para poder apreciarlos.

c) Cuando una persona permanece delante de una pared blanca, la persona puede aparecer demasiado oscura ya que la cámara se ajusta en la exposición para obtener un nivel medio de luz en la imagen, por está razón, la planeación de colores claros visibles ofrecerán mejores resultados en nitidez de la imagen.

En referencia al montaje de cámaras en exteriores o interiores se deben considerar los siguientes aspectos:

a) La utilización de iris automático es indispensable en cámaras ubicadas en exteriores debido a la variedad de luz solar existente, con está característica se controla de manera automática la cantidad de luz que llega al sensor. Usualmente, las cámaras para interiores no tienen esta característica, por lo tanto una buena iluminación del entorno será suficiente para tener video de buena calidad.

b) Evitar en cualquier circunstancia exponer cámaras a la luz solar directa para evitar deslumbramiento y pérdida de color en las imágenes. Siempre es importante colocar cámaras hacía el mismo sentido que la luz natural. En cámaras interiores es importante identificar la ubicación de la cámara con respecto a la posición del edificio, en muchas ocasiones los accesos principales reciben una gran variedad luz durante el día que

perjudican el reconocimiento de rostros u objetos, por está razón es importante ubicar la cámara en esquinas de tal manera de evitar la llegada de luz directa al lente.

d) En los exteriores es importante utilizar un equipo de fijación resistente, y monturas eficaces que eviten el movimiento a causa de vibraciones, fundamental para poder tener la imagen deseada sin distorsiones.

e) Cuando una cámara es protegida por domos de cristal (carcasa o housing), puede haber un efecto de reflejo en la imagen obtenida, apreciándose el propio domo; para reducir estos efectos, la cámara deberá estar lo más cerca posible del cristal que lo protege y colocar recubrimientos antireflejantes.

f) En lugares donde la iluminación no es del todo aceptable, se puede apoyar las cámaras de video con fuentes de luz externas. Luces infrarrojas (IR) ofrecen una gran ayuda para distinguir actividad. La luz infrarroja es imperceptible para el ojo humano, logrando así buen video en blanco y negro donde mejora la resolución y sensibilidad de la imagen.

La instalación profesional de cámaras de video depende en gran medida del cuidado de los parámetros anteriormente mencionados y principalmente del lugar donde será ubicada. Si la cámara estará al alcance del personal, se necesitará una carcasa rígida contra actos vandálicos, contrariamente a las protecciones estéticas que usualmente usan las cámaras domo para interiores.

Otro aspecto importante a mencionar en el proceso de instalación es la consideración del servicio y mantenimiento de los equipos de videovigilancia. Probablemente sería una buena opción colocar una cámara en un lugar apartado de difícil acceso, en aspectos de seguridad del equipo no hay problemas, el inconveniente se daría al momento de su mantenimiento o compostura, los tiempos de acceso incrementarían considerablemente con el simple intento de llegar hasta el equipo. Igualmente mencionar el beneficio que brinda la colocación de domos oscuros en cámaras robóticas el cual genera incertidumbre en la gente teniendo siempre presente la sensación de ser observados.

Como parte del proceso de instalación, se modeló el sistema de videovigilancia en maquetas donde se realizaron pruebas de funcionalidad, cableado, visión, asignación de parámetros de red, etc., como medida para identificar fallas o defectos en los equipos de video. Dentro de un sistema tan complejo como este, es necesario antes de su puesta en producción, identificar y familiarizarse con los componentes implicados en la instalación debido a la problemática que se presenta al intentar identificar fallas en una solución completa en funcionamiento. Algunas características (brillo de imagen, ajuste de foco, sensibilidad al movimiento) se definieron durante el proceso de instalación porque estos parámetros dependen concretamente de los espacios destinados a monitorear y de las condiciones ahí presentadas tales como condiciones de luz, afluencia de personas y color de las superficies existentes.

8.2 Instalación de las Consolas de Monitoreo

El monitoreo continuo de cámaras es importante en la solución ya que permitirá visualizar en tiempo real eventos y tomar parte de ellos; las reacciones inmediatas ante sucesos inesperados evitarán efectos negativos para la comunidad y activos del Instituto.

En la videovigilancia IP, las posibilidades de monitoreo se incrementan, se vuelve innecesario tener equipos dedicados al despliegue de imágenes tales como monitores o videowalls; el video IP ofrecen monitoreo a través de un explorador de internet y en soluciones más profesionales se instalan aplicaciones cliente en aquellas computadoras utilizadas seleccionadas para el despliegue de video. Así, la funcionalidad de un cuarto de control continua siendo utilizada y se ve complementada con lugares remotos para la administración, consulta y visualización de video. Cualquier equipo con conexión a red puede actuar como herramienta de monitoreo si así se requiere.

El software de administración elegido, ofrece variantes para la conexión remota de acuerdo a la velocidad de conexión existente. El acceso remoto no se limita solamente a la visualización de cámaras IP, se utiliza también para la administración y configuración de cada una de las cámaras implicadas en el sistema. Con estas características que ofrece el video IP, las posibilidades de acceso son tres:

Milestone Xprotect Remote Client. Tipo de monitoreo que ofrece acceso a video en vivo o almacenado hasta en 16 cámaras al mismo tiempo. Permite exportar el video a formatos AVI y manejar cámaras robóticas directamente desde el cliente de ser necesario. Aplicación sencilla diseñada para hacer las tareas básicas en videovigilancia.

Milestone Xprotect Smart Client. Es la herramienta para monitoreo más avanzada. Smart Client está implementada con el lenguaje .NET que logra su integración con otros sistemas de seguridad electrónica. Este cliente ofrece las mismas funcionalidades que los programas de administración existentes en el mercado (búsqueda, visualización, configuración) así como algunas otras capacidades de análisis de video como:

- Búsqueda inteligente que permite seleccionar áreas especificas de la imagen que permite visualizar cambios solo en secciones de interés, los tiempos de búsqueda se reducen considerablemente y ayuda al usuario a encontrar acontecimientos con mayor facilidad
- Visualización rápida de secuencias con detección de movimiento.
- Visualización rápida de eventos y alertas

Milestone Xprotect PDA Client. Tipo de acceso móvil diseñado para responder más rápidamente ante situaciones. Esta opción permite llevar un control más dinámico de las cámaras y no verse en la necesidad de ubicar una computadora personal para utilizar el sistema. Xprotect PDA ofrece:

- Visualización y consulta de video de cualquier cámara de la solución.
- Control PTZ de cámaras robóticas por medio de presets o manualmente.

- Acceso determinado de acuerdo a perfiles de usuario para visualización, administración o consulta.

Xprotect Enterprise v 6.0 incluye las tres alternativas de acceso para un número ilimitado de usuarios. Con esto se tiene la flexibilidad de escoger entre tres formas diferentes de acuerdo con las necesidades existentes. Una de las ventajas de *remote client* es su capacidad de utilizarse desde el servidor central de administración al contrario de las otras versiones que son aplicaciones que debe instalarse directamente en la computadora o PDA donde se requiera.

La manera de realizar el monitoreo será por medio de una de estas alternativas. Una ventaja básica es que todas las versiones están incluidas en Milestone Xprotect Enterprise y su licenciamiento no implica ningún costo. El monitoreo continuo es una tarea complicada que comprende paciencia y completa atención por la importancia de identificar sucesos. Pensando en despliegue de imágenes trascendentales que reduzca la información en video, la versión *smart* de Milestone ofrece herramientas eficaces para ambientes de seguridad hacia múltiples usuarios. Los operadores del sistema podrán desplegar el video de cualquier cámara en cualquier monitor de computadora.

La instalación de consolas de monitoreo se limita a identificar los lugares donde se desea tener imágenes en vivo, consulta o administración. Aprovechando los beneficios de la tecnología IP, se puede tener un entorno distribuido en despliegue de video que permita responder ante situaciones que así lo ameriten. Con un buen diseño de acción y respuesta ante eventos el aseguramiento del entorno en el que se encuentra el Instituto estará garantizado.

8.3 Asignación de Recorridos y Esquemas de Grabación

La asignación de recorridos (*patrolling)* son secuencias o trayectorias que una cámara PTZ deberá realizar bajo tiempos delimitados que permitirán abarcar las zonas de mayor interés o mayor criticidad. Los recorridos son principalmente implementados en espacios abiertos donde la visión es clara y no obstaculizada.

Una cámara configurada para hacer recorridos permitirá obtener imágenes de diferentes lugares, sin embargo, la posibilidad de pérdida de acontecimientos es latente por la incapacidad de observar dos imágenes contrapuestas, la ocurrencia de dos eventos simultáneos originará la pérdida del registro de uno de ellos necesariamente. Los recorridos establecidos deben ser pensados para abarcar la mayor cantidad de espacio en el menor tiempo posible y así lograr aumentar la probabilidad de registro de incidentes.

Los recorridos establecidos para las cámaras PTZ realizarán movimientos con base a 10 presets definidos, suficiente para abarcar las áreas prioritarias en espacios abiertos. El tiempo de traslación hacía cada posición será definido pensando en tener recorridos lo suficientemente rápidos en estacionamientos, áreas de esparcimiento y de transito vehicular.

La ubicación estratégica de las cámaras permite tener un resguardo continuo de aquellos lugares críticos. El recorrido de cada cámara estará secuenciado con la dirección de movimiento existente en la cámara más cercana y así lograr un complemento en la visualización de los espacios y nunca perder de vista las áreas con mayor trascendencia.

Un recorrido también puede ser planificado por medio de eventos, la posibilidad de utilizar alarmas que indiquen a una cámara hacía donde dirigir su visión es una de las cualidades que ofrecen los sistema de videovigilancia basados en IP. Este tipo de diseño es más utilizado en interiores tales como accesos no principales o áreas restringidas donde la apertura de puertas o tránsito no es constante. Los recorridos en este tipo de aplicaciones se reducen a dos posiciones preestablecidas las cuales servirán de referencia para el comienzo de monitoreo y grabación.

Un recorrido puede ser interrumpido si así se requiere por órdenes de movimiento alternas, y puede ser continuado automáticamente después de un cierto periodo de inactividad. La alternativa de administración remota siempre está activa y puede ser bien coordinada con las secuencias establecidas en cada cámara.

Los recorridos afectan directamente en los esquemas de grabación ya que su constante movimiento origina cambios continuos de imágenes que provoca ineficiencia en los algoritmos de grabación. Como la diferencia entre cada frame siempre existe, el algoritmo de grabación lo interpretan como movimiento lo que ocasiona una grabación continua de todo el recorrido, por esto se vuelve una buena práctica la planeación de eficientes recorridos dependiendo de la cantidad de actividad en la escena.

La manera de realizar una grabación es a través de tres criterios:

1. Grabación continúa. Este tipo de registro hace referencia a las soluciones de videovigilancia de primera generación donde toda actividad era registrada sin importar los tiempos de inactividad existentes. Actualmente su utilización es aun aplicada en entornos de seguridad donde otros criterios de grabación no son útiles.

2. Grabación por evento. Tipo de registro que está condicionado a sucesos de interés particular. La seguridad electrónica ha tomado un papel importante en el ambiente de videovigilancia IP ya que permite captar solo aquellos acontecimientos que realmente podrán ser de utilidad. La eficiencia de la grabación es mejorada con este tipo de esquemas, no obstante, este tipo de diseño es más costoso por los elementos necesarios para la integración con alarmas, controles de acceso y sensores. Cada cámara puede asociarse a una alarma y activar la grabación de la cámara a una velocidad mayor a la de visualización. Para obtener secuencias completas es posible configurar el inicio de grabación segundos antes del disparo de la alarma y finalizarla segundos después de su desactivación.

3. Grabación por detección de movimiento. Este tipo de grabación es una opción no tan exacta como la basada en eventos, pero si ofrece una reducción considerable respecto a una grabación siempre continua. La idea general es la comparación sucesiva de frames que permita arrojar alguna diferencia entre ellos, bajo está

técnica, el registro de la imagen se realiza con la mínima distinción, logrado así la recolección de video que solo implique algún tipo de movimiento. Dentro de la práctica real, la detección de movimiento tiene algunos detalles que evitan que sea una opción completamente convincente; Por un lado existen problemas en ambientes donde luz natural es parte del espacio vigilado, los cambios naturales de iluminación serán reconocidos como movimiento por el proceso comparativo de imágenes subsecuentes. Por otro lado, en espacios abiertos, la actividad natural provocará cambios de imagen que serán identificados como variación lo que ocasionará almacenamiento de información intrascendente.

Las tres alternativas anteriormente mencionadas permitirán el aprovechamiento eficiente y real de los medios de almacenamiento de la solución. Un esquema de grabación bien diseñado podrá ofrecer registro en video útil que brinde evidencias claras y entendibles. Los esquemas de grabación dependerán de la ubicación y la programación de recorridos en cada cámara.

8.4 Manejo de Almacenamiento

Una vez que el video está alojado en los servidores de almacenamiento, será de suma importancia establecer políticas que definan la vigencia de la información. La cantidad de información almacenada está en función de la capacidad de los discos duros dedicados a este fin.

El esquema de almacenamiento que se tiene con el software de gestión seleccionado se basa en un repositorio temporal por cada cámara en una base de datos propietaria del software. Esta base de datos es capaz de contener hasta 600,000 imágenes o 40GB de video por cámara antes de que el registro más antiguo sea sobrescrito. Un almacenamiento alterno a unidades externas de mayor capacidad evitará sobrepasar estos límites establecidos asegurando la existencia de la información de acuerdo a los tiempos de vigencia establecidos.

El proceso de almacenamiento temporal se realiza directamente en un directorio local ubicado en el mismo sitio que los archivos de configuración e instalación del software. Dentro del directorio, subdirectorios serán creados haciendo referencia a cada una de las cámaras implicadas. El almacenamiento alterno se realiza con la utilización de una unidad de red remota donde el video será trasladado de acuerdo a una instrucción que indicará el momento de envío de información. Considerando está información y la restricción por parte del fabricante de realizar hasta 23 envíos de información, se realiza la siguiente planeación:

En la arquitectura esclavo-maestro diseñada, se estimará un crecimiento de hasta 25 cámaras por servidor como máxima cantidad de crecimiento. Una recomendación importante en los sistemas de videovigilancia en red es el despliegue de video a un frame rate bajo y el almacenamiento en mayor número, por esta razón, se considerará una monitoreo constante del video hasta 6fps en todos los casos y en actividad hasta 10 fps suficiente para distinguir detalles. Por lo tanto la cantidad de video en cada cámara será:

Video generado en cada cámara diariamente		
Frame = 50k , Frame Rate = 10fps		
Estándar	*Espacio en DD [GB]*	*Ancho de Banda [Mbps]*
M – JPEG	20.6	4.1
MPEG – 4	6.69	1.3

Así mismo, la cantidad de información máxima en cada uno de los servidores que contienen hasta 25 cámaras es:

Cantidad diaria de video en M-JPEG por servidor

No. de cámaras: 25, Resolución 4CIF y Frame Rate: 10
Cantidad de Video: 514.98 [GB]
Ancho de Banda: 102.44 [Mbps]

Cantidad diaria de video en MPEG-4 por servidor

No. de cámaras: 25, Resolución: 4CIF y *Frame Rate: 10*
Cantidad de Video: 348.69 [GB]
Ancho de Banda: 32.5 [Mbps]

Conforme a especificaciones, los registros en video tendrán hasta siete días de vigencia, de modo que la capacidad de almacenamiento para la unidad externa se obtendrá incrementando la cantidad diaria de video el número de días solicitados para su almacenamiento.

Video semanal generado por servidor	
Almacenamiento Total [TB]	
MJPEG	3.60
MPEG-4	1.17

Como se puede apreciar con anterioridad, la reducción de recursos utilizando MPEG-4 como técnica de compresión es considerable, tanto ancho de banda como almacenamiento se ven reducidos en un 50%.

Debido a la gran cantidad de información obtenida diariamente por servidor, es importante diseñar un esquema de almacenamiento alterno hacía la unidad externa para reducir los recursos utilizados en la transacción de información. Los envíos de información serán realizados paulatinamente en horas específicas con la finalidad de no saturar el disco duro local del servidor de administración con la totalidad de video de 25 cámaras. Idealmente el tipo de conexión hacía la unidad externa debe ser confiable y seguro, un enlace dedicado permitirá tener tránsito único y evitará la corrupción del video por fallas de comunicación.

Es importante identificar momentos idóneos para realización de resguardos, en caso de unidades masivas de almacenamiento en red, el tráfico generado será demasiado, por esta razón los envíos se realizarán en horas óptimas donde el porcentaje de utilización de red sea el menor, por el contrario en arreglos de almacenamiento locales, definir envíos en horas no cruciales también se vuelve importante por características propias del software que retira de funcionamiento las cámaras implicadas en envíos momentáneamente.

En el ámbito de la seguridad, los efectos concretados por amenazas son siempre negativos e inmediatos. El archivo histórico de video asegurará tener evidencia útil y permitirá delimitar las unidades de almacenamiento para evitar sus costos excesivos.

8.5 Comprobación y Evaluación del Sistema de Videovigilancia

El sistema de videovigilancia que actualmente funciona en las instalaciones del Instituto está basado en las soluciones de video IP más avanzadas hasta este momento, el diseño se realizó con base en un análisis técnico detallado donde una gran cantidad de soluciones fueron presentadas y de las cuales se eligió la de mejor relación *costo-beneficio.* Los resultados obtenidos hasta este momento han sido acordes a las expectativas planteadas al inicio del proyecto, como en cualquier proceso de implantación, algunos pormenores se presentaron en la instalación que obstaculizaron la puesta a punto del sistema.

En lo que respecta a la ubicación física de las cámaras de video, algunas ubicaciones fueron de difícil acceso lo cual dificultó su instalación y complicará su mantenimiento, las cámaras exteriores están expuestas a un mayor número de variables naturales que afectan su desempeño y funcionamiento óptimo. Primeramente las variaciones de iluminación en espacios abiertos, las velocidades alcanzadas por el viento así como la lluvia y polvo deterioran en gran medida las imágenes obtenidas y han hecho reconsiderar algunos factores como el tipo de soporte utilizado o la aplicación de algún recubrimiento repelente al agua o polvo. Es importante planificar esquemas de mantenimiento periódicos para la identificación y reconocimiento del estado de los equipos del sistema para seguir cubriendo las expectativas.

Una parte importante no considerada en el diseño original fue la instalación de un sistema no interrumpible que garantizará el funcionamiento continuo de los sistemas CCTV analógicos ya existentes. Para esto se utilizaron sistemas UPS de gran capacidad que ofrecieran dicha funcionalidad al grabador digital y a las cámaras analógicas; con este tipo de sistemas se asegura la integridad del equipo grabador en los sectores de arranque de su sistema operativo comúnmente afectados en fallas eléctricas.

Para transmisión de la información, se establecieron enlaces dedicados exclusivos para el video generado por el sistema de videovigilancia, con este tipo de medidas, se asegura la eficiencia de los otros servicios ofrecidos en la red y así también se evita que el video sature estos medios de transmisión. Con la existencia de un enlace lógicamente independiente, se garantiza la disponibilidad e integridad del video hacía cualquiera que sea su destino.

Referente al software de administración, la instalación de actualizaciones ha permitido tener un mayor número de herramientas y seguridad en el sistema. Nuevas características en gestión y visualización han sido integradas a la solución para incrementar las posibilidades en identificación de eventos y control remoto. Cabe mencionar que el cambio de versiones es un proceso laborioso del cual se necesitan tener algunas consideraciones para realizarlo. Las actualizaciones periódicas permiten realizarse sin necesidad de detener el sistema de monitoreo lo que ha sido un acierto para su buen funcionamiento.

El sistema de videovigilancia es funcional y estable, como parte de una primera etapa, actualmente contempla alrededor de 17 cámaras de video distribuidas en cuatro edificios, en los cuales diferentes esquemas de grabación han sido configurados de acuerdo con las características particulares de cada uno y la actividad existente en ellos. Actualmente conviven bajo un mismo entorno los sistemas CCTV analógicos así como las cámaras IP de última generación por lo cual se encuentra funcionando ya un sistema completamente digital.

Finalmente, la videovigilancia IP ha cumplido con lo esperado al principio del proyecto, las demandas solicitadas han sido cubiertas satisfactoriamente (a reserva de algunos detalles presentados en la primera etapa que servirán para ser considerados en etapas posteriores). Las soluciones de video basadas en IP se encuentran en desarrollo constante lo que permite tener buenas expectativas sobre el futuro del sistema y ofrece la certeza de poder satisfacer las necesidades que se puedan presentar siempre a costos bajos. Las siguientes etapas del proyecto será la inclusión del resto de los edificios al sistema, mejoramiento de esquemas de grabación con apoyo en la seguridad electrónica y la elaboración de campañas de concientízación a la comunidad para que sean participes de todos los beneficios que este tipo de tecnología ofrece.

8.6 Costo de la Solución

El costo de la solución probablemente sea el aspecto más importante en la toma de decisiones. En el ámbito de la videovigilancia hay soluciones complejas que ofrecen grandes funcionalidades de almacenamiento y gestión del video, sin embargo, el costo de implantación y manejo se torna elevado lo que las convierte en opciones inaccesibles. Realizar una evaluación económica tiene por objetivo determinar el impacto que el proyecto produce en el sentido monetario e identificar algunas alternativas que pudieran amortizar el gasto de futuras etapas.

El siguiente escenario es una recopilación económica referente al desarrollo del proyecto de videovigilancia. Por ser una tecnología relativamente reciente y tener una gran penetración en los mercados de seguridad en la actualidad, los costos totales pueden variar y no representan el gasto total definitivo de la solución.

Gastos generados en la primera etapa del proyecto de videovigilancia

Elemento	*Número*	*Costo USD*
Cámaras IP PTZ	3	**4,823.68**
Cámaras IP Fijas	7	**8,846.95**
Montajes para protección	10	**598.00**
Codificadores	3	**5,865.00**
Decodificadores	2	**2,902.00**
Infraestructura de red	-	**6,855.00**
Software de administración	1Base, 10DLK,10PMA	**7,196.70**
Instalación y configuración	-	**1,140.00**
T O T A L		**37,427.93**

La primera etapa contempla al nuevo edificio 18, algunas cámaras del Edificio 12 así como los elementos necesarios para realizar la integración de los CCTV existentes en el sistema de videovigilancia IP de este proyecto.

En el proceso de integración de tecnologías analógicas, se buscó el aprovechamiento de los componentes tales como grabadoras digitales de video, monitores y cableado en el caso de que aun sean funcionales buscando tener redundancia en la información en algunos casos.

La continuación del proyecto se realizará en una segunda etapa con la integración del resto de las cámaras implicadas en el diseño así como los equipos que servirán para la administración y almacenamiento en el esquema esclavo-maestro contemplado; por ser equipos de cómputo de grandes capacidades, su adquisición dependerá del presupuesto otorgado para el proyecto a su debido tiempo.

Según los costos observados y los elementos necesarios para la segunda etapa, se hace una estimación del gasto total necesario contemplado en esta parte del proyecto.

Gastos contemplados para la segunda etapa del proyecto de videovigilancia

Elemento	*Número*	*Costo USD*
Cámaras IP PTZ	35	56,276.26
Cámaras IP Fijas	7	8,846.95
Montajes para protección	42	2,511.61
Licencias DLK	42	12,684.00
Infraestructura de red	-	26,176.42
Servidor de Administración	5	40,037.82
Unidad de Almacenamiento Externo	5	52,884.47
Instalación y configuración	-	12,925.00
Total		**212,342.53**

Por ser un sistema distribuido, el costo de la solución se incrementa por el número de equipos necesarios para la administración en los lugares remotos, pensando en 5 ubicaciones diferentes distribuidas para gestión y almacenamiento. En está parte se considerarán 35 cámaras de movimiento y 7 fijas. Las cámaras fijas darán la confiabilidad y seguridad de registro de imágenes, la utilización de cámaras de movimiento tienen por objetivo realizar seguimiento y sirven como apoyo de visualización. En esta etapa se deberá considerar el licenciamiento individual por cámara para su inclusión en el sistema.

Con respecto a los montajes y protecciones de los equipos de monitoreo, existen diversas opciones que pueden considerarse. Para este sistema, las cámaras fijas serán protegidas por medio de carcasas para montura en pared que nos permitan la flexibilidad y el ajuste con respecto a la posición final de la cámara. Para las cámaras de movimiento, la importancia del no reconocimiento de visión es un aspecto ya considerado, para el cual se sugiere adquirir domos presurizados oscuros para evitar estudios de los recorridos de cámaras o visualización de objetivos.

La etapa tres es probablemente la fase más importante del proyecto, se trata de los ajustes que permitirán tener un sistema equilibrado que pueda tener información todavía más útil, asegurando que cualquier registro pueda ser claro e irrevocable como evidencia. Una vez teniendo toda la infraestructura de videovigilancia, se pueden mejorar los esquemas de grabación que optimicen las unidades de almacenamiento y así obtener mucho más información en menos espacio. Para esto la seguridad física toma un papel importante en el diseño, se plantea basarse en todos los elementos existentes en este campo de la seguridad y mejorar la calidad de la información recolectada.

La etapa tres también incluirá todos lo elementos no técnicos importantes para resguardar la integridad del propio sistema. En muchas ocasiones los beneficiados se sienten perjudicados o agredidos con el hecho de que una cámara los este observando, provocando actos agresivos hacía los equipos de video y probablemente a las personas implicadas en el proyecto. Por esta razón es trascendental notificar a la comunidad el objetivo real y primordial del sistema y de los beneficios que puede traer consigo una solución de esta naturaleza para sus actividades diarias. El objetivo es una estrategia de integración que permita incluir a todos los individuos que utilizan la estructura tecnológica en una organización lógica funcional. Los usuarios tomarán conciencia del hábito de la seguridad para la toma de decisiones y reacción ante situaciones complicadas acordes a su función dentro del Instituto. Un estudiante, investigador o administrativo sabrá que realizar y a quien recurrir en caso de verse afectado en algún delito.

Este sistema de videovigilancia no está limitado a recopilar información y buscar eventos de acuerdo a peticiones. Inicialmente reducirá los delitos presentados en las instalaciones del este instituto de investigación por los efectos disuasivos propios del sistema, posteriormente habrá evidencias en video de aquello sucedido en lugares considerados trascendentes dentro del Instituto. Sin embargo es importante hacer notar que los verdaderos beneficios de este sistema se verán reflejados de mejor manera con apoyo de estrategias de seguridad enfocadas a la integridad de los activos del Instituto. La identificación de la forma de reaccionar antes y después de un suceso permitirá mantener la integridad de dichos activos y minimizar los efectos que estos tendrían en caso de perdida.

Conclusiones

Este trabajo de investigación tuvo por objetivo implementar un sistema de videovigilancia apropiado para el Instituto de Ingeniería. Durante el desarrollo de la solución se establecieron etapas para la instalación y puesta a punto del sistema debido a las dimensiones del proyecto y el gasto económico que implica un sistema de esta naturaleza.

En la primera etapa del proyecto se identificaron las necesidades y requerimientos por parte de la dirección del Instituto de acuerdo a problemáticas de seguridad presentadas en sus instalaciones; se estudiaron las opciones existentes en el mercado buscando la opción técnica y financiera más adecuada; se implementó el sistema de videovigilancia en algunos edificios y laboratorios, para finalmente definir las bases y consideraciones para futuras etapas del proyecto, postergadas debido a los gastos económicos realizados hasta este momento.

Dentro del proceso de evaluación de tecnologías de videovigilancia, se comprendió la evolución de estos sistemas a través de los años. Actualmente la tercera generación basada en el protocolo IP es la forma más eficiente y segura para transportar video, que promete fuertes inversiones para desarrollos tecnológicos en este campo. Sistemas conformados por VCR's o DVR's (primera y segunda generación respectivamente) siguen siendo funcionales pero la evolución hacia nuevas tecnologías pone en entredicho su continuidad. Con respecto a esto, las inversiones ya existentes en sistemas de circuito cerrado de televisión fue una problemática presentada en el transcurso del proyecto. Se planeó una migración gradual que permitiera la convivencia de estas tecnologías en un único entorno digital. En este momento los equipos anticuados CCTV tienen la facultad de ofrecer los mismos beneficios que aquellos basados en el protocolo de comunicación IP.

El aprovechamiento de la capacidad de la red de datos del Instituto de Ingeniería fue el sustento para buscar una solución basada en IP. De acuerdo con un estudio realizado de disponibilidad de ancho de banda, los resultados arrojaron un porcentaje de utilización menor al 10 %, lo que significó una posibilidad real de utilización de este medio para aplicaciones de seguridad basadas en video con la utilización de protocolos y técnicas de compresión adecuadas.

Las etapas posteriores constarán de la puesta en marcha del resto de las cámaras en los diferentes edificios; la metodología es conocida y las consideraciones a tomar en cuenta en una correcta instalación están documentadas. El mejoramiento y el buen funcionamiento del sistema dependerá de una actualización constante en tecnologías de videovigilancia que permitan integrar nuevas funcionalidades y de un plan de mantenimiento que contemple la revisión periódica de sus componentes.

La administración y operación del sistema son tareas esenciales que deberán complementarse para garantizar la funcionalidad correcta de la solución. Las personas encargadas de la parte operativa deberán estar respaldadas con políticas de seguridad que definan los criterios y procedimientos de reacción a seguir ante diversas circunstancias. Así también, deberá ser gente comprometida con el proyecto, que lo opere de manera responsable y siempre en beneficio de la comunidad del Instituto, nunca en su contra. Con

respecto a las tareas de administración, deberán existir tiempos reducidos de respuesta ante fallas presentadas y una permanente actualización en conocimientos de videovigilancia IP por parte del administrador, para buscar el mejoramiento e integración de nuevas tecnologías.

Ciertamente, la videovigilancia no es un concepto nuevo, el gran auge que ha tenido este mercado en los últimos años ha originado nuevas posibilidades para obtener mejores sistemas de seguridad mucho más adecuados a las necesidades de usuarios finales. Para que un sistema sea recomendable debe estar apegado a diseño técnico estructurado y conformado por las mejores recomendaciones de diversos especialistas en el tema. El diseño presentado se fundamenta en un proceso de evaluación exhaustivo que incluyó entrevistas, conferencias, demostraciones, congresos y cursos especializados en el área de videovigilancia y sus aplicaciones.

De modo que, la solución expuesta en este trabajo es acorde a requerimientos específicos del Instituto de Ingeniería. No existe un único método para la implantación de tecnologías referentes a videovigilancia ya que los factores que influyen en el diseño de este tipo de proyectos son variados y en función de cada escenario.

Esta solución de videovigilancia no acabará con delitos dentro del Instituto, ni garantizará la integridad de las personas que ahí trabajan. El sistema será un elemento de apoyo dentro de una estrategia de seguridad global actualmente inexistente. Hasta este momento, las respuestas serán del tipo reactivas ante eventos lo que convierte a la solución en una herramienta de consulta de sucesos.

La planeación urgente de estrategias y procedimientos de reacción se vuelve indispensable para obtener todos los beneficios del sistema. Cambiar el paradigma de que la seguridad es un gasto y no una inversión, es una tarea difícil que implica participación de todos los niveles laborales. La cultura de la seguridad es un hábito aun no adquirido y es base esencial para cualquier proyecto de seguridad. Todas las partes implicadas deben comprender el objetivo real de un proyecto de esta naturaleza que es el de ofrecer apoyo a los elementos de seguridad existentes, así como dar confianza a la comunidad del Instituto de realizar sus labores en ambientes seguros.

Finalmente, los riesgos no podrán ser nulificados en su totalidad, la complejidad de un sistema de seguridad no garantiza su eficiencia ya que se desconocen las técnicas utilizadas en futuros ataques. Lo que es bien sabido es el destino de ataque, por está razón se debe estar preparado para reaccionar ante diversas situaciones y minimizar en lo más que se pueda el impacto que podría tener para el Instituto de Ingeniería.

Bibliografía

LIBROS

[1] Wes Simpson, *Video over IP: A Practical Guide to Technology and Applications*, Focal Press, Elsevier 2006.

[2] *Microsoft Fundamentos de Redes Plus, Curso Oficial de Certificación MCSE*, Mc Graw Hill, Tercera Edición, Año 2000.

[3] Msc. Marco Antonio Vigueras Villaseñor, *Apuntes de Redes de Computadoras*.

DOCUMENTOS, MANUALES y ARTICULOS

[4] Product Specification Book, Pelco, April 2005.

[5] Cómo elegir una cámara IP: Los diez factores principales de una elección correcta, Axis Communications, Febrero de 2006.

[6] Cámaras IP, IndigoVision, Mayo 2006.

[7] Vigilancia IP Axis, Soluciones profesionales para aplicaciones de seguridad, industriales y de supervisión a distancia, Axis Communications, Mayo 2004.

[8] Streaming Live MPEG-4, The VBasics, VBrick Systems Inc., Marzo 2003

[9] Vigilancia IP inalámbrica para Aplicaciones de Seguridad, Cómo implementar un sistema de seguridad altamente funcional, Axis White Paper Communications, Junio 2003.

[10] From VCR's to IP Surveillance, Axis White Paper Communications, Mayo 2003.

[11] Los diez principales mitos sobre el video en red, Axis White Paper Communications, Junio 2006.

[12] What is a video server?, Axis White Paper Communications, 2002

[13] Guía Técnica de video IP, Axis Communications, Agosto 2005.

[14] La migración al video IP, IndigoVision, Septiembre de 2006.

INTERNET

· **3Com Corporation**
www.3com.com

· **Microsoft Corporation:**
  – Academia Latinoamericana de Seguridad Informática,
  www.mslatam.com/latam/technet/cso/html-es/home.asp
  – Disciplina de administración de riesgos de seguridad,
  www.microsoft.com/spain/technet/recursos/articulos/secmod134.mspx

· **Communications Specialties, Inc.**
Balance inteligente de video
www.commspecial.com/deuceguidespa.htm

· **Infokrause**
www.camarasip.cl

- **LSB, Tecnología Inteligente**
  www.lsb.es
- **Cyber College**
  www.cybercollege.com/span/tvp015.htm
- **Facultad de Ciencias, Departamento de Ingeniería de Sistemas y Automática, Universidad de Valladolid España**
  www.isa.cie.uva.es/proyectos/codec/teoria1.html
- **Sección de Informática Gráfica, Universidad Politécnica de Valencia**
  www.sig.upv.es/websig/index.html
- **Fotonostra, Teoría de lentes**
  www.fotonostra.com/fotografia/objetivos.htm
- **Departamento de Tecnología Electrónica, Universidad de Sevilla, España**
  www.dte.us.es/tec_ind/electron/tc/Tema7.pdf
- **Universidad Complutense Madrid, Video Digital en Red**
  www.ucm.es/info/multidoc/multidoc/revista/cuadern5/blesa.htm
- **Servicio de Protección Civil Barcelona**
  Procedimiento de evaluación de riesgos tecnológicos en el entorno
  www.bcn.es/proteccio_civil/es/informacion/omaia/guiaomaia.pdf

FABRICANTES

- **Axis Communications**
  www.axis.com
- **Bosch Security**
  www.boschsecurity.com.mx
- **Canon, Network Video Solutions**
  www.usa.canon.com/consumer/controller?act=ProductCatIndex1Act&fcategoryid=108
- **Sony, Broadcast and Business Solutions Company**
  http://bssc.sel.sony.com/BroadcastandBusiness/index.shtml
- **Pelco Corporate**
  www.pelco.com
- **Toshiba**
  www.toshibasecurity.com
- **Panasonic**
  www.panasonic.com/business/security/home.asp

ILUSTRACIONES

Capítulo 1

Figura 1-9, Figura 1-10, Figura 1-11, Figura 1-12, Figura 1-13.
www.fuac.edu.co/autonoma/pregrado/ingenieria/ingelec/proyectosgrado/compresvideo/
Figura 1-14, Figura 1-15, Figura 1-16, Figura 1-17
www.fuac.edu.co/autonoma/pregrado/ingenieria/ingelec/proyectosgrado/compresvideo/compresion_sin_perdidas.htm

Apéndices

Apéndice A

Lentes

La calidad de la imagen es una de las características más importantes de una cámara y con mayor razón en aplicaciones de videovigilancia en las que hay mucho que perder. La calidad puede variar considerablemente según la óptica y el sensor de imagen elegidos. La lente de la cámara es un elemento que permitirá transmitir la imagen real de un objeto hasta un CCD que procesara la información recibida.

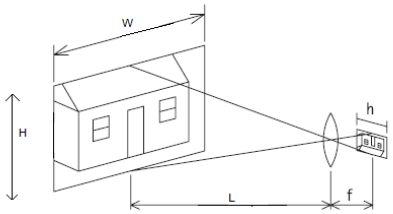
Una imagen clara y convincente dependerá de la capacidades propias de la cámara y del las configuraciones establecidas. El tipo de lente seleccionado definirá el campo de visión de la escena así como la capacidad de controlar algunos otros factores como luminosidad, sobre exposición, ruido, etc. Una medida importante en los lentes es la *longitud focal* (distancia en mm existente entre el centro óptico hasta el CCD) debido a que permite variar la distancia hacia el objeto y obtener mayor campo de profundidad; el incremento de la longitud focal acercará más los objetos debido a un ángulo de campo más estrecho.

Para identificar los detalles de alguna persona claramente, éste deberá abarcar por lo menos el 10% de la altura de la imagen. Por esta razón es importante identificar los espacios a cubrir en cada una de las cámaras para escoger el lente mas adecuado.

La elección de lentes se apoya en expresiones matemáticas que ofrecerán la mejor longitud focal de acuerdo con algunas variables físicas. La fórmula para el cálculo del tipo de lente en 1/3” y 1/2" para el tamaño del sensor se menciona a continuación:

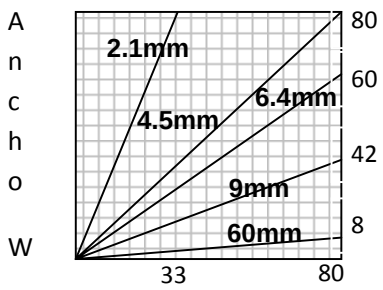
Tamaño del Sensor	**1/4"**	**1/3”**	**1/2"**
Tamaño Físico (h)	3.6 x 2.7 mm	4.8 x 3.6 mm	6.4 x 4.8 mm

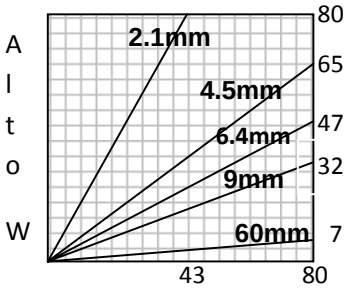
Lente 1/3”	**Lente 1/2"**
W = (4.8/f) x L	W = (6.4/f) x L
H = (3.6/f) x L	H = (4.8/f) x L



En la tabla anterior se menciona diferentes valores *h* para distintos tamaños de sensor, de acuerdo con el tipo de sensor de cada cámara, este valor tendrá que ser sustituido en la expresión matemática para el cálculo de alto y ancho de la imagen.

Relación de ancho y alto de una imagen con respecto a distintos valores de longitud focal



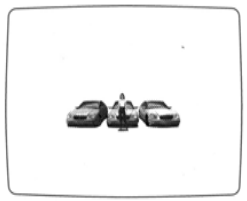
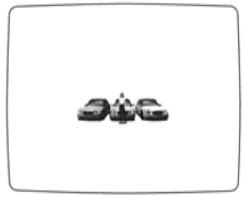
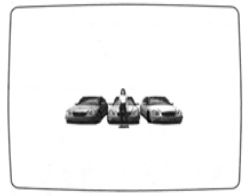
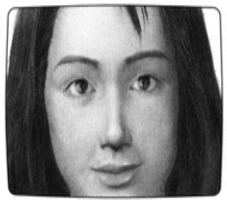
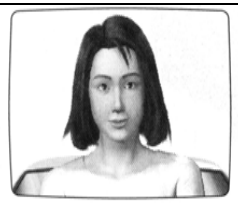


Como se puede apreciar en las gráficas, el longitud focal es directamente proporcional al tamaño de la imagen, es decir, entre más grande sea el valor f, de menor tamaño serán sus dimensiones. A medida de la longitud focal incremente, existirá un efecto de acercamiento (zoom) natural de la imagen; en los lentes varifocales existentes en el mercado (3.8 – 8mm) y (5-40mm) el efecto de zoom es de 2x y 8x respectivamente.

Los lentes no varifocales son mucho más económicos, de hecho es recomendable su utilización cuando se conoce el lugar preciso de la ubicación de la cámara y la distancia al objeto. Sin embargo para situaciones donde hay una incertidumbre de posición exacta y del escenario a visualizar, es indispensable la utilización de lentes varifocales que permitan adecuar la mejor imagen.

En el siguiente cuadro comparativo se muestra el campo de visualización con respecto a diferentes valores de longitud focal, en la representación se utilizan diversas distancias entre la cámara y el objeto. La medida *ratio* determina la proporción del área ocupada por el objeto en la imagen. Sí este abarca completamente la imagen, el ratio es de 100%; reduciendo el ratio a un 50%, el objeto disminuirá la mitad de sus dimensiones.

Está tabla servirá de herramienta para la selección del mejor lente en la adquisición de cámaras.

Longitud focal		**Distancia entre cámara y el objeto**				
		2m	4m	6m	8m	10m
3.8- 8mm CCD 1/3" 2x,varifocal	3.8mm	 2.5m x 1.9m, 84% ratio	 5.1m x 3.8m, 42% ratio	 7.6m x 5.7m, 28% ratio	 10.1m x 7.5m, 21%ratio	 12.6m x 9.5m, 17%ratio
	8mm	 1.2m x 0.9m, 178% ratio	 2.4m x 1.8m, 89% ratio	 3.6m x 2.7m, 59% ratio	 4.8m x 3.6m, 44% ratio	 6m x 4.5m, 36% ratio
5 – 40mm CCD 1/3" 8x, varifocal	5mm	 1.9m x 1.4m, 111% ratio	 3.8m x 2.9m ,56% ratio	 5.8m x 4.3m, 37% ratio	 7.7m x 5.8m, 28% ratio	 9.6m x 7.2m, 22% ratio
	40mm	 0.24m x 0.18m, 889%	 0.48m x 0.36m , 444%	 0.72m x 0.54m, 296%	 0.96m x 0.72m, 222%	 1.2m x 0.9m , 178%

* Panasonic, Security Systems, Lens Selection Chart (www.panasonic.com/security)

Apéndice B

Transformada Discreta de Coseno

La Transformada Discreta de Coseno (DCT) es usada en el estándar MPEG como una manera de compresión de video. Esta herramienta matemática permite obtener imágenes de alta precisión con menor cantidad de bits que los utilizados en una imagen original.

El DCT utilizado en MPEG utiliza bloques de imagen de 8 x 8 pixeles donde la información de luminancia y crominancia son tratadas en forma separada. La entrada del proceso DCT es un bloque compuesto por 64 pixeles que serán procesados para obtener una salida de coeficientes representativos sin información redundante. La salida obtenida no será una imagen identificable por lo que se necesitará realizar el proceso inverso (decodificadores MPEG) para crear un grupo de pixeles entendibles para el ojo humano.

El grupo de números obtenidos en la salida DCT representan la información de los 64 pixeles de entrada. Los valores obtenidos, tal como brillo e intensidad, son calculados por la comparación sucesiva de pixeles adyacentes tanto en sentido vertical como horizontal. El principio de DCT se basa en las series de Fourier aplicado al procesamiento y compresión de una imagen. Su principal diferencia es que DCT es mejor para representar en el dominio de la frecuencia, imágenes de tamaño pequeño, característica importante por el manejo de pequeños bloques de pixeles. La transformada de Fourier modelaría la imagen como si fuera periódica lo que daría como resultado representación de discontinuidades de los bordes de las imágenes que realmente no existen, lo que ocasionaría una imagen errónea.

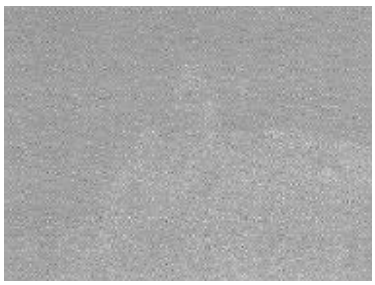
Para DCT, la transformación busca representar una imagen en el dominio de la frecuencia en forma de sus componentes fundamentales (brillos en los pixeles). Existen áreas en la imagen donde los componentes de frecuencia tendrán un valor muy pequeño al realizar la transformada, lo que permitirá omitir la redundancia de la imagen. La versión obtenida es generalmente una representación muy eficiente de la imagen original.

La técnica DCT explota la propiedad de eficiencia de la imagen de frecuencia, simplemente descartando los componentes de la imagen en frecuencia que tienen valores muy pequeños ya que al realizar el proceso inverso de reestructuración de la imagen, la eliminación de estos, representan una distorsión muy pequeña. La calidad de la imagen descomprimida dependerá de distorsiones imperceptibles logradas en el proceso. La calidad es inversamente proporcional a la relación de compresión.

El siguiente ejemplo es una muestra de la técnica DCT aplicada a una imagen con diferentes intensidades de brillo donde se pueden apreciar los beneficios reales de esta técnica con pérdidas insignificantes.

Imagen original

Imagen codificada con DCT con ratio de compresión de 20:1



Error de imagen

Las nuevas técnicas de compresión (MPEG-4) han logrado incorporar nuevas tecnologías para la compresión de video que permiten utilizar imágenes de mayor calidad en menor ancho de banda con respecto a muchos productos MPEG-2 existentes en el mercado. Como nueva innovación, el tamaño de cada bloque deja de ser fijo, lo que ocasiona que menores bloques puedan ser utilizados en áreas de la imagen con finos detalles. Otro adelanto es el uso de compresión fractal, la cual es una alternativa matemática de DCT que es usada en una gran cantidad de imágenes complejas.

Por lo tanto, la calidad de la imagen descomprimida depende del número y del tipo de componentes eliminados de la imagen de frecuencia. DCT es una técnica bastante usada en otro tipo de aplicaciones tales como H.260, H.261 y H.263 así como QuickTime y algunos gráficos JPEG. La popularidad de este algoritmo es entendible ya que es capaz de conseguir niveles de compresión 100:1, lo cual implica que la imagen descomprimida contiene 100 veces menos bits que su versión original con una muy aceptable calidad de imagen.

Apéndice C

Condiciones Generales para Videovigilancia

Constitucionalmente no existe normatividades que regulen la utilización de sistemas de videovigilancia en nuestro país, lo que origina tomar como referencia algunas leyes internacionales utilizadas eficientemente en otros países que permitan reglamentar la utilización y manejo de la información recabada en este tipo de sistemas. La grabación de imágenes de terceras personas y su tratamiento es una parte importante a considerar que puede afectar los derechos de las personas con respecto a la utilización de su propia imagen.

A continuación se citan algunas recomendaciones que podrán ser útiles en el ejercicio de grabación de video y visualización de personas, basado en aspectos legales establecidos en países europeos como España (**Ley Orgánica 15/1999**, *Protección de datos de carácter personal*) se pueden comenzar adoptando algunas normas importantes de utilidad para la integridad de la información que en este tipo de sistemas es de carácter crítico. La imagen en todo momento debe ser utilizada como un *dato de carácter personal* si aporta información clara que permita ser a una persona identificable. Por lo tanto un sistema de videovigilancia que permita a una persona física ser identificada se proponen las siguientes medidas:

a. Notificar debidamente la existencia de cámaras de video en las instalaciones a toda persona que se vea implicada en el sistema como trabajadores, visitantes, estudiantes, etc. Sugerentemente, la notificación debe hacerse de manera personal, sin embargo en entidades muy extensas basta colocar avisos que indiquen que se dispone de un sistema de visualización y grabación de imágenes.

b. En caso de las cámaras ubicadas en exteriores orientadas hacía fuera de las instalaciones, la imagen obtenida no deberá permitir la identificación de personas.

c. Las imágenes que vayan a ser visualizadas por terceras personas que permitan la identificación de rostros y que no formen parte de la estructura de funcionamiento del sistema, deberá existir el consentimiento inequívoco de las personas existentes en las imágenes.

d. Las imágenes grabadas solo podrán ser utilizadas para el reconocimiento sin exposición, y deberán ser destruidas en un tiempo de un mes a partir del momento que fueron grabadas.

e. El administrador del sistema tendrá la responsabilidad de guardar en secreto las contraseñas de administración y no divulgar información irrelevante generada.

f. Es importante establecer medidas de control para los usuarios dedicados a visualización de cámaras por medio de firma de contratos de no divulgación y sustracción de información recabada por el sistema.

El crecimiento que últimamente ha existido en los sistemas de videovigilancia ha generado dudas con respecto al tratado de las imágenes obtenidas y datos personales. En otros países la reacción hacía estas problemáticas ha sido inmediata y se han establecido normas que protegen tanto la libertad de utilización de estos sistemas como a las personas involucradas en las imágenes.

A pesar de la inexistencia de leyes en este país que respalden la utilización de este tipo de herramientas de seguridad, es importante considerar la protección de la imagen como un dato personal buscando con esto mantener la confianza de la comunidad del Instituto de Ingeniería en la realización de sus actividades

.

Glosario

Aspect ratio. Relación entre el alto y ancho de una imagen. Por ejemplo una imagen con 16:9 de aspect ratio, tiene un ancho de 16 unidades por un alto de 9. En muchas cámaras existe la posibilidad de hacer una corrección del aspecto, siendo una característica que permite el mejoramiento de imágenes analógicas cuando son desplegadas en pantallas digitales. Los pixeles que conforman la imagen se adecuan para proporcionar una representación más exacta de la imagen.

Audio channels. Funcionalidad utilizada cuando el modo de audio está activo. La transmisión de audio puede ser de diferentes tipos:

Full duplex. Audio simultaneo en dos sentidos. Transmisión y recepción de audio al mismo tiempo

Half duplex. Transmisión de audio de dos sentidos pero solamente un sentido a la vez. El proceso de comunicación se realiza por medio de un interruptor que puede activar la transmisión al ser presionado y recibir audio al soltarlo. En muchas cámaras este tipo de comunicación no funciona cuando se utiliza una compresión MPEG- 4 por características propias del estándar.

Simplex. Tipo de transmisión basada en half duplex con aplicaciones especifica, utilizado generalmente cuando se desea un canal de un único sentido. Aplicado cuando se desea dar órdenes o escuchar conversación en la escena.

Audio input. Parámetro utilizado para identificar el tipo de dispositivo conectado a la entrada de una cámara tal como un micrófono o dispositivos que proveen audio a nivel de línea.

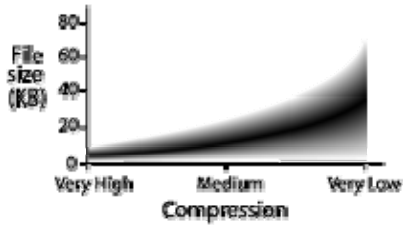
Auto Focus. Configuración que permite a una cámara utilizar su ajuste de foco de manera automática. Parámetro comúnmente utilizado en cámaras de video del tipo PTZ que continuamente están cambiando de imagen.

AVI. Formato de video desarrollado por Microsoft con información de video y audio. Soporta una extensa variedad de algoritmos de compresión y puede ser convertida a otros formatos como MPEG. Este tipo de archivo es usualmente usado para exportar segmentos pequeños de video.

Back Light Compensation (BLC). Cuando el fondo de la imagen es demasiado brillante o el objeto demasiado oscuro, BLC hace parecer al objeto más claro. La utilización de BLC es solamente posible cuando se utilizan lentes del tipo auto iris.

Bit Rate Control. Característica que permite ajustar la cantidad de bit rate utilizado por la cámara para controlar el ancho de banda disponible. Definiendo un bit rate sin límite permitirá proveerá imágenes consistentes de muy buena calidad pero con la utilización de mayores anchos de banda con respecto a mayor complejidad en la imagen. Limitando el bit rate a un valor definido prevendrá uso excesivo ancho de banda pero las imágenes se perderán cuando el límite sea superado.

Compression. El nivel de compresión afecta la cantidad de ancho de banda utilizada, menor compresión mejora la calidad de imagen pero usa más ancho de banda. El nivel de compresión también afecta el tamaño de las imágenes utilizadas, a continuación se muestra una gráfica comparativa cuando es utilizado M-JPEG a resolución CIF.



Crhoma. Parte de una señal analógica que contiene información referente a color.

DCT (Discrete Cosine Transform). Técnica matemática usada en MPEG y otros algoritmos de compresión. Se utiliza para reducir la cantidad de datos requeridos para representar un bloque de pixeles.

DHCP (Dynamic Host Configuration Protocol) Servicio para asignar una dirección IP a un dispositivo cuando es integrado a una red. Permite llevar un mejor control de las IP asignadas y simplifica la administración de equipos.

Dynamic DNS Service. Servicio que ofrece un registro dinámico de la cámara ante servidores de resolución de nombres. La idea principal es ofrecer un acceso único definido sin importar la variación de direcciones IP otorgadas a la cámara de video.

Echo Cancellation. Cuando el audio de una bocina es capturado por un micrófono, este producirá un eco. Con esta opción se reduce el efecto acústico generado.

ElS (Electronic Image Stabilization). Característica que permite por medio de un proceso electrónico controlar la estabilidad de una imagen, sí el sensor de la cámara detecta un movimiento, EIS responde con un mínimo movimiento en la imagen para que esta se mantenga en el mismo sitio en el sensor CCD, la desventaja de utilizar esta característica es la afectación en la resolución de la imagen.

Exposure Control. Opción que permite controlar el tipo y cantidad de luz en la escena. Las posibilidades permiten adecuar la imagen a condiciones de luz variables o respecto a condiciones especiales de luz.

FireWall. Elemento utilizado para proteger redes locales de agentes maliciosos existentes en Internet. Puede ser implementado vía hardware o software de manera perimetral para evitar ataques a servicios críticos.

Gain. Medida en decibeles (dB). La ganancia describe la cantidad de amplificación aplicada a una señal (información visual en la imagen). Aunque es posible recuperar imágenes en niveles de luminosidad bajos, altos niveles de ganancia incrementan la cantidad de ruido en la imagen.

Gbps (Gigabit per second). Tasa de transmisión de datos a una velocidad de 1 billón de bits por segundo.

GOV length. Parámetro que determina la cantidad de imágenes del tipo I o P serán enviadas antes que el siguiente grupo sea enviado en el estándar MPEG-4. Una estructura del tipo I, describe el número de I imágenes a utilizar. Una estructura del tipo IP, determina la suma total de imágenes del tipo I y P en el GOV. Entre más grande sea el tamaño de GOV menor cantidad de ancho de banda será utilizado pero la calidad de imagen decaerá considerablemente.

GOV structure. Determina la composición de los streams de video MPEG-4 por medio de sus elementos básicos. La estructura puede ser de dos tipos diferentes I o IP, la cual describe el tipo de imágenes incluidas en el stream así como su orden interno. La imagen I es una imagen completa mientras que la imagen P son las diferencias de la imagen de comparaciones precias de otras imágenes. (GOV = Group of VOP's, VOP = Video Object Plane, Video Object Plane = imágen).

IR cut filter. Este parámetro controla la visualización de luz infrarroja. Si está configurado como auto, la cámara automáticamente cambiará de acuerdo a las condiciones de luz presentes.

Luma. Parte de una señal de video analógica que contiene información de brillo de la imagen. La señal de luma puede ser convertida a una imagen de video monocromática (blanco y negro). Cuando una señal luma es procesada en conjunto con una señal croma, una imagen completa a color puede ser creada.

Macroblock. Unidad fundamental en los algoritmos de compresión utilizados en MPEG que contiene una porción de imagen de 16 x 16 pixeles de un frame. El termino “macroblocking” es usado para describir el deterioro en una imagen donde porciones han sido remplazadas con bloques de colores que ocupan 16 x 16 pixeles. Este efecto es causado por perdida de información durante el proceso de decodificación

Mbps (Megabits per second). Tasa de transmisión de datos igual a 1 millón de bits por segundo.

MPEG (Moving Pictures Experts Group). Organización formada en 1988 para desarrollar estándares internacionales para codificación y almacenamiento de video digital. Una gran cantidad de estándares han sido producidos por este grupo con aprobación internacional de ISO/IEC. Actualmente el acrónimo MPEG es utilizado para describir una amplia diversidad de formatos de compresión.

Multicast. Transmisión de datos desde un único origen a múltiples y simultáneos destinos

Noise canceller. Configuración que permite reducir el ruido de una imagen. Una aplicación típica es cuando la cámara se encuentra en una ambiente de mucho ruido natural y solamente existe el interés en escuchar un sonido en particular. Para optimizar esta función existen dos parámetros: Noise Canceller Treshold Value y Noise Canceller Attenuation

Unicast. Transmisión de datos desde un único origen a un único destino.

WDR (Wide Dynamic Range).Es una característica de algunas cámaras que permite mantener un contraste aceptable en imágenes ante condiciones lumínicas complejas, A pleno sol, a contraluz y en áreas de sombras

White Balance. Parámetro utilizado para hacer parecer a los colores siempre los mismos y compensar su diferencia ante diferentes fuentes de luz.