UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

Facultad de Estudios Superiores Aragón

"IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV) CON ACCESO Y MONITOREO VÍA INTERNET."

TESIS
PARA OBTENER EL TÍTULO DE
INGENIERO MECÁNICO ELECTRICISTA
AREA: ELÉCTRICA - ELECTRÓNICA

PRESENTA:

DE HARO PÉREZ ALMA VIRIDIANA

QUIJANO BAZÁN HÉCTOR ABRAHAM

ASESOR: MTRO. VÍCTOR MANUEL SÁNCHEZ MORALES

Bosques de Aragón, Estado de Mexico, Mayo de 2015.

Objetivo general

“RELACIONAR LA IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO DE UN SISTEMA DE CIRCUITO CERRADO DE TELEVISIÓN (CCTV) CON ACCESO Y MONITOREO VÍA INTERNET.”

Objetivos particulares

- Conocer los tipos de cables así como realizar la conexión adecuada para evitar ruido y perdida de video en sus instalaciones de cámaras de vigilancia
- Diferenciar los tipos de cámaras, de lentes así como la configuración de funciones básicas para diferentes entornos de exposición.

Introducción

Con el transcurso de los años, el rango de entornos en el que se implantan sistemas de seguridad ha crecido considerablemente debido a la creciente demanda de seguridad y de soluciones más sofisticadas por parte de la sociedad.

La Ciudad de Mexico ha decidido instalar cámaras en las calles principales (decisión que ha creado cierta polémica en la población, ya que consideran que con la presencia de estas cámaras se atenta contra la intimidad).

Las nuevas propuestas para la mejora de los sistemas de seguridad se realizan tanto en el ámbito académico como en el comercial La principal diferencia entre unas y otras, es que las propuestas comerciales están bastante más orientadas a la utilización de hardware específico y a la implantación inmediata con el objetivo de obtener grandes beneficios económicos. La mayoría de estos sistemas no van más allá de la detección de intrusos y seguimiento de los mismos en la escena. Sin embargo, las propuestas que se realizan en el ámbito académico suelen ser algoritmos avanzados de gran complejidad, que no están ligados a dispositivos hardware concretos y no suelen ser utilizados en el mercado hasta que no trascurren algunos años desde su publicación. Algunos de los entornos donde se instalan sistemas de seguridad comerciales y se realizan investigaciones desde el ámbito académico son los siguientes:

- **Aeropuertos.** Los aeropuertos son uno de los entornos que demandan mayores medidas de seguridad, debido en gran parte a que son uno de los principales objetivos de los grupos terroristas.
- **Entornos marítimos.** Los sistemas de vigilancia también tienen cabida en entornos marítimos. los sistemas de seguridad para la vigilancia en puertos de carga y descarga de mercancías.
- **Estaciones de tren.** Seguridad en estaciones de tren y vigilancia en vías de ferrocarril.

- **Vigilancia en tráfico**. Cada año los departamentos de tráfico de los países más desarrollados invierten una cantidad de dinero importante en la instalación de cámaras de seguridad en las carreteras públicas. La principal función de estos sistemas es la detección de congestiones en el tráfico y posibles accidentes que requieran la atención de los servicios sanitarios.

En varios países, la videovigilancia no ha sido objeto de legislación específica en la actualidad, sin embargo, las autoridades de protección de datos, fundamentalmente de los países europeos, han estado trabajando para garantizar la aplicación adecuada de las disposiciones generales sobre la materia, en el caso de nuestro país existe una regulación por estado, (**Revisar Anexo**) y se usa para seguridad pública y no para uso particular

Actualmente, el incremento de atentados llevados a cabo por diferentes grupos, los delitos cometidos por pequeñas bandas organizadas, o el aumento de vandalismo en las grandes ciudades, son algunas de las principales fuentes de preocupación e incertidumbre en la actualidad. Tanto es así, que un gran número de gobiernos e instituciones han tomado la decisión de reforzar las medidas de seguridad como posible solución. Por tanto, hoy en día es común observar cámaras de seguridad instaladas en bancos, casinos, comercios, grandes empresas, calles conflictivas, etc.

La instalación de dichas cámaras permite aumentar la seguridad en la zona y reducir el índice de delincuencia y degradación. En más de una ocasión, los sistemas de seguridad se han convertido en los aliados perfectos de los cuerpos de seguridad, ya que las grabaciones han servido para evitar delitos, o como indicio para conseguir pruebas en el caso de que éstos se hayan producido.

La operación de 12 mil cámaras de vigilancia hará de la Ciudad de México una de la ciudades más seguras del mundo. El proyecto de alta tecnología instrumentando desde 2008 por el Gobierno del Distrito Federal, a iniciativa del

jefe de Gobierno, permitirá a las autoridades responder de manera inmediata ante emergencias, situaciones de crisis y actos ilícitos.

El Proyecto Bicentenario: Ciudad Segura consta de equipos de vigilancia, botón de emergencia y altavoz, para interactuar con la ciudadanía; con ello mejorará el nivel de vigilancia y la acción policial, ya que al realizar un trabajo coordinado de todas las áreas de gobierno, el tiempo de respuesta se acota a 5 minutos desde el momento que la autoridad tome conocimiento de la emergencia o el ilícito.

El Gobierno del Distrito Federal analizó los sistemas de videovigilancia que se han implementado en ciudades como: Jerusalén en Israel; Londres y Liverpool, en Inglaterra; Singapur; París, en Francia; Baltimore y Chicago, en Estados Unidos; Medellín y Bogotá, en Colombia. De esta forma, se instrumenta el Proyecto Bicentenario: Ciudad Segura con base en las necesidades propias de la capital del México, para disminuir la incidencia delictiva con el apoyo de la tecnología.

El Proyecto inició con la instalación de cámaras y sensores en todas las delegaciones del Distrito Federal, luego de que se emitió la Ley que Regula el Uso de la Tecnología para Seguridad Pública, que establece en más de sus preceptos "Contribuir al mantenimiento del orden, la tranquilidad y estabilidad en la convivencia, así como a prevenir situaciones de emergencia o desastre e incrementar la seguridad ciudadana".
Con el Proyecto Bicentenario Ciudad Segura, la Ciudad de México se coloca como la primera a nivel mundial en materia de seguridad urbana al incorporar alta tecnología para garantizar la tranquilidad de sus habitantes.

En este trabajo de tesis se enfocara en la implementación y puesta en marcha de un sistema de videovigilancia de uso particular donde se presentara el equipo a utilizar y la realización de un caso práctico señalando el costo y alcance del mismo.

Capítulo 1
Antecedentes de sistemas de video vigilancia

Durante los últimos años, se registró un considerable incremento en la cantidad de equipos de vigilancia en video instalados por empleadores dentro de los establecimientos de su empresa. Ya sea que estas cámaras de video se encuentren ocultas o no, persiguen básicamente el mismo objetivo: la protección del negocio de empleador no solamente contra posibles intrusos, sino también contra sus propios empleados. Tomando en cuenta la protección de privacidad dispuesta, razonablemente podríamos objetar la legalidad de esas instalaciones.

¿Se protegen los derechos de privacidad del empleado en su lugar de trabajo? En caso afirmativo, ¿Hasta dónde se aplica la protección de privacidad en el lugar de trabajo dado que el empleador también tiene el derecho de proteger su empresa?

La privacidad no se limitaba a la residencia de los ciudadanos y que se podía aplicar a otras situaciones, como por ejemplo el lugar de trabajo. Dicho esto, la protección de privacidad del empleado en el lugar de trabajo no constituye un derecho totalmente inalienable. De hecho, también debemos tener en cuenta el derecho del empleador a proteger su empresa.

En vista de los derechos precedentes, que se encuentran en oposición directa, surge la siguiente pregunta: ¿Dónde se traza la línea entre el derecho del empleado a la protección de la privacidad y el derecho del empleador a la protección de su propia empresa?

1.1 Concepto de luz

La luz es una forma de energía radiante electromagnética que percibimos con el sentido de la visión. Se considera a la luz como un fenómeno electromagnético,

por lo tanto está constituida por partículas electromagnéticas denominadas “fotones” que se desplazan a través del espacio a una velocidad constante, siguiendo trayectorias rectilíneas, con un movimiento ondulatorio y propagándose en el vacío, en el aire y a través de todos los cuerpos transparentes como el agua y el vidrio.

La luz es irradiada a través del espacio en todas las direcciones. Su movimiento ondulatorio se propaga en línea recta y la velocidad de esta propagación depende de la densidad del medio transparente que atraviesa.

El sol emite energía radiante electromagnética (espectro radiante) compuesta por energía radiante visible (luz), y energía radiante invisible como las radiaciones ultravioleta (U.V.) e infrarroja y otras radiaciones. Figura 1.1

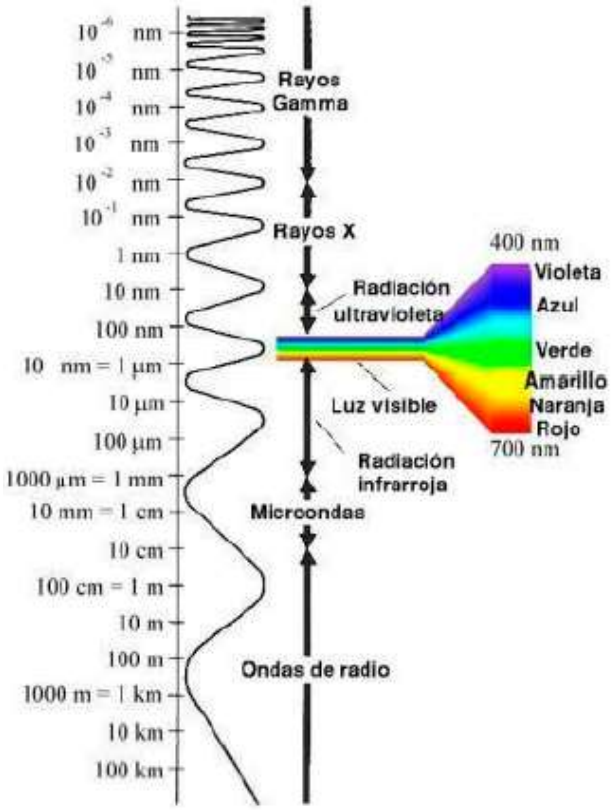


Figura 1.1 longitudes de onda (nanómetros) Del espectro electromagnético.

Como se puede apreciar en la figura anterior , la luz ocupa una zona muy reducida en el conjunto de ondas electromagnéticas del espectro total, también integrado por un grupo de ondas invisibles que abarcan, desde un extremo a otro, a los rayos cósmicos, rayos gamma, rayos X, radiación ultravioleta, rayos infrarrojos, microondas, ondas de TV, de radio, etc.

A pesar que estas radiaciones son invisibles al ojo humano, varias de ellas pueden estimular los componentes fotosensibles del material fotográfico, como por ejemplo los rayos X (radiografías), los rayos gamma (gammagrafías), haces de electrones (fotografías obtenidas con el microscopio electrónico) y las fotografías que se captan con instrumentos especiales (microscopios y cámaras fotográficas) que “iluminan” o irradian a los objetos con rayos ultravioleta (fluorescencia) o con radiación infrarroja. Los fotones son partículas sumamente pequeñas, de masa igualmente pequeña que no puede ser medida pero poseedoras de gran energía que, al desplazarse en el espacio lo hacen de manera ondulatoria y en línea recta, por lo tanto un rayo luminoso posee las características del movimiento ondulatorio.

1.2 Propiedades de una onda luminosa

Las propiedades de una onda luminosa son:

a) **Longitud de onda.** Es la distancia que existe entre dos crestas o dos valles sucesivos de la onda luminosa. Las longitudes de onda de la luz son muy pequeñas: Generalmente se miden en nanómetros (nm) o en angstroms (Å). Si observamos la figura 1.1. (página anterior) Las longitudes de onda del espectro radiante visible abarcan entre 400 nm. (Color violeta) a 700 nm. (Color rojo). La longitud de una onda luminosa se expresa por la letra griega lambda (λ).

   Existen otras formas de energía radiante que poseen longitudes de onda muchos menores como la radiación ultravioleta, los rayos X, la radiación de electrones, los rayos gamma y aún más cortas como los rayos cósmicos.

Entre las formas de energía cuyas longitudes de onda son más largas que las de la luz, están consideradas la radiación infrarroja (calórica) y las ondas de radio que suelen medir varios metros de longitud.

Las diferentes longitudes de onda de la luz son percibidas como colores. Esto significa que cada color observado por el ojo humano o captado por el material fotográfico sensible se debe a la estimulación por una determinada longitud de onda del haz luminoso.

Un haz de luz blanca es visualizado como tal, cuando lo integran una mezcla uniforme de rayos luminosos de todas las longitudes de onda. El ojo humano percibe el color porque la retina contiene dos tipos de células nerviosas fotosensibles conos (perciben colores) y bastones (captan sensaciones de blanco y negro). Los conos, a su vez, son células que dependiendo de la longitud de onda que los estimula, captan los tres tipos de colores primarios: azul, verde y rojo.

El material fotográfico sensible (películas y papeles) a colores, posee tres capas sensibles para cada una de estas longitudes de ondas luminosas, por lo tanto debemos considerar que el espectro visible que capta este material está integrado por los citados rayos luminosos. Figura 2.2

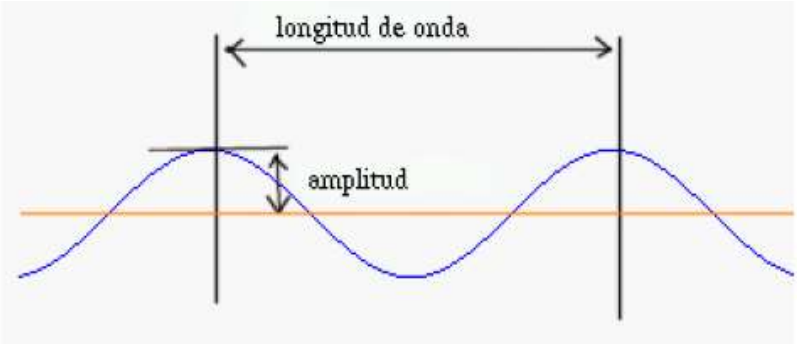


Figura 1.2 Esquema de una onda luminosa mostrando su longitud y su amplitud.

La figura muestra el esquema de una onda de luz, en el que se observan las crestas (a) de la onda así como sus valles (b). Se denomina un ciclo de la onda a la distancia recorrida por el fotón entre dos crestas o dos valles.

b) **Amplitud de onda.** Es la distancia que existe entre la parte superior e inferior de la onda (fig. 1.2) La amplitud de onda le confiere a un rayo luminoso, la intensidad luminosa o brillantez sin modificar el color. Esto significa que si un haz luminoso de un color determinado es más intenso o más brillante que otro del mismo color es porque la amplitud de onda del primero es mayor que la del segundo.

c) **Características de la luz.** En un determinado medio, la luz se desplaza en línea recta y con una velocidad constante. La luz se desplaza también en un espacio relativamente vacío y en el vacío total, esto a diferencia de las ondas sonoras y de las ondas de agua que requieren de un medio material para que puedan existir y desplazarse. Cuando un rayo luminoso pasa de un medio menos denso (aire, por ejemplo) a otro transparente de mayor densidad, como el agua, vidrio o plástico, su velocidad disminuye. Sin embargo, si abandona este medio más denso y se desplaza nuevamente en el medio menos denso, recobra su velocidad original. Estos cambios de velocidad son importantes pues producen una de las características de la luz: la refracción.

La luz que se origina de una fuente emisora se desplaza o irradia en todas direcciones. De tal forma que su energía se dispersa a medida que se aleja de su punto de origen; por lo tanto, la energía luminosa que incide sobre una superficie situada a cierta distancia será menor que la que incide sobre la misma superficie pero situada más cerca de la fuente emisora. Este hecho se percibe como un cambio en la luminosidad. Cuando la luz se desplaza a través del aíre suele llegar a la superficie de algún objeto, figura 1.3 y, en ese punto la luz puede ser:

- **Reflejada:** Las superficies de los objetos no transparentes reflejan o "rebotan" la luz.

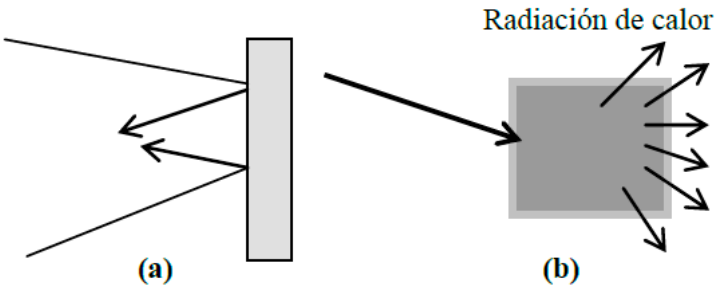


Figura 1.3 a) luz reflejada; b) luz absorbida

- **Absorbida:** Si el objeto es opaco (no transparente), la luz no
- reflejada en su superficie es absorbida por el objeto y desaparece. La energía luminosa absorbida se transforma en energía calórica dentro del objeto.
- **Transmitida:** Si el objeto es transparente, la mayor parte del haz luminoso lo atraviesa y continúa su desplazamiento a través del mismo.

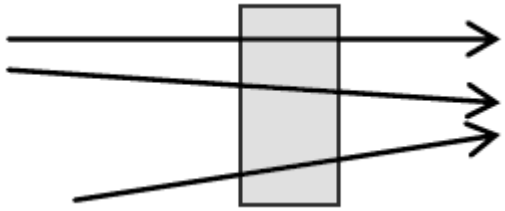


Figura 1.4 Ondas luminosas transmitidas a través de un objeto transparente.

La energía total de un haz luminoso que llega a un objeto (luz incidente) debe equivaler a la suma de la energía de la luz reflejada, absorbida y trasmitida. El material óptico que trasmite los rayos luminosos, de acuerdo a una disposición y orientación definida y regular de sus moléculas, se denomina transparente. Si trasmite la luz pero desordena el trayecto de los rayos y los dirige en todas las

direcciones, recibe el nombre de translúcido. Si un material absorbe la mayoría de los rayos luminosos se dice que es opaco.

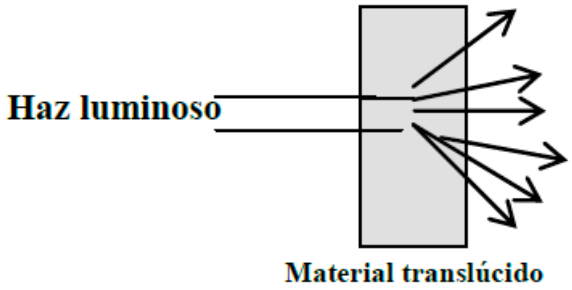


Figura 1.5 Recorrido de los rayos luminosos en un material translúcido.

Cuando un rayo luminoso emitido en un medio de menor densidad incide sobre un cuerpo transparente de mayor densidad y que posee superficies planas (un vidrio grueso, por ejemplo) lo puede hacer en varios ángulos de incidencia. Dependiendo del ángulo de incidencia el rayo luminoso experimenta varios fenómenos:

I. Si lo hace perpendicularmente a la superficie del cuerpo transparente. El rayo luminoso lo atraviesa sin experimentar ningún tipo de desviación en su trayectoria. La modificación que experimenta es disminuir su velocidad.

El rayo luminoso incide de manera oblicua sobre la superficie, en un ángulo equivalente a 45o grados o menos. En estas condiciones, el rayo luminoso no atraviesa el cuerpo transparente, y “rebota” sobre su superficie, en un ángulo similar al de incidencia. A esta característica se le denomina reflexión de la luz.

La velocidad de la luz es de 300,000 Km/seg en el aire. Al atravesar ese medio transparente (vidrio) su velocidad se reduce a 200, 000 km./seg. Por lo tanto el vidrio tendrá un poder de refracción de 1.5 pues el índice de refracción se expresa de la siguiente manera:

$$R = \frac{\text{Velocidad de la luz en el aire}}{\text{Velocidad de la luz en el medio}} \qquad \textbf{Ec. 1.1}$$

La cifra expresa la relación que existe entre la velocidad de la luz en el aire y su velocidad en el medio transparente utilizado. De la misma manera, se pueden obtener los índices de refracción de una serie de sustancias que se utilizan tanto en microscopía como en fotografía o en otras actividades en las que se utilizan medios ópticos.

En la tabla 1.1 se muestran los índices de refracción de una serie de sustancias transparentes:
Página siguiente

Tabla 1.1 Índices de refracción

Sustancia	Índice de refracción
Aire	1.0003
Agua	1.3300
Fluorita	1.4340
Glicerina	1.4700
Aceite de inmersión	1.5150
Vidrio	1.5200
Flint	1.6600
Zirconia	1.9200
Diamante	2.4200
Sulfuro de plomo	3.9100

II. El rayo luminoso incide de manera oblicua sobre la superficie, en un ángulo equivalente a 45o grados o menos. En estas condiciones, el rayo luminoso no atraviesa el cuerpo transparente, y “rebota” sobre su superficie, en un ángulo similar al de incidencia. A esta característica se le denomina reflexión de la luz. El esquema representa la trayectoria de tres rayos luminosos que inciden en la superficie de un cuerpo transparente (vidrio). Figura 1.6

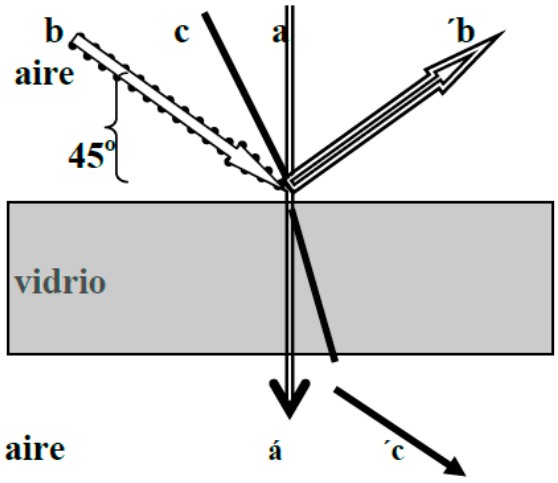


Figura 1.6 Tres rayos luminosos que inciden en la superficie de un cuerpo transparente (vidrio).

III. El rayo luminoso incide de manera oblicua sobre la superficie en ángulos mayores a 45o grados. En este caso el rayo luminoso se desvía en su trayectoria acercándose hacia el rayo que incide de manera perpendicular (rayo “a” o normal) y no se desvía.

Al abandonar el medio transparente y discurrir en el medio de menor densidad, el rayo luminoso vuelve a desviarse (fig. luz.6c), pero ahora alejándose de la normal. A esta característica del rayo luminoso se le denomina refracción[1].

1.3 Óptica

La Óptica ha sido definida, históricamente, como “la ciencia de la luz”. En la actualidad, esta definición se precisa afirmando que la Óptica es la parte de la Física que estudia los fenómenos relacionados con la propagación de la radiación

[1] Montalvo Arenas César Eduardo, Óptica agosto de 2010.

electromagnética en un rango determinado del espectro, denominado rango de frecuencias ópticas.

Este rango, habitualmente descrito en la escala equivalente de longitudes de onda, incluye tres franjas (o, genéricamente, espectros): el ultravioleta (desde 10 nm hasta 390 nm), el visible (desde 390 nm hasta 760 nm) y el infrarrojo (desde 760 nm hasta 1mm). Dentro del espectro visible, conjunto de frecuencias a las que es sensible el sistema visual humano, se denominan colores a ciertas subfranjas particulares:

Rojo: desde 650 nm hasta 760 nm
Naranja: desde 590 nm hasta 650 nm
Amarillo: desde 570 nm hasta 590 nm
Verde: desde 490 nm hasta 570 nm
Azul: desde 420 nm hasta 490 nm
Violeta: desde 390 nm hasta 420 nm

Una posible clasificación de la Óptica define la Óptica Geométrica (OG) como aquella que abarca el estudio de los fenómenos relativos a la propagación de la luz sin incluir los efectos de interferencia ni de difracción, considerando los objetos compuestos por un conjunto de fuentes radiantes puntuales independientes. Esta descripción, basada en el análisis de las trayectorias (rayos) de propagación de la energía, es válida siempre que la longitud de onda de la perturbación que se desplaza sea mucho menor que las dimensiones características de los objetos con los que se encuentra, y justifica la gran aplicabilidad de los formalismos de la OG, Originariamente obtenidos para la luz pero válidos para cualquier perturbación ondulatoria (mecánica o electromagnética) en las condiciones indicadas.

Cuando, en el rango de frecuencias ópticas, es necesario incorporar los citados efectos de interferencia y difracción, surge la Óptica Ondulatoria, y para tener en

cuenta el carácter vectorial transversal del campo electromagnético, se define la Óptica Electromagnética, incluyendo a ambas.

Para describir los fenómenos relacionados con la interacción luz-materia se define la Óptica Cuántica, marco teórico general que, en los límites adecuados, nos permite re obtener los demás formalismos indicados.

1.3.1 Elementos de los sistemas ópticos, criterio de signos

En las condiciones de validez de la Óptica Geométrica, los sistemas ópticos se caracterizan por los siguientes elementos:

- El eje de simetría de un sistema óptico con simetría rotacional se denomina **eje óptico** y es el eje z del sistema de referencia.
- El plano y-z es el **plano meridional** del sistema y es el plano habitualmente utilizado para representar los elementos en el sistema.
- Todas las distancias se miden respecto a un punto/línea/plano de referencia en sentido cartesiano: las **distancias orientadas** sobre/hacia la derecha de la/s referencias son positivas, por debajo/hacia la izquierda son negativas.
- Todos los **ángulos** se miden respecto a una línea/plano de referencia en sentido cartesiano (usando la regla de la mano derecha): los ángulos antihorarios (horarios) son positivos (negativos).
- El **radio de curvatura** de una superficie se define como la distancia orientada desde su vértice hasta su centro de curvatura.
- La luz viaja de izquierda a derecha (de –z hacia +z) en medios con índice de refracción positivo.
- Tras una reflexión, la luz viaja de derecha a izquierda y su velocidad se puede tomar como negativa por lo cual los signos de los índices de refracción se consideran negativos tras una reflexión. Figura 1.7

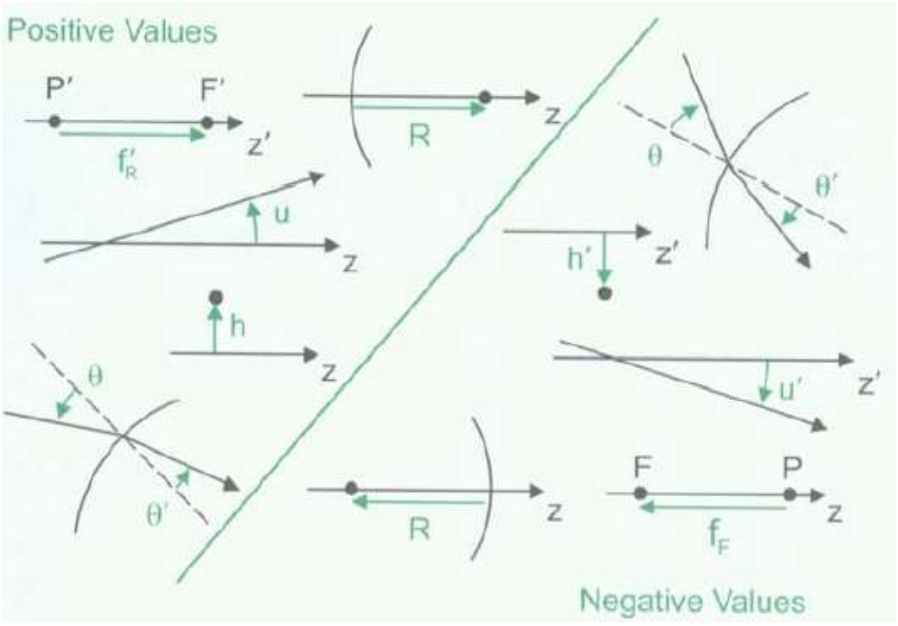


Figura 1.7 Criterios de signos

Dentro de la óptica geométrica, la óptica de primer orden abarca el estudio de los sistemas ópticos ideales (perfect optical systems) que son aquellos sistemas ópticos carentes de aberraciones. Los métodos de análisis incluyen la “Óptica Gausiana” y la “Óptica Paraxial”. Los resultados de estos análisis incluyen las propiedades “de formación de imagen” (imaging properties), es decir, posición y magnificación de la imagen formada por el sistema así como las propiedades radiométricas (non imaging properties) del mismo. Hay sistemas formadores de imagen (imaging systems) y sistemas no formadores de imagen (non imaging systems) Las aberraciones son las desviaciones del comportamiento ideal de los sistemas ópticos, inherentes al diseño de los mismos y existen aun cuando los procesos de producción, fabricación y manufactura sean perfectos (ideales). Estos procesos pueden aportar otras aberraciones añadidas.

La “Óptica de Tercer Orden” (y la “Óptica de Órdenes Superiores”) incluye los efectos de las aberraciones en el comportamiento de los sistemas y permite

evaluar la calidad de los mismos. A veces también incluye los efectos de difracción.

1.3.2 Refracción y reflexión

Ley de Snell de la refracción: Cuando sobre una superficie de discontinuidad, separadora de dos regiones del espacio con índices de refracción n_1 y n_2, incide un rayo luminoso, tiene lugar una transferencia total o parcial de la energía luminosa de un medio al otro en la que los rayos incidente y refractado verifican:

$$n_1 \operatorname{sen}\theta_1 = n_2 \operatorname{sen}\theta_2 \qquad \textbf{Ec. 1.2}$$

Siendo θ_1/ θ_2 los ángulos que forman los rayos incidente/refractado con la normal a la superficie. Asimismo,

- los rayos incidente, refractado y la normal a la superficie son coplanares.
- en la propagación a través de una serie de interfases paralelas, se conserva la cantidad “n senθ”

Ley de la reflexión: En las condiciones de la ley de Snell, si parte (o toda) la energía incidente es reflejada hacia el medio del que procede, los rayos incidente y reflejado verifican

$$\theta 1 = -\theta 2 \qquad \textbf{Ec. 1.3}$$

- Los rayos incidente, reflejado y la normal a la superficie son coplanares.
- La reflexión se interpreta como una refracción con n2 = - n1

En general, desde el punto de vista de la Óptica Geométrica, cuando se produce la incidencia de un rayo luminoso sobre una superficie de discontinuidad, tienen lugar una reflexión y una refracción. La fracción de la energía reflejada depende del coeficiente de reflexión (reflectividad o reflectancia) de la superficie.

La reflectancia (ρ) de una superficie de separación entre dos medios (regiones del espacio) con índices de refracción n1 y n2 está dada por los coeficientes de reflexión de Fresnel, (dependientes, entre otros factores, del ángulo de incidencia y de la absorción). En el caso de incidencia normal, y admitiendo que no haya absorción en la interfase, se tiene que

$$\rho = \left(\frac{n_2 - n_1}{n_2 - n_1} \right)^2 \qquad \textbf{Ec. 1.4}$$

Reflexión total interna (total internal reflection, TIR) ocurre cuando el ángulo de incidencia de un rayo que se propaga desde un medio con un índice de refracción mayor hacia un medio con índice de refracción menor supera el valor del ángulo límite (critical angle, θc)

1.3.3 Espacios Ópticos

Cualquier superficie óptica (superficie de separación o interfase) crea dos espacios ópticos: un espacio objeto y un espacio imagen. Cada espacio óptico se extiende desde -∞ hasta +∞ y tiene asociado un índice de refracción. En general, hay subespacios (segments) reales y virtuales en cada espacio óptico.

Los rayos se trazan desde un espacio óptico a otro. Dentro de cada espacio óptico, los rayos son trayectorias rectilíneas desde -∞ hasta +∞ con segmentos reales y virtuales. Los rayos de espacios adyacentes se encuentran (coinciden) en la superficie óptica común.

Si un sistema tiene N superficies ópticas, entonces tiene N+1 espacios ópticos. Los objetos e imágenes individuales existen en cada espacio. Comúnmente, se combinan múltiplessuperficies ópticas en un único elemento individual y se

consideran únicamente los espacios objeto e imagen del elemento resultante sin tener en cuenta los espacios intermedios, interiores al elemento. El caso más sencillo son las lentes, obtenidas como las regiones del espacio (volúmenes) intersección de superficies (alabeadas) limitantes.

A continuación se describe los puntos la teoría requerida para este trabajo de tesis

1.4 Inseguridad

La inseguridad se entiende como la consecuencia de todo desorden social y económico: es argumento político, ético, económico, moral, y cultural para justificar la intervención de los poderes gubernamentales, mediáticos y financieros, en la esfera del espacio público y de la vida privada. Se tiene actualmente en la sociedad un monstruo llamado inseguridad, que transita entre lo paranoico imaginario y lo fáctico. La inseguridad no es producida necesariamente por la falta de seguridad. La inseguridad es un problema sistémico e integral más que un problema de falta de vigilancia.

La seguridad en nuestros días recae en gran medida en la vigilancia pública, privada y la tele-vigilancia que se realiza tanto en algunos lugares públicos como en forma externa e interna de muchas empresas. En el caso de la vídeo vigilancia esta puede ser llevada a cabo mediante un circuito cerrado de televisión (CCTV), programas de reconocimiento facial, sensores de proximidad, cámaras infrarrojas, cámaras robots, secuenciadores de vídeo, cámaras de intemperie con radiofrecuencia, cámaras de baja iluminación con cobertura de hasta 120 m. en total obscuridad, de interiores visibles u ocultas, cámaras acuáticas, etcétera.

Este tipo de sistemas de seguridad ha sido implementado en cajeros automáticos, transmisiones telemáticas, en tiendas departamentales, centros comerciales y de entretenimiento, bancos, escuelas, cárceles, instituciones públicas y privadas, calles, plazas, carreteras, tráfico vehicular, seguridad infantil, clima, medio

ambiente, hospitales empresas, casas y puede ser implementado en “cualquier espacio que requiera vigilancia”.

Debido al aumento de la inseguridad, la sociedad se ha visto en la necesidad de adquirir servicios que les brinden una mayor protección, y uno de los más requeridos es el sistema a través de cámaras de vídeo que se ha ido desarrollando a pasos agigantados comenzando con los circuitos cerrados de televisión hasta las cámaras IP (Protocolo de Internet) en nuestros días.

Los sistemas de vigilancia por vídeo se están volviendo más comunes en los edificios de oficinas, estructuras externas, escuelas e incluso en las calles. La vigilancia se ha convertido en un componente integral de los métodos de control de acceso enriquecidos con sistemas biométricos y sistemas de rastreo.

En la actualidad han surgido y crecido diversas empresas que se especializan en el monitoreo a través de cámaras a las que se puede acceder desde cualquier parte del mundo. Dichas empresas tienen como propósito principal ofrecer seguridad con facilidad de acceso y manejo sin importar la distancia ni el tiempo.

1.5 Sistemas de seguridad en lugares públicos

Una de las prioridades en los lugares públicos es mantener el orden y la seguridad para el beneficio de la población es por ello que se ha comenzado a implementar equipos de vídeo vigilancia en muchos de estos lugares.

1.5.1 Vídeo vigilancia en el metro del D.F

Hoy en día el metro es uno de los medios de transporte más utilizados, si no el de mayor demanda entre la población capitalina, así como también un lugar con alto índice de delincuencia en sus diversas estaciones de cada línea. Por tal motivo el

gobierno está trabajando en la prevención y control de dicho problema y así proteger a sus usuarios.

En la línea 1, operan 150 cámaras de vigilancia en las estaciones Merced, Candelaria, Pino Suárez, Salto del Agua, Balderas, andenes de Pantitlan y otras funcionando en la línea 1 que a Observatorio[2].

El Sistema de Transporte Colectivo Metro instalará próximamente la infraestructura para colocar 2500 cámaras que integrarán el sistema de vídeo vigilancia en las estaciones de mayor afluencia. Además se tiene el proyecto para la instalación del sistema de fibra óptica para la colocación de las cámaras en el interior de las instalaciones del transporte subterráneo. Para ello se requiere que en varias de las estaciones del metro se realice la instalación del cableado de fibra óptica para colocar el equipo y transportar la imagen. Además de las 150 que ya están instaladas y funcionando en la línea 1 que corre de Pantitlán a Observatorio con lo que sumarán un total de 2650 equipos de video vigilancia. Figura 1.8

Figura 1.8 Vídeo vigilancia en el metro.

El sistema de vídeo vigilancia del Metro estará conectado al centro de mando “C4” de la Secretaría de Seguridad Pública para atender situaciones de emergencia.

[2] http://laprimeraplana.com.mx/2011/10/07/publican-video-con-mujeres-peleando-y-cayendo-a-las-vias-del-metro/ , Pagina recuperada Septiembre 16 2014

Las aspiraciones que se tienen son que las cámaras cuenten con un micrófono para mantener comunicación directa con los usuarios, e incluso, hacerles señalamientos al presentarse alguna situación de peligro para los usuarios o cuando realicen actividades de grafiti, desórdenes y otros.

1.5.2 Guarderías con vigilancia

El ritmo de vida actual es realmente frenético y no deja tiempo a casi nada. Y es muy difícil para los padres cuidar a los hijos, es por ello que una solución a este problema en la actualidad es poder vigilar a sus hijos pequeños a distancia.

Con la tecnología que se ha desarrollado rápidamente en nuestros días los padres pueden ver a sus hijos en las guarderías a través de la vídeo vigilancia en Internet y pueden dejar con más confianza en manos del personal de guarderías y jardines de infancia el cuidado de sus hijos mientras ellos trabajan o están en el hogar y en cualquier momento poder observar a sus hijos desde sus casas o trabajo. Figura 1.9

Figura 1.9 Vigilancia en guarderias

Cuando una guardería o jardín de infancia haya decidido instalar e guarderías, se realizará la instalación de las diferentes cámaras y equipamiento adicional que se utilizará para visionar diferentes partes del edificio:

- Aulas.

- Entrada.
- Jardín.
- Patio de juegos.
- Etc...

Una vez acabada la instalación, los padres que quieran acceder al sistema e-guarderias tendrán que solicitar un nombre de usuario y una contraseña para poder visionar las imágenes que están sirviendo las diferentes cámaras instaladas. El centro solicitará el alta para cada padre al proveedor del servicio e- guarderias y automáticamente se le remitirá un login y una contraseña para que dicho usuario pueda tener acceso al sistema de video vigilancia. Figura 1.10

Figura 1.10 e-guarderias

Una vez que los padres accedan al sistema podrán:
Los padres podrán acceder al sistema mediante un usuario y contraseña. Después podrán ver a su hijo en la guardería a través de internet

- Inspeccionar las instalaciones del centro educativo.
- Observar el comportamiento de sus hijos.
- Conocer el funcionamiento y la metodología de trabajo de la guardería y jardín de infancia.
- Intercambiar información vía e-mail con el centro y con otros padres.

- Comprobar de primera mano el trato que recibe su hijo[3].

1.6 Circuito cerrado de televisión

La sigla CCTV viene del inglés "Closed Circuit Televisión" que traduce circuito cerrado de televisión. El objetivo de este sistema es la supervisión, el control y el eventual registro de la actividad física dentro de un local, predio o ambiente en general. Se denomina circuito cerrado porque, a diferencia de la televisión tradicional, este solo permite un acceso limitado y restringido del contenido de las imágenes a algunos usuarios.

El sistema puede estar compuesto de una o varias cámaras de vigilancia, conectadas a uno o más monitores o televisores, los cuales reproducen las imágenes capturadas, estas imágenes pueden ser, simultáneamente, almacenadas en medios analógicos o digitales, según lo requiera el usuario.

Los componentes de este circuito pueden ser entonces: cámaras, conmutadores matriciales análogos, grabadores digitales (Digital Video Recorder: DVR) o matrices de video (Video Matrix: VMX).

La selección del protocolo de comunicación entre los componentes del CCTV y del medio sobre el cual se transmite debe ajustarse a las necesidades de la aplicación, garantizando así que la inversión se ajuste a lo que en realidad se necesita, es decir, diseñar el sistema acorde a los parámetros de tipo y distancia de la comunicación[4].

Las cámaras de video-vigilancia, por el solo hecho de poder ser vistas por las personas, crean un efecto persuasivo contra robo y vandalismo. En el caso de los robos funciona tanto con los clientes externos, como con los propios empleados,

[3] http://www.e-guarderias.com/funciona.php Página recuperada Septiembre 16 2014
[4] Filipo rugeles, Fundamentos de diseño para un circuito cerrado de televisión Scientia Et Technica, vol. XV, núm. 42, agosto, 2009, pp. 46-547 Universidad Tecnológica de Pereira ,Pereira Colombia

ya que en la mayoría de las ocasiones, las perdidas por robo en los comercios proceden de los propios empleados.

La ventaja de implementar estos sistemas, es que, el propietario o personal autorizado, no necesita estar físicamente en el lugar de monitoreo, cada vez que ocurra algún incidente, se pueden consultar las grabaciones para comprobar lo que ocurrió. Los grabadores digitales suelen ser de 4, 8 ,16 y 32 cámaras, por lo tanto se puede observar en cada pantalla hasta el monitoreo de 32 cámaras.

Para poder llevar a cabo un monitoreo adecuado, es necesario hacer una elección de cámaras correcta bajo las siguientes condiciones: área que se pretende vigilar, ubicación, nivel de seguridad, calidad de imagen requerida, entre otros. Las características dependen de las necesidades del usuario principalmente, siendo la principal necesidad la seguridad de sus bienes y el aviso oportuno en caso de ocurrir algún evento. Más adelante se abordaran estas características a profundidad para poder hacer una correcta selección de equipo y cubrir todas o la mayor parte de las necesidades.

1.7 Diseño de CCTV

El circuito cerrado de televisión (CCTV), es una tecnología de vídeo vigilancia visual diseñada para supervisar las actividades realizadas en distintos ambientes. Los primeros sistemas de CCTV se crearon antes que la misma televisión para el público, la cual tuvo mucho más crecimiento. Tuvo un uso muy especializado debido al precio de las cámaras, el cual limitaba tremendamente las aplicaciones. Con la llegada de los nuevos sistemas de captación de imagen en las cámaras, y el incremento del crimen y la inseguridad, provocaron un crecimiento en la producción y un decremento en los precios.

La televisión comercial que comúnmente se conoce, está abierta al público ya que a través del aire e incluso a través de cables (televisión por cable) se hace llegar a

todo aquel que quiera observar la programación. En el caso del circuito cerrado, el video generado se conserva privado y únicamente son capaces de observarlo las personas asignadas.

En la actualidad los sistemas CCTV están al alcance de cualquier organización, empresa o familia, y sus aplicaciones prácticamente no tienen límite. Al disminuir significativamente su precio las videograbadoras se integraron a los sistemas de, y desplazaron al monitor como parte fundamental de un sistema. Las nuevas videograbadoras digitales compiten en precio con las analógicas, ya que almacenan una gran información para ser analizada posteriormente.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos o computadoras.

Las cámaras pueden estar sostenidas por una persona pero esto puede afectar la calidad del video, normalmente se encuentran fijas en un lugar determinado elegido estratégicamente para no perder detalle de los eventos que sucedan en el área vigilada. En un sistema moderno las cámaras que se utilizan pueden estar controladas remotamente desde una sala de control, donde se puede configurar su panorámica, inclinación y zoom.

El uso más conocido del CCTV está en los sistemas de vigilancia, seguridad y en aplicaciones tales como establecimientos comerciales, bancos, oficinas gubernamentales, edificios públicos, aeropuertos, etc. En realidad, las aplicaciones son casi ilimitadas. Aquí se enlistan algunos ejemplos:

- Vigilancia periférica y perimetral de todo tipo de instalaciones.
- Supervisión de espacios de control de acceso y seguimientos interiores.
- Control del estado de áreas restringidas y zonas internas.

- Protección específica de objetos de valor.
- Detección volumétrica.
- Supervisión y control a distancia de instalaciones.
- Grabación, transmisión y almacenamiento de imágenes y sonido.

En la mayoría de los casos el CCTV tiene que estar acompañado de la grabación de los eventos que se vigila con el objeto de los obtener evidencia de todos movimientos importantes, y además el minimizar la vigilancia humana de los monitores.

El sistema de vigilancia por circuito cerrado de televisión (CCTV) consta de un conjunto de dispositivos que permiten captar y enviar datos (imágenes, sonido) desde la zona vigilada a los lugares donde elija el cliente con el objetivo de controlar y proteger un espacio definido.

Para la instalación de CCTV, con enlaces inalámbricos de un establecimiento hacia otro son necesarios una serie de equipos.

- Medios de captación de imágenes.
- Equipos para la visualización de imágenes.
- Medios de transmisión.
- Equipos para el almacenamiento.
- Equipos de conmutación.
- Medios de control de vídeo.
- Equipos de alarma.

Básicamente, los sistemas de CCTV admiten desde sencillas instalaciones compuestas de cámaras, monitor y video grabadora hasta complejos sistemas integrados por múltiples y avanzados elementos: multiplexores, matrices distribuidas, servidores IP, transmisores y grabadores digitales, dispositivos motorizados, etc.

Entre las aplicaciones más extendidas destacamos el empleo de los sistemas combinados de CCTV e intrusión, que es nuestro caso de interactuar con los dos sistemas para aumentar el nivel de seguridad, adecuando a las instalaciones con la pretensión de obtener imágenes de las zonas donde se produce la intrusión y almacenar las imágenes captadas.

1.8 Elementos que integran un sistema CCTV

- **Cámara.** El punto de generación de video de cualquier sistema de CCTV es la cámara, existen cámaras que incluyen un micrófono para poder tener grabación de audio además de la grabación de video, así como diversos tipos de cámara, cada una para diferentes aplicaciones y con diferentes especificaciones y características, como las mencionadas a continuación:
  - Sistema de lentes, Intervalo de longitud focal, 2,8 - 10 mm
  - Vídeo, Número de líneas de TV 1000
  - Visión nocturna, Distancia de visión nocturna, 30m
  - Diseño, Color blanco/negro y duales (para aplicaciones de día y noche).
  - Código IP (International Protection) IP66
  - Factor de forma, Dome
  - Desempeño, Colocación soportada, Interior, Tipo IP
  - Temperatura de funcionamiento
  - Resistencia a la intemperie.
  - Iluminación (sensibilidad).
  - Condiciones ambientales (temperatura mínima y máxima, humedad, salinidad).
  - Sistema de formato (americano NTSC, europeo PAL).
  - Tensión de alimentación.
  - El más frecuentemente utilizado en el CCTV es el de 1/3", pero existen de ¼" (menores) y también de ½" (mayores). Figura 1.11

Figura 1.11 Cámara CCTV Domo MVA-308M

- **Monitor.** La imagen creada por la cámara necesita ser reproducida para un análisis posterior, ese análisis de imagen se realiza por medio de un monitor de CCTV, el cual es prácticamente el mismo que un receptor de televisión, excepto que el sistema de vigilancia CCTV, no tiene circuito de sintonía, y la durabilidad del monitor de CCTV es más extensa, a comparación de un receptor de televisión. Figura 1.12

  Tamaños de monitor

  - 19 pulgadas
  - 22 pulgadas
  - 25 pulgadas

Figura 1.12 Monitor CCTV

- **Grabadoras de Lapso de Tiempo (VCR).** Las videograbadoras en el circuito cerrado de televisión aparentemente tienen el mismo diseño que un sistema doméstico, con la diferencia de que cuentan con funciones adicionales diseñadas específicamente para el mercado de la seguridad. También funcionan con casetes ordinarios de tipo VHS, lo cual a largo plazo es una gran desventaja, ya que es necesario un espacio adicional para almacenar dichos casetes, los cuales pueden romperse o simplemente dejar de tener un funcionamiento adecuado debido al uso. Figura 1.13

Figura 1.13 Grabadoras de Lapso de Tiempo (VCR).

La utilización de gabinetes industriales diseñados para soportar el uso continuo de la videograbadora, es la característica principal con la cual se diferencian de las demás videograbadoras (hechas para funcionar por 3 ó 4 horas diarias). El principio de la funcionalidad de una VCR para seguridad es que deberá de grabar por lo menos 24 horas, la grabación se hará en forma 'periódica' en lugar de 'continua'.

La videograbadora de seguridad permite seleccionar los intervalos de tiempo en los que se desea grabar, dependiendo de sus requerimientos, lo cual se recomienda ya que en caso de algún evento importante que suceda fuera de los intervalos de tiempo, no se podrá contar con la grabación de dicho evento.

- **Grabación DVR:** Un grabador de vídeo digital (DVR por las siglas en inglés de digital video recorder) es un dispositivo interactivo de grabación de televisión y video en formato digital. Figura 1.14

Figura 1.14 Un grabador de vídeo digital

El DVR se compone, del hardware, que consiste principalmente en un disco duro de gran capacidad, un microprocesador y los buses de comunicación; y del software, que proporciona diversas funcionalidades para el tratamiento de las secuencias de vídeo recibidas, acceso a guías de programación y búsqueda avanzada de contenidos. El DVR surge debido al formato digital de la televisión y permite almacenar la información y manipularla posteriormente con un procesador.

- **Enrutadores (router).** Un router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos. Figura 1.15

Figura 1.15 Router

- El tipo de router a emplear en un sistema de video vigilancia depende de las necesidades del usuario. Existen diversos tipos de routers, por ejemplo:
  - Conectividad Small Office, Home Office (Pequeña casa y oficina) (SOHO)

- Los enrutadores se utilizan con frecuencia en los hogares para conectar a un servicio de banda ancha tales como IP sobre cable o ADSL. Un enrutador usado en una casa puede permitir la conectividad a una empresa, a través de una red privada virtual segura.
- Distribución Los routers de distribución agregan tráfico desde otros routers, ya sea en el mismo lugar, o de la obtención de los flujos de datos procedentes de múltiples sitios a la ubicación de una importante empresa. Los enrutadores de distribución son con frecuencia, responsables de la aplicación de la calidad del servicio a través de una WAN, por lo que deben tener una memoria considerable, múltiples interfaces WAN y transformación sustancial de inteligencia.
- Núcleo. En las empresas, el enrutador puede proporcionar una "columna vertebral" interconectando la distribución de los niveles de los enrutadores de múltiples edificios de un campus, o a las grandes empresas locales. Tienden a ser optimizados para ancho de banda alto, debido a que el manejo de información es muy elevado.

1.9 Video

Existen algunas formas de transportar los datos (video, audio) capturado por las cámaras por un medio de comunicación, hacia los monitores, sistemas de almacenamiento o equipos de tratamiento. Los medios de transmisión podemos clasificarlos por la vía en que se transporta la información:

- Vía cable o cableados: necesitan este soporte para cumplir su misión: par trenzado cable coaxial, fibra óptica.
- Vía radio o inalámbricos: la información de propaga en determinadas frecuencias por el aire en forma de ondas electromagnéticas: microondas, láser, infrarrojos, etc.

Los constantes requerimientos de las necesidades actuales han acelerado la evolución e implantación de los medios de transmisión digitales en remplazo de la

tecnología analógica. Ello está provocando la sustitución de los, ampliamente extendidos, sistemas de cable bifilar o coaxial por tendidos de fibra óptica o enlaces vía radio que permite una mayor capacidad y velocidad en la transmisión de datos, y cada día mientras la tecnología sigue avanzando, se vuelven más accesibles para el usuario final. Sin embargo para el proyecto se utilizó como medio de transmisión físico el cable UTP 6a, el cual nos permite una capacidad de transporte de video en hasta 90 metros, además de permitirnos transportar señales eléctricas de alta frecuencia, este medio.

El sistema de transmisión permite obtener las imágenes u audio en tiempo real, los medios por los cuales se pueden transmitir son:

- Por cable bifilar.
- Par trenzado.
- Por cable coaxial.
- Por fibra óptica.
- Por línea telefónica.
- Transmisión RDSI.
- Enlace por microondas.
- Enlace por radiofrecuencia.
- Transmisión por Internet.
- Transmisión multiplex.
- Enlace por láser e infrarrojo.

En el proyecto a realizar (capitulo 3) se interconecta por medio de los siguientes métodos de propagación

1.9.1 Transmisión por radiofrecuencia

Técnica que se usa para la transmisión a distancia de audio, vídeo y datos mediante ondas electromagnéticas cuya frecuencia está comprendida entre 30 KHz y 300 GHz

Como características principales indicamos:

- El equipo consta de emisor, receptor y repetidores intermedios.
- Tiene elevadas prestaciones y alcance, lo que le convierte en un medio de los más empleados.
- Transmisión inalámbrica, no precisa cables conductores, se propagan por el aire.
- Precisa un modulador de radiofrecuencia en la salida de la cámara y un demodulador RF en la entrada al dispositivo final.
- Es posible la transmisión en tiempo real.
- Permite emitir y recibir señales de vídeo, audio, alarmas y telecontrol. Transmisión bidireccional.
- Las ondas electromagnéticas se propagan por el espacio a la velocidad de la luz, ello implica una alta velocidad de transmisión.
- Para conseguir elevados alcances se precisa, además de repetidores, elevada potencia de salida y receptores muy sensibles. Incluso se emplean satélites de comunicaciones.

1.9.2 Enlace por microondas

Las microondas son ondas (pueden propagarse en el vacío sin necesidad de un soporte material) cuya frecuencia está comprendida entre 2 y 40 GHz. Como podemos deducir se trata de un sistema de transmisión inalámbrica ya que no precisa la instalación de líneas de cableado.

Las características principales son:

- La transmisión se realiza entre un emisor (modulador de microondas) y un receptor (demodulador), ayudados por repetidores intermedios para conseguir mayores alcances.
- Es imprescindible el contacto directo entre el emisor y receptor, pudiendo intercalar muchos repetidores (antenas parabólicas).
- Permite la transmisión en tiempo real.

- Permite transmitir y recibir señales de vídeo, audio, alarmas y telecontrol.
- Sensibilidad a ciertas interferencias y condiciones atmosféricas adversas.
- Alta capacidad de transportar datos.
- Largos alcances sobre el terreno e incluso, con la ayuda de satélites de comunicaciones.

1.9.3 Transmisión por Internet

El diseño de equipos (servidor de vídeo) que utilizan el protocolo TCP/IP se ha generalizado en la fabricación de dispositivos para sistemas de vigilancia por CCTV fundamentalmente por dos motivos:

- Las prestaciones: vídeo, audio y control remoto, incluida la verificación de alarmas, con plenas garantías de fiabilidad.
- La instalación: más económica al disponer de una red de uso público.

La transmisión de imágenes y audio de las distintas cámaras, utilizando el protocolo TCP/IP en redes LAN o WAN, se realiza por medio de RDSI, ADSL, fibra óptica, GSM o módem.

Algunas de las características de estos medios de transmisión son:

- Transmisión de vídeo y audio por red (Internet o Intranet), facilitando la verificación de alarmas, control remoto y la tele vigilancia.
- La transmisión puede llegar a cualquier lugar del mundo a través de la línea RDSI, ADSL, GSM solo con disponer de una ordenador de sobremesa o portátil en red o conectado a Internet, con sus correspondientes contraseñas o password.
- Manejo y configuración por medio del navegador de Internet.
- Software específico para la gestión y tratamiento de imágenes.
- Notificación de las alarmas al titular, a un autorizado o servicios de seguridad, por medio de correo electrónico, teléfono fijo o móvil, etc.

- Control de sensores, relés, alarmas y equipos auxiliares de calefacción, aire acondicionado, etc.
- Grabación digital en disco duro del equipo o VCR, incluidas imágenes previas de alarma.
- Visualización de imágenes en tiempo real o de las almacenadas.
- Utilización de sistemas de compresión de datos: MPEG, JPEG, Wavelet,... que agilizan las transmisiones y reducen los espacios de almacenamiento.
- Empleo de métodos criptográficos que aseguren la confidencialidad de las comunicaciones
- Puertos para conexión de periféricos (módem, adaptador) y enlaces a ordenadores o redes.
- Integración en cualquier sistema existente.

1.9.4 Conexión, cableado estructurado

La conexión del equipo se realizó con cable UTP categoría 6a.Figura 1.16

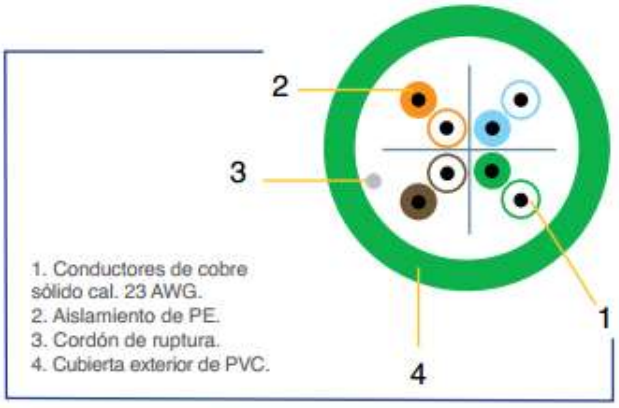


Figura 1.16 Cable UTP categoría 6a.

Es un estándar de cables para Gigabit Ethernet y otros protocolos de redes que es retrocompatible con los estándares de categoría 5/5e y categoría 3. La categoría 6 posee características y especificaciones para evitar la diafonía (o crosstalk) y el ruido.

El estándar de cable se utiliza para 10BASE-T, 100BASE-TX y 1000BASE-TX (Gigabit Ethernet). Alcanza frecuencias de hasta 250 MHz en cada par y una velocidad de 1 Gbps. La conexión de los pines para el conector RJ45 que en principio tiene mejor inmunidad a interferencia arriba de 100Mbps es el T568A. Cable de cuatros pares construido con aletas en la superficie interna de la chaqueta y un aislante en el centro del cable que lo divide en dos sectores el cual mejora el funcionamiento requerido para el uso de banda ancha.

- **Especificaciones**
  - Calibre del conductor: 23 AWG.
  - Tipo de aislamiento: Polietileno.
  - Tipo de ensamble: 4 pares con cruceta central.
  - Tipo de cubierta: PVC
  - Separador de polietileno para asegurar alto
  - desempeño contra diafonía.
  - Para conexiones y aplicaciones IP.
  - Conductor de cobre sólido de 0.57 mm.
  - Diámetro exterior 6.1 mm.
  - Desempeño probado hasta 300 MHz.
  - Impedancia: 100 Ω.
- **Aplicaciones**
  - 1.2 Gbps ATM.
  - 622 Mbps ATM.
  - 100 Base T.
  - 100 Mbps TP-PMD.
  - 100 BASE VG ANYLAN.
  - 1000 Base T.
  - Video digital.
  - Video Banda Base y Banda Ancha.
- **Normas Aplicables**
  - ANSI/TIA/EIA 568B.2-1.

- ANSI/ICEA S-102-700.
- ISO/IEC 11801 (2a edición, clase E).
- NEMA WC66.
- EN 50173-1.
- UL.
- NMX-I-248-NYCE-2005.

1.9.5 Transmisión múltiplex

Sistema de transmisión que permite el envío simultáneo de varias informaciones por un solo canal. La transmisión puede efectuarse de dos formas:

1. - Por división de frecuencia: se procede a asignar una frecuencia portadora diferente para cada una de las informaciones transmitidas.
2. Por división de tiempo: las diferentes informaciones se envían al canal de transmisión común durante intervalos de tiempo distintos.

Esta tecnología, adoptada por sistema de CCTV, permite la transmisión mediante un solo canal de vídeo de las imágenes multiplexadas de varias cámaras y la reconstrucción por separado de cada señal, obteniendo una imagen separada y estable. Sus componentes son:

- El canal de transmisión: puede ser cable coaxial, fibra óptica, enlace a microondas o láser, radio frecuencia...
- El equipo multiplexor: mezcla y ajusta la señal de vídeo de entrada y la codifica para la transmisión.
- El demultiplexor: separa y ajusta la señal multiplexada para enviarla a su salida correspondiente.

1.9.6 Power over Ethernet (Energía eléctrica por Ethernet)

Power over Ethernet (PoE, energía eléctrica por Ethernet, solo para cámaras IP) integra energía eléctrica y datos en una única infraestructura de cableado y elimina la necesidad de disponer de corriente alterna en todos lados.

La energía y los datos se integran en el mismo cable, soportando la categoría 5e/6a hasta 100 metros. Durante fallas de corriente, PoE asegura el funcionamiento continuo de dispositivos conectados de forma remota, como teléfonos IP, puntos de acceso LAN inalámbricos y cámaras de seguridad IP, al ser usados junto con una fuente de alimentación eléctrica ininterrumpida (UPS) centralizada.

En este caso usar POE puede no ser muy recomendable en seguridad electrónica, por varias razones:

- Se limita el funcionamiento, por una distancia máxima que no siempre se cumple.
- La alimentación sale del mismo equipo activo incrementando el riesgo de daño y costo de mantenimiento.

La cámara debe cumplir con el estándar POE y no todas lo hacen. Finalmente es inseguro compartir todo el cableado de datos y comunicaciones con seguridad.

La norma que rige la alimentación remota de dispositivos Ethernet a través de infraestructura LAN, es la norma IEEE 802.3af. Esta norma define las especificaciones de la transferencia de energía eléctrica a través de cables Ethernet y estipula el modo de diseño de equipos de alimentación eléctrica y de terminales alimentadas, también define la transmisión de energía eléctrica por infraestructura de cableado existente, incluyendo la Categoría 5e/6a, cables de interconexión, tableros de conexión y hardware de conexión.

Un sistema PoE se compone de un Equipo de Alimentación Eléctrica (PSE, Power Sourcing Equipment) y de un Dispositivo Alimentado (PD, Powered Device). El equipo de alimentación eléctrica puede ser un End-span (Alimentador desde el extremo), mientras que el dispositivo alimentado es una terminal capacitada para operar con PoE (por ejemplo, un teléfono IP, un punto de acceso LAN inalámbrico, etc.). Figura 1.17

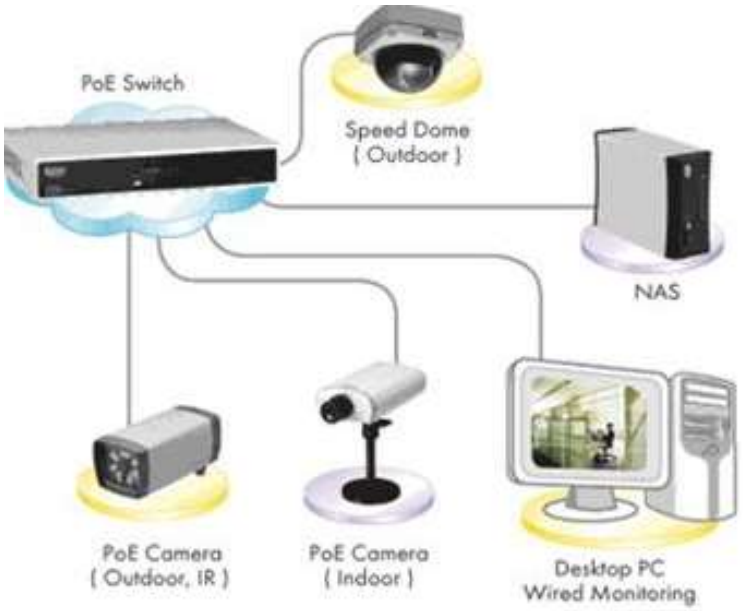


Figura 1.17 Power over Ethernet (PoE)

Principales ventajas del PoE:

- Menor costo: PoE elimina la necesidad de montar cables de datos y cables de energía.
- Más flexible: Los dispositivos de red pueden ser instalados y reubicados, sin la necesidad de tener una toma de corriente CA.
- Más confiable: Una fuente de poder centralizada para todos los dispositivos protegida por una batería en caso de una falla eléctrica.

PoE elimina la necesidad de instalar cargadores y tomas de corriente CA.

- Envío de corriente
- Hasta 15 watts con el estándar IEEE802.3af
- Más de 30 watts con el estándar IEEE802.3at

Productos frecuentes alimentados vía PoE:

- Teléfonos IP
- Access Points Inalámbricos
- Cámaras de Red

Existen dos tipos de productos PoE:

1. **PSE.** Power Sourcing Equipment El Equipo Fuente de Alimentación (PSE) es un dispositivo como un switch, que provee ("fuentes") de alimentación sobre el cable Ethernet (PoE). El máximo permitido por cable bajo la norma IEEE 802.3af es de 15.40W. Una especificación más reciente, IEEE 802.3at, ofrece 25.50 W o más. Cuando el dispositivo es un switch, se le llama un "endspan". En otro caso, si es un dispositivo intermedio entre un Switch sin capacidad Poe y un dispositivo PoE, es llamado "midspan".
2. **Powered device**. Un dispositivo alimentado (PD) es un dispositivo alimentado por un PSE el cual consume energía. Por ejemplo Access Points, Teléfonos IP y Cámaras IP.

   Varios dispositivos alimentados tienen un conector auxiliar de energía para una fuente de energía externa. Dependiendo del diseño del PD, puede ser alimentado por un puerto auxiliar, los puertos auxiliares algunas veces actúan como respaldos de energía en caso de que el cargador PoE falle.

1.10 Selección del CCTV adecuado

Cada sistema de acuerdo con sus espacios y usos debe tener las cámaras aplicables a ese entorno.

El criterio de selección involucra ciertos parámetros a tomar en cuenta tales como: sensibilidad, resolución y capacidad para aislar el ruido en la señal. Figura 1.8

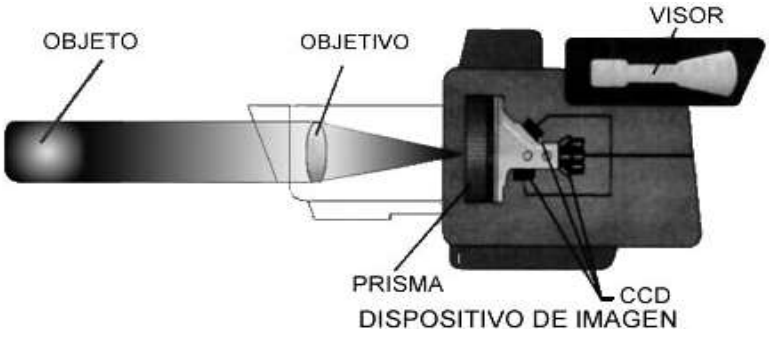


Figura 1.18 Partes de una cámara de video

1.10.1 Sensibilidad

Es la capacidad de captar la luz que refleja un objeto, la sensibilidad de una cámara da una idea de la capacidad de reproducción de imágenes de video en condiciones de baja iluminación. Cuanto mayor es la sensibilidad de la cámara, mayor es la calidad de reproducción en dichas condiciones. La sensibilidad se mide en LUX. A menor cantidad de LUX, mayor sensibilidad posee. Existe una gran ventaja de las cámaras B/N frente a las de color cuando el nivel de iluminación es escaso. Cuando se realiza el diseño de un CCTV, se debe tener en cuenta la luz reflejada por los objetos que componen la escena. Figura 1.19

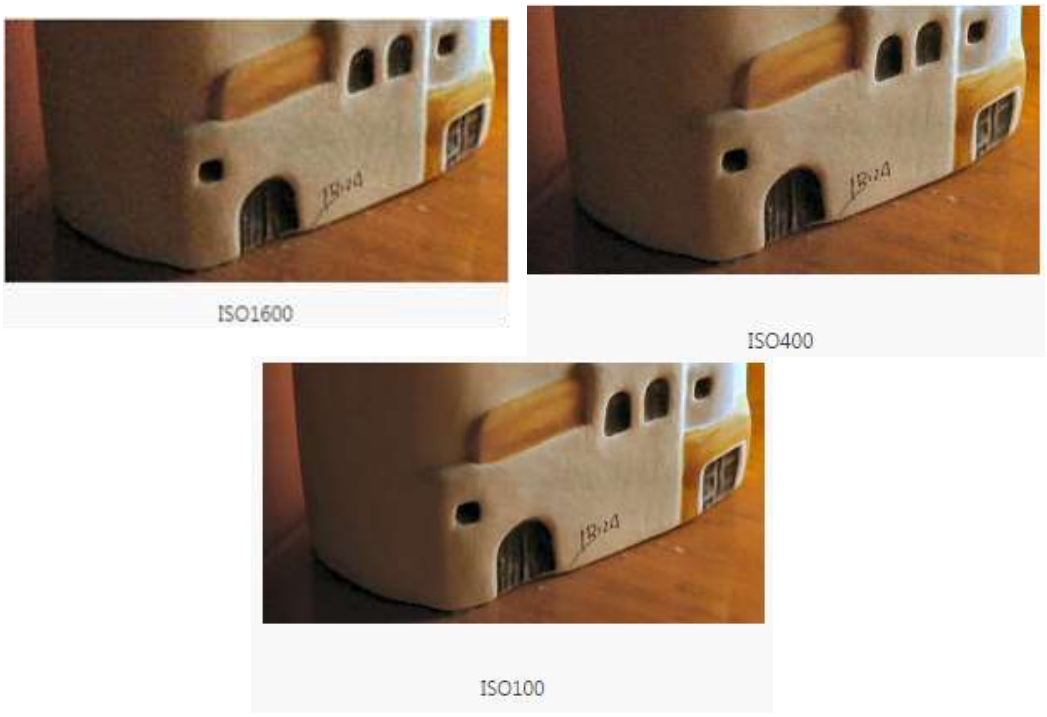


Figura 1.19 a menor sensibilidad mayor calidad de imagen y a mayor sensibilidad peor calidad de imagen.

Cuanto mayor sea la luz reflejada, menor será la iluminación real necesaria de la escena, para obtener una buena calidad de imagen. Esto permite usar en los sistemas profesionales cámaras más económicas cuando la escena está bien iluminada.

1.10.2 Resolución

Una medida de la habilidad de una cámara o sistema de televisión para reproducir el detalle de la imagen con fidelidad. La resolución en líneas horizontales de TV es el número de transiciones blanco/negro que pueden ser resueltas a través de la imagen. Es una función del número de pixeles que puede manejar un sensor de imagen (CCD) y el ancho de banda de circuito de la cámara. Típicamente la resolución de las cámaras es 350 TV líneas, aun cuando hay cámaras de alta resolución con 450 TV líneas.

Existen cámaras de color que en cambio de sobreponer la señal de crominancia en la de luminancia, las suministra en líneas separadas. Es conocido como separación Y/C y requiere dos cables coaxiales desde la cámara para llevar las señales separadamente. Esta técnica incrementa el ancho de banda y por tanto la resolución. Además de la sensibilidad y la resolución, también es necesario tomar en cuenta ciertos aspectos, tales como:

- Tipo
- Ubicación
- Formato
- Iris
- Compensación de contraluz
- Rango Dinámico Extendido
- Montura
- Lente
- Velocidad de Obturación

El tipo de cámara puede ser monocromática, a color y día/noche (combinación de color y monocromática), además según el área a cubrir puede ser fija o PTZ (Pan, Tilt, Zoom), para nuestro proyecto se escogió, que las cámaras sean a color día/noche y fijas, ya que no existe una persona que las controle, además que se requiere de mucho más presupuesto, y para la aplicación son suficientes.

La ubicación es un factor que depende mucho también, se debe ver si es para exteriores o interiores, si corre riesgo de vandalismo, o si requiere de soportes o accesorios adicionales para su montaje; Para los interiores de los centros ferreteros en su mayoría fueron cámaras tipo domo para interiores, y para los exteriores cámaras tipo bala o bullet, equipadas con empaques y con una carcasa metálica para este ambiente.

Las Dimensiones del sensor que garantiza una baja o alta resolución, esto es manejado por un chip CCD o CMOS, el CCD "Charged-Couple Device" Consiste de varios cientos de miles de elementos de cuadro (pixeles) en un pequeño chip de 1/2", 1/3", o 1/4". Cada uno responde a la luz incidente almacenando una carga proporcional. Se arreglan en una malla precisa con registros de transferencia verticales y horizontales (dirección) que llevan la señal de cada punto al video procesador. Esta transferencia ocurre 60 veces por segundo.

El microprocesador es un elemento sensible a la luz que convierte una imagen en un flujo eléctrico. Inventado en los 70´s los CCDs inicialmente se emplearon como memorias. También se emplean en telecine, fax, scanners, etc. No son susceptibles de imágenes manchadas o con retardos y hacen posible las cámaras livianas.

El chip de 1/3" CCD es el formato más empleado, su tamaño es 5.5mm (diagonal), 4.4mm (horizontal) y 3.3mm (vertical). El chip de 1/4" es más empleado últimamente en cámaras de color 4mm (diagonal), 3.2mm (horizontal) y 2.4mm (vertical), su gran ventaja es que su fabricación es posible en cualquier planta de fabricación de memorias, microprocesadores y demás controladores sin apenas realizar cambios en la cadena de montaje, lo que repercute en un menor costo.

Estos dispositivos se caracterizan ante todo porque cada fotodiodo integrado en el sensor lleva consigo la electrónica necesaria para convertir la carga de electrones generada en voltaje, así como un registro individual de este voltaje. Esto afirma

que la superficie necesaria para captar la luz a un mismo tamaño de celda, es menor que en un CCD, pero tiene la gran ventaja de poder acceder a la información captada no solo en la totalidad del dispositivo sino también a una zona particular de éste.

El chip sensor CMOS no sólo integra los fotodiodos sino que también integra toda la electrónica necesaria para el control y lectura de estos, así como el conversor analógico-digital, lo que se traduce en un menor tamaño de los circuitos necesarios para la captura de imágenes.

1.10.3 Formato

Los avances tecnológicos han logrado la disminución de las dimensiones del formato de los sensores de CCD.

Para las instalaciones de cámaras, una consideración fundamental es garantizar que el formato de las lentes acopladas a las cámaras sea igual o mayor que el diseño del formato de la cámara. Si sucediera lo contrario, la imagen de video en pantalla del monitor saldría sombreada situación que se la conoce como (visión de túnel).

Tabla 1.2 Relación entre formato y milímetros de resolución

Formato		Milímetros
1"	=	12.8 H / 9.6 V
2/3"	=	9.6 H / 7.2 V
1/2"	=	6.4 H / 4.8 V
1/3"	=	4.8 H / 3.6 V
1/4"	=	3.2 H / 2.4 V

A continuación se muestra en la figura 1.20

Figura 1.20 Relación entre formato y milímetros de resolución

- **Iris** Abertura de lente ajustable que regula la cantidad de luz que entra en la cámara está directamente relacionada con el focus.
- **Focus** La zona al frente y atrás del objeto en la cual el enfoque permanece. Cualquier cosa dentro de esta área aparecerá claramente definida. La profundidad de campo tiene las siguientes características:
  - Números grandes de Focus dan gran profundidad de campo. Entre más pequeño es el iris mayor es la profundidad.
  - Distancias focales cortas dan grandes profundidades de campo.
  - Distancias grandes al objeto dan grandes profundidades de campo.
  - La profundidad de campo es mayor detrás que delante del sujeto.

- **Compensación de contraluz (Backlight).** Se utiliza para ayudar a corregir los tiempos cuando la luz detrás de un objeto que está intentando ver es mucho más brillante que la del objeto mismo. Mediante el uso de BLC el brillo de la luz se reduce hasta que el sujeto aparezca más brillante y crear una mejor imagen detallada de la materia. Otra solución para las cámaras de puertas y de entradas, es instalar cámaras que tienen un amplio rango dinámico (WDR).

1.10.4 WDR

La FUNCIÓN WDR (Wide dynamic Range) (Rango Dinámico Extendido) evita el problema que tienen las cámaras con los contrastes de luz extremos, que pueden presentarse por deslumbramientos, luz directa del sol o sombras, el captador de imagen está basado en píxeles, digitalizan la luz en el punto de captura, produciendo imágenes muy claras bajo cualquier tipo de iluminación. Básicamente es la fusión de varias imágenes tomadas en diferentes espectros de frecuencia. Este trata de recrear todos los elementos que el ojo humano puede ver simultáneamente.

- **Montura** Los lentes para cámaras de CCTV poseen montura a rosca y existen dos tipos:
  1. montura “C” y
  2. montura “CS”.
     - Los de montura “C” son los antiguos lentes usados en cámaras de 2/3”de tubo y tienen un foco trasero a 17,5mm del último lente.
     - Los de montura “CS” son los modernos lentes que se usan cámaras de 1/2”, 1/3” y 1/4”CCD y tienen un foco trasero a 12,5mm del último lente.

       Los lentes de montura “C” se pueden usar en cámaras CCD con montura “CS” mediante un anillo adaptador. Los lentes de montura “CS” no se pueden usar en cámaras de montura “C”.

En general, los lentes se fabrican para adaptarse a cada medida de sensor de cámara, pero como regla se utiliza lo siguiente:” el de mayor cobertura sirve para el de menor cobertura, pero no al revés”. Esto significa que el lente para 2/3” sirve para el de 1/2” y para el de 1/3” y para el de 1/4”; el de 1/2” sirve para 1/3” y 1/4” y así sucesivamente. Pero el lente para 1/3” no sirve para 1/2” ni para 2/3”. Existen otros tipos de lentes que vienen construidos con la placa de cámara, que también tienen una rosca más pequeña en diámetro que las de montura ”C” o “CS”, estos lentes no son

intercambiables y se los denomina OEM pues sólo sirven para dichas cámaras.

1.10.5 Lente

Son los encargados de enfocar la escena sobre el sensor CCD de la cámara. Se dividen primariamente en lentes normales, gran angular y teleobjetivo o simplemente tele. Figura 1.21

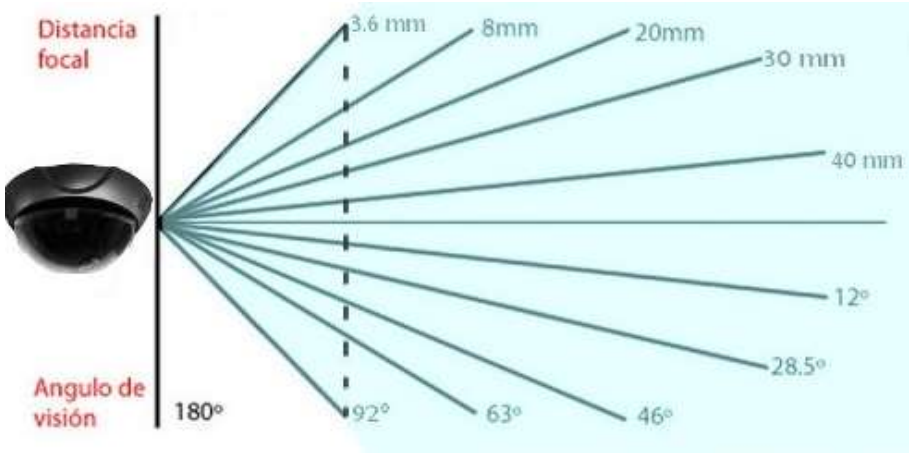


Figura 1.21 Lente de CCTV.

Los lentes normales o de ángulo normal, toman o ven casi igual que el ojo humano, un ángulo de 33/39º (sexagesimales). Los lentes tele o de ángulo estrecho, toman o ven menos que el ojo humano, un ángulo de 30/1º o menos según el tipo. Secundariamente todos los lentes se dividen en: con iris fijo, sin iris, con iris manual o con auto-iris.

Los de iris fijo o sin iris no poseen ajuste para regular el pasaje de la luz a través de sí mismo (el iris es el elemento que al abrirse o cerrarse regula el paso de la luz). Los de iris manual poseen un ajuste que permite variar el paso de la luz a

través del lente. Los de auto-iris poseen un motor que regula el pasaje de la luz en forma automática.

Existen dos tipos de auto-iris: los pasivos (CC) y los activos (Video). Los auto-iris pasivos, tienen el motor pero no la electrónica de comando en el interior del lente. Es la cámara la que debe tener el control electrónico incluido para el comando. También se los denomina CC-Iris. Los auto-iris activos tienen motor y la electrónica de control incluida en el interior del lente. La cámara entrega alimentación en CC y la señal de video. También se los denomina Video-Iris.

Existen también lentes especiales, como son: ultra luminoso, pin hole y zoom. Los lentes ultra luminosos son dispositivos de gran apertura relativa y se utilizan en cámaras ultrasensibles para obtener el máximo rendimiento en horas nocturnas y diurnas. Sólo se disponen como auto-iris activo.

Los lentes pin-hole son dispositivos que tienen un frente de muy pequeño diámetro, sólo 1,5/2mm, lo cual los convierte en espías a través de paredes, bolsos, puertas, etc.

Se disponen con iris manual o auto-iris activo o pasivo. Los lentes zoom son dispositivos de distancia focal variable, es decir, se comportan como varios lentes juntos. Pueden disponerse de varias multiplicaciones: 6x, 10x, 15x, 20x y 30x; es decir, entre la mínima y la máxima distancia focal: 6x-8-48mm; 10x-7,5-75mm; 15x-8-120mm; 20x-12-240mm; 30x-12-360mm.

Todos los lentes a usados en los CCTV deben ser de vidrio óptico para asegurar una correcta visión de la escena a tomar y tener larga vida. Existen algunas cámaras económicas que poseen lentes de plástico, lo cual no asegura una correcta visión y tienen poca durabilidad. Figura 1.22

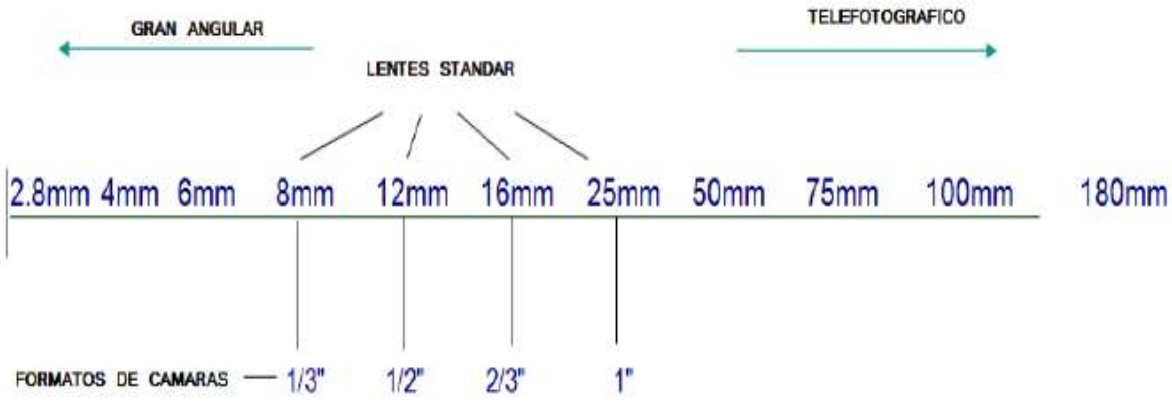


Figura 1.22 Clasificación de los lentes

1.10.6 Sensor de imagen CCD

El sensor CCD (Charge Coupled Device), dispositivo de carga acoplada. Este sensor es uno de los más comunes y más utilizados en la imagen digital. Proporciona buena calidad de imagen, pero por otro lado su fabricación es muy compleja y costosa, por lo que lo fabrican pocas empresas. Las cámaras digitales que llevan incorporado esta clase de sensor, tienen un coste compra elevado. Esta clase de sensor consume mucha energía. Figura 1.23

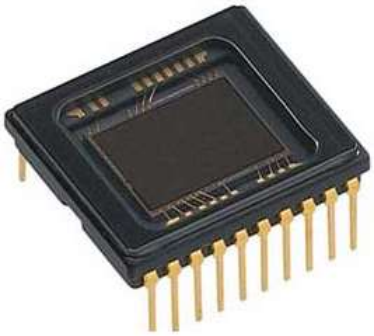


Figura 1.23 Sensor CCD

El funcionamiento del sensor CCD, necesita de un xip externo denominado Analog Digital Converter o ADC, que es el que se encarga de convertir los datos de cada

píxel en datos digitales binarios, para que nuestra computadora (ordenador) los pueda leer. Los potenciales eléctricos obtenidos mediante el CCD se disponen en forma de líneas que posteriormente formarán la imagen en la pantalla. Los mismos potenciales eléctricos pueden ser transformados en señales digitales que podrán ser usadas por el ordenador para su transformación en imágenes. Para digitalizar la imagen habrá que traducir estas señales analógicas en señales digitales (numéricas) por medio de una tarjeta digitalizadora, función que cumple el DVR.

1.10.7 Estructura CCD, trasferencia de cuadros (Frames)

En este tipo de estructura el chip de silicio en el que se encuentran los elementos CCD se divide en dos áreas.

En la mitad superior del dispositivo se encuentra la sección en la que va a incidir la luminosidad de la imagen que se desea captar, denominada área de captación, mientras que en la mitad inferior, se encuentra el área de almacenamiento de cargas y el registro de salida, que es donde pasará la información de la imagen adquirida. Mediante esta configuración se obtiene un mayor factor de relleno. Durante el período de borrado vertical, las cargas generadas en el área de captación son transferidas rápidamente al área de almacenamiento, de forma que cuando comience la captura del siguiente campo los foto sensores se encuentren totalmente descargados para no contaminar la imagen siguiente.

Si durante el proceso de transferencia de cargas los sensores se vieran expuestos a la luz, una carga adicional se sumaría a las que se están enviando hacia el área de almacenamiento, con lo que se contaminaría la imagen.

La única forma de prevenir que esto ocurra, es utilizando un obturador mecánico que proteja de la luz a la matriz de elementos CCD durante el proceso de transferencia.

El inconveniente que presenta este tipo de sensores, es una velocidad de obturación baja, y un coste más alto, al tener que ser el sensor más grande. Figura 1.24

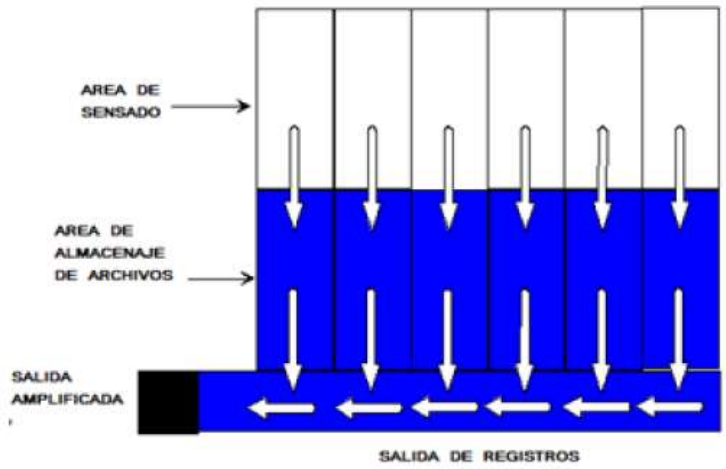


Figura 1.24 Sistema de Transferencia de frames.

- **Transferencia entre líneas** Este tipo de estructura incorpora características de las dos anteriores. La parte superior de la estructura es exactamente igual a su correspondiente en la transferencia interlinea. Las cargas se mueven horizontalmente desde los elementos foto sensores hacia el registro de desplazamiento vertical. Una vez que las cargas están en este registro, en lugar de ser leídas fila a fila, son enviadas al array[5] de almacenamiento, y es desde este array, desde donde las cargas pasan fila a fila al registro de salida.

[5] Un array es un medio de guardar un conjunto de objetos de la misma clase. Se accede a cada elemento individual del array mediante un número entero denominado índice. 0 es el índice del primer elemento y n-1 es el índice del último elemento, siendo n, la dimensión del array. Los arrays son objetos en Java y como tales vamos a ver los pasos que hemos de seguir para usarlos. http://www.sc.ehu.es/sbweb/fisica/cursoJava/fundamentos/clases1/arays.htm Página recuperada Septiembre 16 2014

La diferencia con el tipo anterior se encuentra en que en esta zona de almacenamiento los “paquetes de información” no corren ningún peligro de ser contaminados por excesos de carga que hayan penetrado en el registro de desplazamiento vertical, ya que permanecen en éste durante un período de tiempo muy pequeño. Este tipo de estructura ofrece las mejores prestaciones de los CCDs actuales. Sin embargo, su estructura es compleja y requieren un área total mayor, debido a que tiene la zona de almacenamiento separada. Figura 1.25

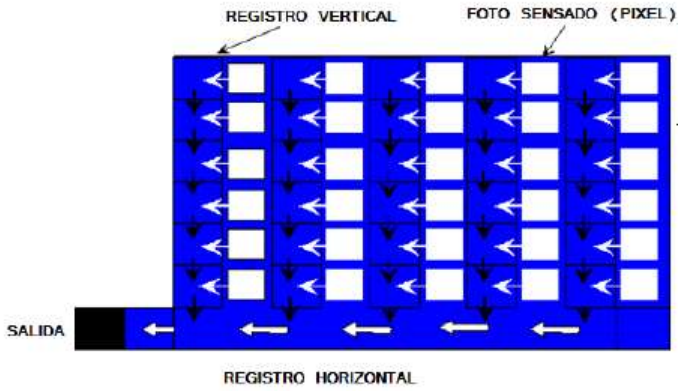


Figura 1.25 Sistema de transferencia entre líneas.

- **Velocidad de obturación** Las cámaras básicas muestran u “observan” una imagen a una tasa de 60 veces por segundo (la velocidad de un obturador de 1/60). La tecnología de procesamiento de señal digital en la cámara ha sido mejorada. Por tanto, este circuito puede analizar la señal de video y si es necesario cambiar la frecuencia de muestreo de la imagen a hasta 100.000 veces por segundo.

  Esto permite que las imágenes más oscuras puedan ser sometidas a una mayor cantidad de muestreos “digitales”, utilicen la luz existente y produzcan así mejores imágenes.

Tabla 1.3 Relación entre distancia focal y velocidad de obturación

Distancia Focal de la Lente	Velocidad de Obturación Mínima
20 mm , 24 mm , 28mm, 35 mm	1/30 seg
50 mm, 80 mm	1/60 seg
105 mm, 135 mm	1/125 seg
200 mm, 300 mm	1/250 seg
500 mm	1/500 seg

1.11 Ancho de banda

El ancho de banda es la velocidad de transmisión simultánea que un medio de comunicación puede transmitir. Esta dado numéricamente y sus unidades son los bits por segundo (bps), ya que se mide la cantidad de bits se pueden transmitir durante un segundo.

La ecuación, se emplea para calcular el consumo de ancho de banda:

AB=Tamaño de la Imagen x Cuadros por Segundo x Canales **Ec. 1.1**

Una cámara PAL en tiempo real (30cuadros por segundo) a compresión normal y tamaño normal consume:

8 kb x 30 Fps x 1 = 240 kbps.

Como se puede observar en el resultado del ejemplo anterior, el ancho de banda requerido, después de la compresión de video hecha por la cámara, no es un valor muy elevado, por lo cual, se llevaría a cabo una buena transmisión y almacenamiento de video, sin interferir en el desempeño de otros equipos conectados a la misma red.

Dentro de una cámara IP, la señal digital y comprimida es entregada a través de una tarjeta de red de tipo Ethernet estándar existente en la gran mayoría de redes actuales. Finalmente la información es ordenada siguiendo protocolos de transmisión conocidos y usados en las redes de cómputo. Por lo tanto es deseable que la cámara maneje múltiples protocolos, de comunicación.

Hoy en día a diversas cámaras se les pueden realizar ajustes a través del mismo conector usando la red como medio de transmisión. De no ser así, las cámaras poseen un puerto adicional de comunicaciones (RS232, RS485, LAN) mediante el cual se cambian los parámetros, por los adecuados para un correcto funcionamiento, según las exigencias del medio y del usuario.

1.12 Longitud focal del lente

La distancia focal combinada con el tamaño del sensor es el ángulo de visión. Una distancia focal pequeña dará una visión de gran ángulo y una distancia focal grande dará una visión estrecha de teleobjetivo. Los objetivos con un gran ángulo, tienen una profundidad de campo mejor.

Esto significa que se puede enfocar de cerca a las cámaras, así como a distancia. Figura 1.26

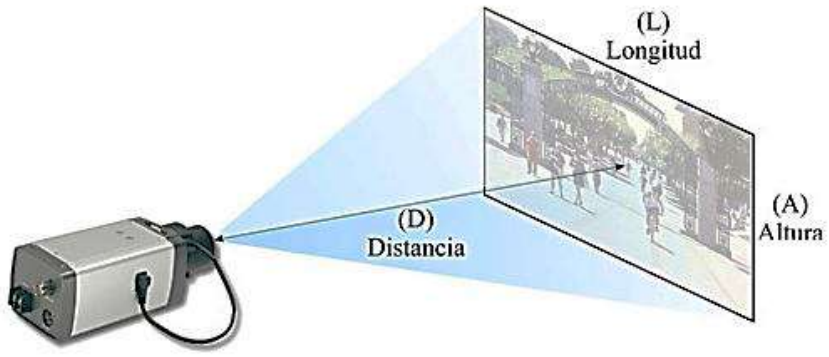


Figura 1.26 Datos a considerar para determinar la longitud focal del lente.

Los datos que se muestran en la figura anterior, son necesarios en caso de no conocer el valor del sensor de la cámara. Los objetivos a vigilar, requieren un ajuste de enfoque preciso, esto es posible por medio de la siguiente ecuación 1.2

$$f = (h \times D) / H \qquad \text{Ec. 1.2}$$

f = Distancia focal, [m].
D = Distancia, [m].
H = Distancia a la que se observa el objetivo, [m].
h = Valor del sensor de imagen, [m].

Los datos que se muestran a continuación, son datos del sensor de imagen y su correspondiente valor en “h”, dicho sensor permite tener un área de grabado más amplia o más reducida, a una distancia mínima del objeto que se desea monitorear, dichos valores son necesarios para emplearlos en la ecuación anterior.

1 / 4 "sensor: h = 3.6mm
1 / 3 "Sensor: h = 4.8 mm
1 / 2 "del sensor: h = 6.4 mm

Con las cámaras IP, la calidad del video digital que se muestra en la sala de control depende del sensor de la cámara, la tecnología de compresión y el software que gestiona el sistema de video IP. Con la ayuda de un buen software de control para el monitoreo y control de las cámaras, la funcionalidad de grabado se potencializa, dándole al software la posibilidad de incrementar sus aplicaciones. Dichas aplicaciones de software posibilitan el control, administración y visionado, tanto de las grabaciones en directo como del video grabado a través de la red IP.

El poder del circuito cerrado de TV IP no se encuentra en la cámara sino en el software de gestión, que ofrece una aplicación útil al usuario final. Por lo tanto, el

rendimiento general depende fundamentalmente de la interacción del software con la cámara IP, el hardware de grabación y la red.

Capítulo 2
Componentes del circuito cerrado de televisión (CCTV)

Cuando nos referimos a la parte de infraestructura de una red de datos, ya sea una red doméstica o una red empresarial, se hace mención a los diferentes elementos que lo conforman, tanto en la parte física (dispositivos de Hardware y tipo de cableado) como en la parte lógica (Software, protocolos, programación, etc.), todos estos elementos en conjunto son necesarios para así, tratar de brindar todas las particularidades que tiene una red.

Aunque hay muchos tipos de redes locales, entre ellas hay unas características comunes, destacando algunas de estas particularidades tenemos:

- La capacidad de conectividad,
- Capacidad de conmutación,
- Capacidad de enrutamiento,
- Seguridad de la red, y
- Control de acceso.

2.1 Infraestructura

Para diferenciar a groso modo los elementos de una red tenemos:

2.1.1 La infraestructura física de la red

Se refiere al diseño físico de la red junto con los dispositivos físicos o de hardware que serán implementados. En cuanto a las conexiones físicas de las redes, tenemos algunas configuraciones para realizar dichas conexiones entre ordenadores, a continuación presentaremos las más comunes:

- Conexión de Red en Bus,
- Conexión de Red en Anillo,

- Conexión de Red en Estrella,
- Y se puede realizar una Conexión Híbridas (una combinación de las conexiones
- anteriores).

Entre los elementos de la infraestructura física para una red de datos tenemos elementos tales como: Ruteadores (Routers), Concentradores (Hubs), Switch, Gateways (Puertos), Cortafuegos (Firewall), estos elementos necesitan de una conexión física, para ello tenemos el cableado estructurado, el cual nos ayudará para la interconexión de estos dispositivos, esta conexión física puede ser por medio de: Cable Coaxial, Par Trenzado ó Fibra Óptica, de las cuales, la más común es el par trenzado de cobre, pero en la actualidad contamos con elementos híbridos, capaces de trabajar con puertos para fibra óptica y par trenzado de cobre a la vez.

Actualmente se dispone de dispositivos para redes inalámbricas, y pueden alcanzar velocidades de transmisión igual que las redes con par trenzado de cobre, tales como:
Access Point (Punto de Acceso) y Ruteadores Inalámbricos (Routers Wireless) entre los más comunes.

A continuación se muestra en la figura 2 .1, como sería la parte física de una red de datos.

Figura 2.1 Red de datos.

2.1.2 infraestructura lógica de la red

Este grupo se compone de todos los componentes de software, parte de la red que no es visible ni tangible para el cliente, pero es de gran importancia para la funcionalidad de la red, es necesario para permitir la conectividad entre los dispositivos físicos mencionados en la infraestructura física, la parte lógica de una red nos permite proporcionar la seguridad y fiabilidad para comunicar a los clientes de la red. Aquí se define cómo los datos van a circular a través de la red, esto se logra definiendo rutas para que la información de los ordenadores se comuniquen de forma rápida y eficiente. La lógica de la red de infraestructura se compone de productos de software, bases de datos para el almacenamiento de datos, los protocolos para los diferentes dispositivos de la red, aplicaciones, enlaces a Internet o a otras redes, seguridad para la detección y prevención de intrusos (hackers) e incluso control parental para los ordenadores, sistemas cortafuegos (firewalls) y es importante incluir un sistema de acceso para realizar copias de seguridad de los datos almacenados. Figura 2.2

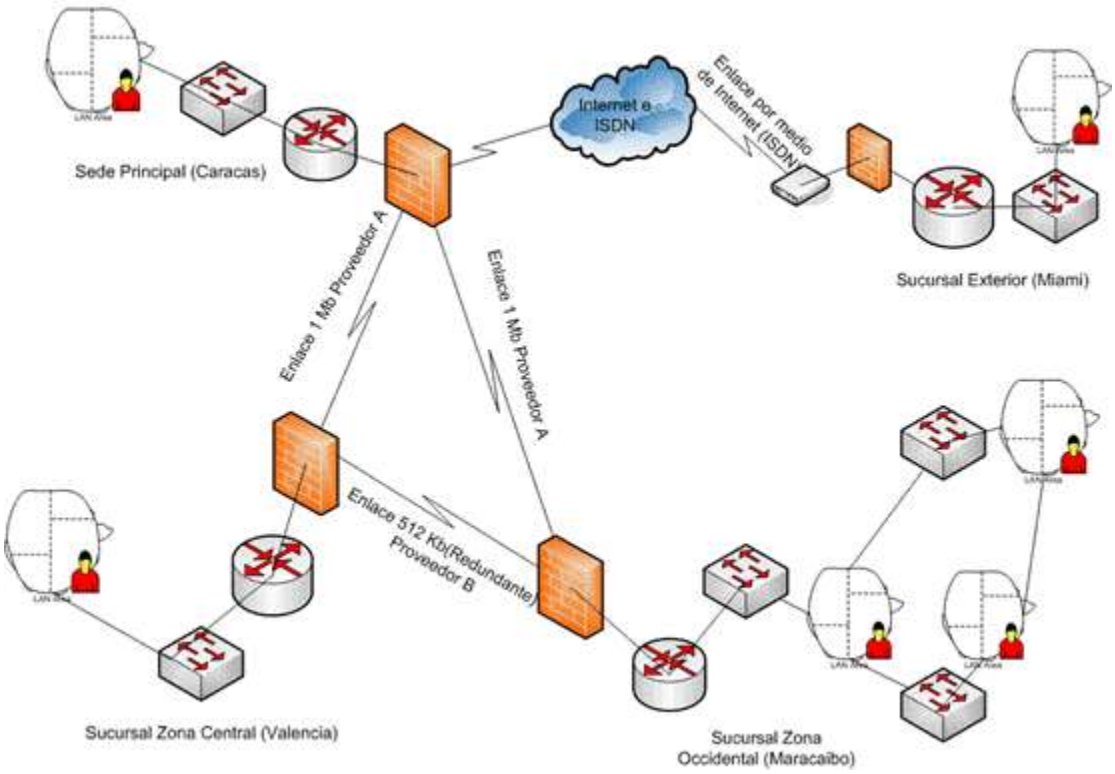


Figura 2.2 Ejemplo una infraestructura lógica.

Y todo este conjunto debe estar albergado en un espacio físico debidamente distribuido (según los requerimientos del cliente) y debe contar con un sistema de seguridad. Es necesario que esté en un ambiente adecuado, para que el conjunto trabaje en condiciones normales (temperatura, humedad, etc.) y estén seguramente cuidados y vigilados (seguridad de acceso restringido, sistema de intrusión, sistema CCTV, sistema contra incendios, etc.), ya que la infraestructura de una red de datos, es la columna vertebral de las comunicaciones, ya sea de una red en el domicilio, en una empresa y/o institución.

Cabe recalcar que para el sistema contra incendio es necesario informarse sobre qué tipo agente extintor utilizaremos para el caso de fuego en nuestros sistemas de servidores, actualmente se utilizan agentes halogenados para evitar el cambio brusco de temperatura, efecto que ocurre con extintores de dióxido carbono.

Otro factor que debemos mencionar, es que el sistema debe estar debidamente apoyado en un Sistema de Alimentación Ininterrumpida “SAI” (ó sistemas UPS en inglés Uninterruptible Power Supply), para las estaciones de trabajo y ordenadores, según los requerimientos de potencia eléctrica del conjunto, estos sistemas pueden ir desde un UPS básico para reserva y protección de equipos domésticos hasta los poderosos Smart UPS (Sistemas de alimentación ininterrumpida inteligentes) que tienen como característica principal su gran capacidad de protección de energía redundante de alto rendimiento con potencia y autonomía escalables para servidores, y para las redes de voz y/o datos. Todos estos sistemas cuentan con un conjunto de baterías y estabilizadores de voltaje para brindar la máxima protección eléctrica al sistema.

2.1.3 Instalaciones de casa habitación

Al referirnos a la instalación de entrada o acometida para una edificación, es necesario dar a conocer que existen algunos tipos de acometidas, tales como:

- **Acometida eléctrica**

  Se entiende por acometida, la parte de la instalación eléctrica que se construye desde las redes públicas de distribución hasta las instalaciones del usuario, y está conformada por los siguientes componentes, Figura 2.3

  - Punto de alimentación.
  - Conductores.
  - Ductos.
  - Tablero general de acometidas.
  - Interruptor general.
  - Armario de medidor.

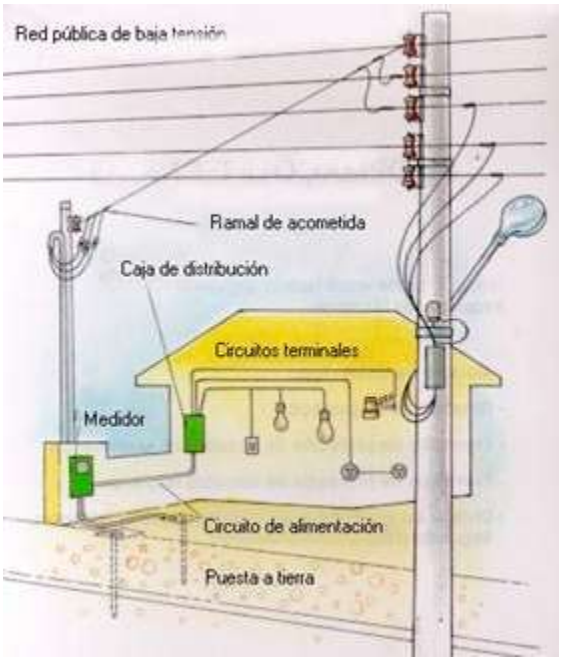


Figura 2.3 Acometida eléctrica.

- **Recomendaciones generales.**

  - Los conductores de la acometida deberán ser continuos, desde el punto de conexión de la red hasta los bornes de la entrada del equipo de medida.

- No se aceptarán empalmes, ni derivaciones, en ningún tramo de la acometida. En la caja o armario de medidores deberá reservarse en su extremo una longitud del conductor de la acometida suficiente que permita una fácil conexión al equipo de medida.

- Tipos de acometida Aéreas: Desde redes aéreas de baja tensión la acometida podrá ser aérea para cargas instaladas iguales o menores a 35 kW.
- Subterráneas: Desde redes subterráneas de baja tensión, la acometida siempre será subterránea. Para cargas mayores a 35 Kw y menores a 225 kW desde redes aéreas, la acometida siempre será subterránea.
- Especiales: Se consideran especiales las acometidas a servicios temporales y provisionales de obra. Deberá constar como mínimo de los siguiente elementos:
  - Conductor de las acometidas
  - Caja para instalar medidores o equipo de medición.
  - Tubería metálica para la acometida y caja de interruptores automáticos de protecciones.
  - Línea y electrodo de puesta a tierra.
- **Acometida telefónica**

  La red de Planta externa es la infraestructura construida en el medio externo de una red, está constituida por todos los elementos asociados a brindar un servicio, incluye el MDF (MDF: main distribution frame), cables, canalizaciones y ductos, armarios, cajas terminales, cables de línea y otras infraestructuras adicionales que se emplean para permitir la comunicación al lugar deseado.
- **Servicios que soporta la red de cobre**

  a) Telefonía:
    - Comunicación a través de señales de voz entre dos personas distantes.

- Es el servicio más antiguo y representativo que brinda una red, el tipo de señal es analógico y su
- Ancho de Banda es de 4 Khz. Figura 2.4

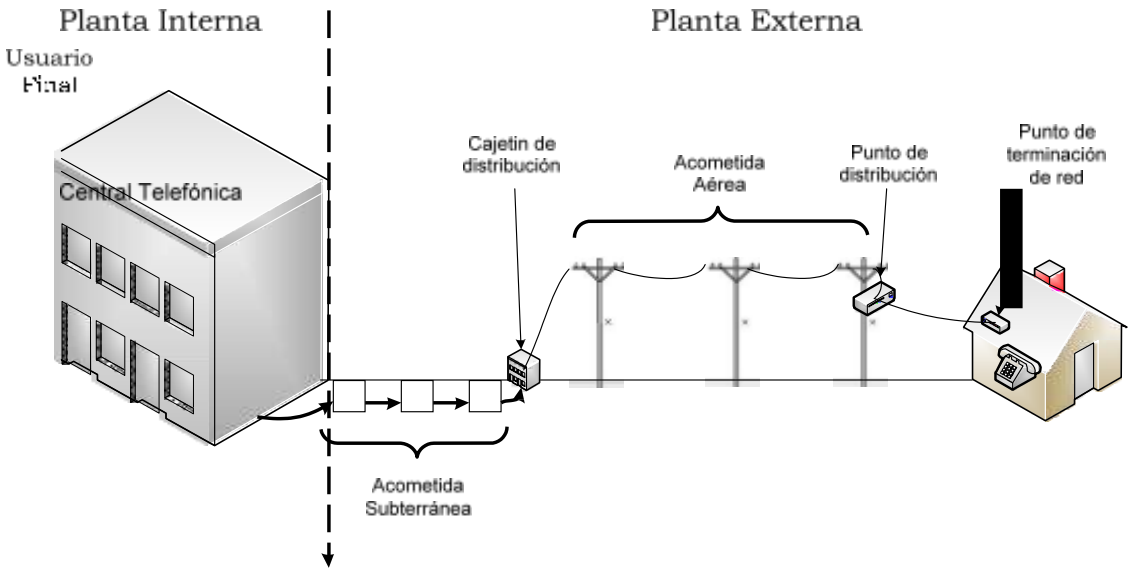


Figura 2.4 Red telefónica de cobre

b) RDSI

- La Red Digital de Servicios Integrados (RDSI), permite al Cliente tener con un solo acceso una multitud de servicios como son voz, datos, video, música , etc.:
- Básico (BRI); consta de dos canales datos de 64 Kbps y uno de señalización de 16 Kbps (2B +D), y en conjunto transmiten a una velocidad de 128 kbps. En este tipo de acceso puede conectarse hasta 8 equipos terminales y se pueden establecer dos comunicaciones simultáneas, una por cada canal B.
- El PRI; consta de 30 canales de datos de 64 Kbps y uno de señalización de 64 Kbps (30 B + D), que en conjunto tienen una velocidad de 1920 Kbps . El medio de transmisión normal es la fibra óptica; sin embargo también puede emplearse la red de cobre con ayuda de ciertos equipos de reciente tecnología.

c) Servicios de transmisión de datos:

- vMeganet, Digired, InterLAN, Unired, son distintos servicios que permiten conectividad digital transmitiendo datos de alta calidad y confiabilidad. Los enlaces de Voz, Datos y otros servicios proporcionados tienen velocidades en línea que alcanzan los 256 Kbps. Estos servicios van por un solo par de hilos de cobre.

d) Líneas Privadas:

- Utilizados como enlaces punto a punto o conmutados y que dependen de las velocidades a las que pueden trabajar los modems de los clientes.

e) Acceso a Internet:

- Permite el acceso a Internet del usuario final. Los Usuarios acceden a Internet a través de los CPIs (Centros Proveedores de Información) interconectados a Telefónica.

f) XDSL

- Los servicios ADSL también son soportados por la red de cobre, sin embargo es necesario conocer que los alcances están limitados en función de la velocidad y la distancia.
- Hoy en día el uso de la acometida para la línea telefónica y para datos son una misma, es más, por el mismo par telefónico, se implementa el paso de telefonía, Internet y transferencia de Datos (si está disponible en el sector y ambos puntos tienen el mismo proveedor de datos), y es posible mediante la tecnología xDSL.
- DSL que significa *Digital Subscriber Line* (en español *Línea de Suscripción Digital*), es un término utilizado para referirse de forma global a todas las tecnologías que proveen una conexión digital de banda ancha sobre la línea de abonado de la red telefónica básica o conmutada como: *"X"*DSL.- ADSL, ADSL2, ADSL2+, SDSL, IDSL, HDSL, SHDSL, VDSL y VDSL2.Figura 2.5

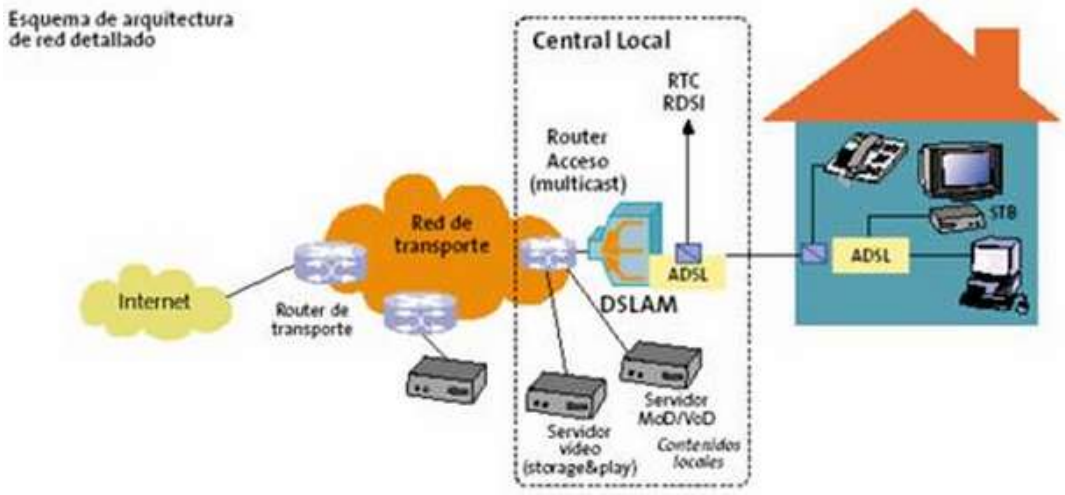


Figura 2.5 Tecnología ADSL

- El común es que usan el mismo par de cobre convencional de la línea telefónica para la transmisión de datos a gran velocidad (conexión al Internet), para el usuario final.
- La principal diferencia entre ADSL y otras tecnologías DSL, es que la velocidad de subida (Upload) y bajada (Download) de datos es asimétrica, es decir, que normalmente permiten una velocidad de bajada mayor que la de subida.
- Permiten altas velocidades de transmisión en ambos sentidos (hasta 20Mbit/s de bajada y 4 o 5Mbit/s de subida), manteniendo el servicio de voz tradicional. Permite tratar la voz y datos de forma separada. La voz sigue su camino tradicional, y los datos son encaminados a una red específica. ADSL es la más estandarizada y extendida. Se trata de una tecnología Asimétrica de banda ancha sobre el par de cobre tradicional.
- El filtro para ADSL es un filtro pasa bajo y alto, para la línea telefónica y el modem ADSL respectivamente, es usado para prevenir interferencia entre ambos servicios que operan en la misma línea que llega al usuario final. Figura 2.6

Figura 2.6 Filtro ADSL.

- Sin este filtro, las señales o ecos de los dispositivos analógicos pueden reducir el rendimiento y producir problemas de conexión con el servicio de ADSL, mientras que para los dispositivos analógicos puede resultar como ruido en la línea y otros problemas, por este motivo se requiere un filtro por cada teléfono, fax, módem analógico, y otros dispositivos que utilicen la línea telefónica, y se puede dejar el módem ADSL como el único dispositivo sin filtrar.
- Este tipo de acometidas tiene como principal y único objetivo, manejar el cableado estándar para las telecomunicaciones del lugar a instalar las cámaras de videovigilancia

Una vez visto los tipos de acometidas que pueden existir para una nueva edificación, es momento de ver las diferentes formas en las que podemos conectar estas acometidas, el tipo de conexión depende de: cómo sea la edificación, el sistema de instalación y las características de la red; y según estos parámetros las acometidas pueden ser de tipo: aéreo, subterráneo o mixta (aéreo y subterráneo simultáneamente).

Para una mejor definición de la Instalación de Entrada ó Acometida de entrada de datos, se pude decir, que es el punto donde entran los servicios de telecomunicaciones hacia la nueva edificación, este punto lo denominan PTR (punto de terminación de red), una vez que tenemos este punto de acceso de datos, lo siguiente es realizar una adaptación para unir estos servicios al edificio y hacerlos llegar a los diferentes lugares del edificio en su parte interior, utilizando

canaletas si la edificación ya está terminada o por tubería que estaría dentro de las paredes.

Cabe señalar que por la acometida de entrada de datos, no necesariamente debe estar dedicado para datos, esta acometida puede ser utilizada también para líneas telefónicas, acceso al Internet (como los servicios de ADSL de banda ancha visto anteriormente), o el Back Bone (cableados que interconectan dos o más redes por medio de un cableado estructurado de alta velocidad como fibra óptica) que venga de otro edificio, sistemas de video como TV digital o TV digital de alta definición (“HD” por sus siglas en inglés de High Definition), etc.

Otras empresas pueden utilizar una conexión satelital como lo vemos en la figura 2.7 y no usarían la acometida para datos.

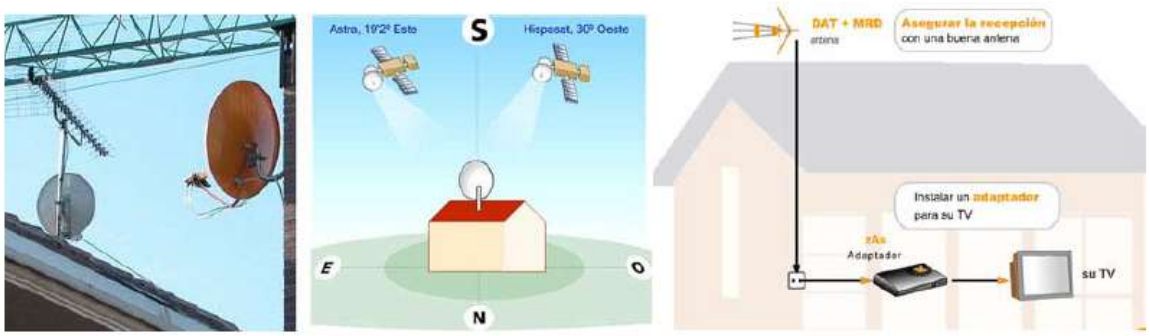


Figura 2.7 conexión TV-Digital HD satelital

2.2 Videograbadoras digitales

Las Videograbadoras Digitales (DVR) y las cámaras IP se han convertido en las impulsoras del circuito cerrado de televisión. Esto es resultado de la integración de las tecnologías ya probadas de computación, redes de datos, tecnología de la información y CCTV.

Es importante tener en mente que la mayoría de las cámaras de CCTV producen señales analógicas, con la consecuente inducción del ruido. Pudiéramos decir que las señales digitales son inmunes al ruido (técnicamente no es así). La ventaja del video digital es la posibilidad de procesamiento y almacenamiento. Mejora de imágenes, compresión, transmisión y correcciónes.

Las copias de las imágenes mantienen la misma calidad de la original, y cuenta con un sistema de “marca de agua” para comprobar la originalidad de la copia.
Hoy los sistemas de grabación hacen uso de disco duro para el almacenamiento de información. Los discos duros tienen un acceso aleatorio a la información, esto hace más eficiente al sistema. Lo que fue un problema hace algunos años, la capacidad de grabación, no lo es en la actualidad gracias a la aparición de discos duros de gran capacidad.

¿Cuántos días de grabación puedo almacenar en un disco duro de 500 GB?
La respuesta dependerá de varios conceptos:

- Tipo de compresión
- Calidad de grabación
- Modos de grabación
- Velocidad de grabación

2.2.1 Digitalización y comprensión de la imagen

La digitalización de una imagen es la representación de una fotografía en forma de unos y ceros. Una vez que una imagen ha sido digitalizada, tendrá la posibilidad de ser manipulada por el sistema de cómputo y podrá realizar funciones de compresión, almacenamiento, marca de agua, transmisión, etc.

La compresión de video utiliza 3 dimensiones: Horizontal, Vertical y Tiempo.

Como resultado tenemos compresiones como: MPEG-1, MPEG-2, MPEG4, H.263, H.264.

Se utiliza en DVR's que requieran alcanzar la mayor calidad de video y buena transmisión. Utiliza una técnica llamada GOP (Group of Pictures).

El CCTV digital sería imposible sin la compresión de video. Un video estándar sin compresión, utilizado en sistemas de televisión para su edición y procesamiento, es de más de 166 Mbps. Lo anterior es lógicamente impráctico, incluso para redes de 100 base T (es uno de los muchos estándares existentes de Fast Ethernet de 100 Mbit/s sobre cable de par trenzado). De tal forma, lo primero que debemos aplicar a un video ya digitalizado es un método de compresión.

A continuación se enlistan los métodos de compresión más utilizados en CCTV:

- JPEG y Motion JPEG (Compresión de Imágenes)
- JPEG-2000 / Wavelet y Motion JPEG (Compresión de Imágenes)
- MPEG-1 (Compresión de Video, Stream de datos 1-3Mbps)
- MPEG-2 (Compresión de Video, Stream de datos 1-30Mbps)
- MPEG-4 (Compresión de Video, Stream de datos 9.6Kbps-1.5Mbps)
- H.261 (Diseñado para Video Conferencia, Stream de datos 64Kbps)
- H.263 (H.261 mejorado, utiliza muy poco ancho de banda)
- H.264 / AVC (Servicio Genérico Audiovisual, nuevo estándar H.26x)

2.2.2 Pixelado de la imagen

Un pixel es la parte más pequeña de una imagen digitalizada, Los pixeles son los átomos de la imagen. En realidad un pixel contiene aún más información, los datos fundamentales del elemento más pequeño de la imagen, color y brillo. Un pixel es equivalente a un bit o un conjunto de bits.

La resolución de una imagen está definida por el número de pixeles de forma horizontal y vertical. La resolución de un cuadro completo de televisión es, d1 720 x 480, wd1 960x 582. Figura 2.8

Estas resoluciones pueden llegar hasta 1920x1080 pixeles en resoluciones HD.

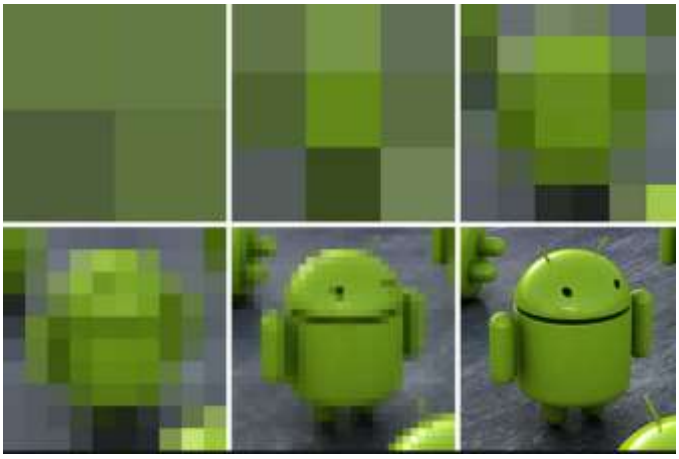


Figura 2.8 Ejemplo de imagen con diferente resolución

Existen técnicas de compresión que utilizan un cuarto 1/4 de los pixeles de un cuadro completo de televisión. Este tamaño es comúnmente conocido como CIF y es típicamente en compresiones actuales como MPEG ó H.XXX. Para la mayoría de las aplicaciones, una imagen en tamaño CIF es más que suficiente en calidad y en velocidad de transmisión. Figura 2.9

Figura 2.9 Resoluciones en grado CIF.

Una cámara fotográfica digital, en la actualidad, realiza tomas superiores a los 10, 000,000 de pixeles; una cámara de CCTV tendrá únicamente valores cercanos a los 415,000 pixeles.

Esta es la razón del por qué muchos usuarios dicen que la imagen se ve "pixelada" o con baja resolución. Siempre se tratará de compararla con una imagen fotográfica y esto no es posible en CCTV.

2.3 Distribución y control de cámaras

El sistema CCTV puede ser utilizado en diferentes escenarios, manteniendo vigiladas tiendas de conveniencia, oficinas, comercios, hospitales, edificios, conjuntos residenciales y cualquier lugar que necesite atención y protección; con la seguridad de que las cámaras captarán con total claridad las imágenes.

Las instalaciones de CCTV tienen tantas posibilidades, que es complicado marcar un estándar, cada problema tiene una solución a la medida[1].

A continuación se mencionan algunos tips y aplicaciones en cuanto al uso de cámaras Color día/noche:

- Los cableados del sistema de CCTV deben ser independientes de la red eléctrica.
- Evite que la cámara quede frente a fuentes de luz intensas como: luz directa, reflejos de rayos del sol directos en paredes o cristales, luces de la calle, etc.
- Tener en cuenta antes de instalar la cámara, el tamaño de la escena a monitorear y las distancias.

[1] www.bticino.com.mx/index.php?id=810 , Página recuperada, Septiembre 20 2014

- Para obtener el mejor enfoque de la cámara, se recomienda la configuración en condiciones de poca luz (noche) para que las condiciones de iluminación activen los LEDs infrarrojos. Instala la cámara lejos de fuentes de radiofrecuencia como: antenas, transformadores, cables de alta tensión o cualquier otro generador de interferencia electrónica.
- Procurar instalar un alimentador por cámara, para evitar fallas generales en caso de daño de la fuente.

2.3.1 Tipos de visualización

- Colocación adecuada de la cámara, la visión es clara y nítida. Figura 2.10

Figura 2.10 Colocacion correcta.

- El campo de visión tiene una fuente de luz directa. Para mejores resultados coloca la cámara con la fuente de luz fuera del campo de visión. Figura 2.11

Figura 2.11 Incorrecta, campo de visión tiene una fuente de luz directa

Fuera de la posición del sol. Figura 2.12

Figura 2.12 Posición correcta, Visualización de día y de noche

La conexión de la alimentación de cámaras debe hacerse respetando la polaridad y garantizando la continuidad en las conexiones.

- Instalar las cámaras entre 3 y 4 metros o fuera del alcance de actos de vandalismo. Figura 2.13

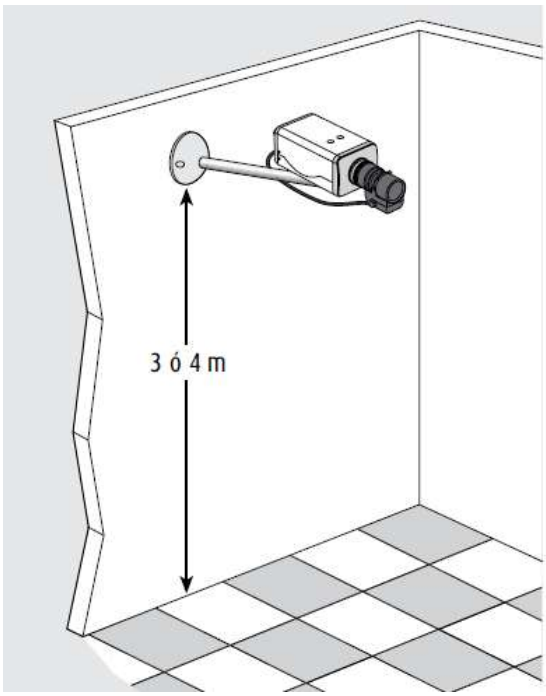


Figura 2.13 Instalación de la cámara de video

2.3.2 Criterios a considerar para la instalación de cámaras

En la actualidad existen diversas formas para controlar el monitoreo y la información adquirida a través de las cámaras de video vigilancia. Generalmente cada una de las cámaras, al adquirirla, contiene su propio software de control, el cual bien puede servir para controlar, y trabajar con otras cámaras (3 cámaras más, generalmente),

Los criterios, son todas aquellas condicionantes que se deben de tomar en cuenta para llevar a cabo una correcta instalación del equipo y no se presenten problemas al momento de operación, así como posibles puntos y tiempos en los cuales no se lleve a cabo una correcta grabación.

- **Profundidad de campo** Es una propiedad determinada por la apertura del iris, la longitud focal y la distancia de la cámara. El problema puede surgir cuando la vigilancia tiene lugar desde una distancia larga.

La profundidad de campo disminuye al utilizar lentes con mayores aumentos, las posibilidades de capturar una cara enfocada son más limitadas.

- **Luminosidad** Es importante tener una distribución de la luz equilibrada dentro del área de vigilancia. Por ejemplo, las fuentes de luz fluorescentes crearan mezclas de color debido a su temperatura del color específica (lo que frecuentemente se conoce como tubos de "luz cálida", de "luz de día", etc.). Es importante tener en cuenta que la luz solar cambia de intensidad y de dirección en el transcurso del día cuando la vigilancia tenga lugar en el exterior.

  La siguiente tabla muestra algunos valores de luminosidad:

Tabla 2.1 Valores de luminosidad

Valores de luminosidad	
Luz solar directa	50.000 lux
Luz indirecta con cielo claro	10.000 - 20.000 lux
Luz de cielo nublado	1.000 - 5.000 lux
Interior de oficina	200 - 500 lux
Mínimo para una lectura confortable	300 lux
Iluminación de pasillos y áreas de trabajo al exterior	50 - 100 lux
Puesta de sol	10 lux
Alumbrado público en la calle principal	15 lux
Alumbrado público por calle con poco tráfico	5 lux
Puesta de sol (inicio)	10 lux
Puesta de sol (al finalizar)	1 lux
Noche de luna llena	0.3 lux
Noche con luna menguante	0.1 lux

Las condiciones meteorológicas también crean diferentes factores de reflexión. Las calles de hormigón intensificará la luz reflejada, mientras que el asfalto mojado amortiguará la mayor parte de la luz reflejada (en caso de instalación en exterior). Llegado el caso, si es inevitable la mezcla de contrastes (como la entrada de un local vista desde adentro), es recomendable emplear lentes con auto iris, también se debe tener muy en cuenta la cantidad de luz que rodea el área de vigilancia. Sin la suficiente

luz solar, natural o artificial adicional, la calidad de la imagen se reducirá debido a fuertes contraluces o manchones blancos.

- **Ajuste de cámaras.** Además de garantizar suficiente luminancia, los ajustes de trabajo de las cámaras, para obtener imágenes son esenciales. Algunos modelos de cámaras IP ofrecen a través de su menú, ajustes de equilibrio de blancos, de brillo y nitidez, esto para obtener una mejor calidad de imagen y poder identificar fácilmente las causas de cualquier evento. Existen algunos modelos de cámaras en los cuales no es necesario hacer un ajuste de brillo, contraste, etc., ya que cuentan con la herramienta de autoajuste.
- **Ajuste de exposición.** Al decidir sobre el modo de exposición, se puede priorizar una velocidad alta (25 cps) o una compresión baja (100kB). Se recomienda una velocidad de obturación alta (o rápida) para registro de movimientos rápidos (por ejemplo cuenta de dinero en cajas), aunque si la escena lo permite, es conveniente reducir la velocidad a fin de obtener más espacio en disco o menor consumo de ancho de banda.
- **Combinación de cámara y lente.** Las lentes de ángulo de visión grande (por ejemplo 2.8 mm o 3.5 mm) no son adecuadas para la identificación de rostros por ejemplo, ya que deforman las proporciones de una cara,
  sin embargo son útiles para monitorear grandes áreas como calles, almacenes, áreas de recepción en hoteles, estadios etc.
- **Ubicación de la cámara de vigilancia.** La cámara de seguridad se debe colocar en soportes estables para minimizar el efecto de distorsión debido al movimiento, y en lugares donde no sufran afectaciones por vandalismo, daño por uso de equipo dentro de la zona a monitorear etc. Por ejemplo, cuando las cámaras PTZ (Pan Tilt Zoom, son las que tienen movimiento horizontal, inclinación vertical y controlan el aumento de la lente) se desplazan, esta acción puede provocar interferencias en la imagen si el domo de protección no esté bien fijado. Las cámaras exteriores deben fijarse a una altura de al menos 3.5 metros para dificultar su acceso pero permitiendo no distorsionar la imagen y acceder a su mantenimiento.

Recomendaciones

En la instalación, los sistemas de CCTV deben ajustarse a los requerimientos de las leyes de privacidad vigentes.

- Grabación, sonidos, voz y nombres son datos de carácter personal y pueden ser sujetos a derechos de autor u otra propiedad intelectual de terceros.
- En consecuencia, quien utiliza el equipo requiere:
  - Cumplir el código sobre la protección de datos personales.
  - Cumplir las obligaciones establecidas en el ámbito de la seguridad de los datos.
  - Respetar el derecho de imagen personal, así como la ley de propiedad intelectual e industrial y derechos de autor.
  - La marca del fabricante no es responsable por el uso ilegal de sus equipos por parte de sus clientes.

En cuanto a los cables

- **Cable coaxial,** Figura 2.14

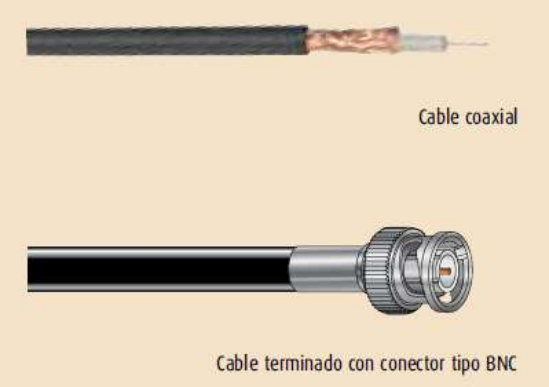


Figura 2.14 Cable coaxial

  - El cable coaxial más utilizado es el RG59
  - Debe acoplarse con conectores BNC, para una conexión más firme.
  - La longitud máxima del cable no debe exceder los 60 metros, cuanto más largo sea el cable, más débil es la señal.

- **Cable UTP**, Figura 2.15

Figura 2.15 Cable UTP.

– Cable UTP Cat. 5E o mayor con sus accesorios de transmisión
– Recepción. (hasta 400m.)
– Para el uso de otro cable UTP, consultar las especificaciones de uso del fabricante.

2.3.3 Guía para la selección de los dispositivos

- **Paso 1** Realizar una inspección junto con el cliente con la ayuda de un mapa o plano de las zonas a vigilarse. Figura 2.16

Figura 2.16 Zona a vigilar.

– Definir mediante una inspección del lugar las zonas a vigilar.
– Marcar en un plano con la aprobación del cliente.

- **Paso 2** Define con el cliente qué es lo que desea obtener: reconocimiento, identificación, o monitoreo de un área.

Si el sujeto es una persona y el sistema de CCTV se caracteriza por un límite de resolución efectivo superior a 400 líneas de televisión, el tamaño mínimo recomendado de este sujeto son:

a) Identificación: el objeto/sujeto debe representar no menos de 120% de la altura de la pantalla.

b) Reconocimiento: el objeto/sujeto debe representar no menos del 50% de la altura de la imagen.

c) Monitoreo de un área: ésta debe representar no menos de un 10% del espacio de la imagen.

La figura 2.17 muestra un ejemplo sobre el tamaño relativo de una persona (sujeto) en la pantalla:

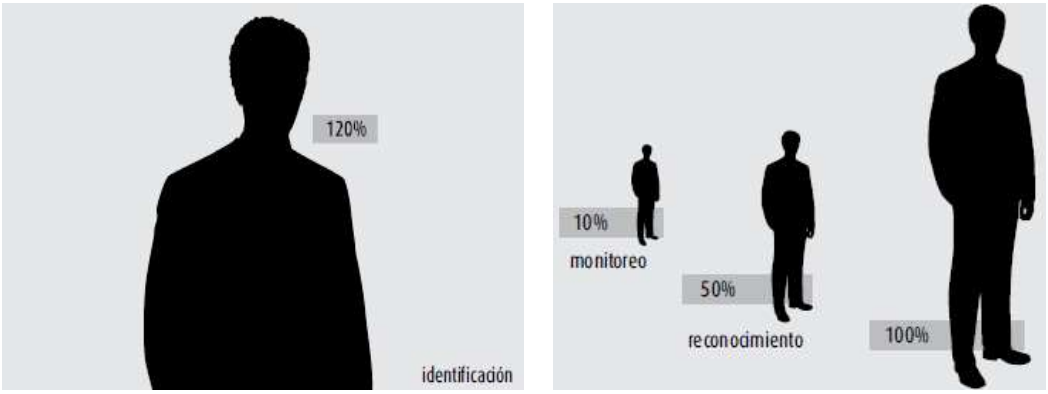


Figura 2.17 tamaño relativo de una persona

- **Paso 3:** definir el número de cámaras

  Identificar la posición más adecuada para cada cámara considerando los siguientes parámetros:

  – El tamaño de los objetos en el monitor (resultados esperados).
  – La distancia entre la cámara y el objeto a vigilar.
  – La ubicación de la cámara.
  – Las características de la cámara y aplicaciones (interna o externa, montaje techo o pared, etc.).

– El número de cámaras debe estar en cumplimiento con la legislación en vigor en cuanto a privacidad y protección de las personas.

Figura 2.18 Cámara CCTV, Tipo Domo

- **Paso 4:** DVR y accesorios, DVR's: en base al número de cámaras a instalar, elige el DVR.
  – MONITOR: elige el tamaño de la pantalla y el espacio disponible.
  – En su instalación y uso, los sistemas de CCTV deben ajustarse a los requerimientos de las leyes de privacidad vigentes.
  – Grabación, sonidos, voz y nombres son datos de carácter personal y pueden ser sujetos a derechos de autor u otra propiedad intelectual de terceros.
  – En consecuencia, quien utiliza el equipo requiere:
    ✓ Cumplir el código sobre la protección de datos personales.
    ✓ Cumplir las obligaciones establecidas en el ámbito de la seguridad
    ✓ de los datos.

- ✓ Respetar el derecho de imagen personal, así como la ley de propiedad intelectual e industrial y derechos de autor. El fabricante no es responsable por el uso ilegal de sus equipos por parte de sus clientes[2].

A continuacion se muestran los diagramas generales de conexión

Figura 2.19 DVR Serie

[2] www.biticiño.com,mx Septiembre 20 2014

Figura 2.20 Conexión básica de DVR

Figura 2.21 Conexión de cámaras al DVR en enlace ethernet

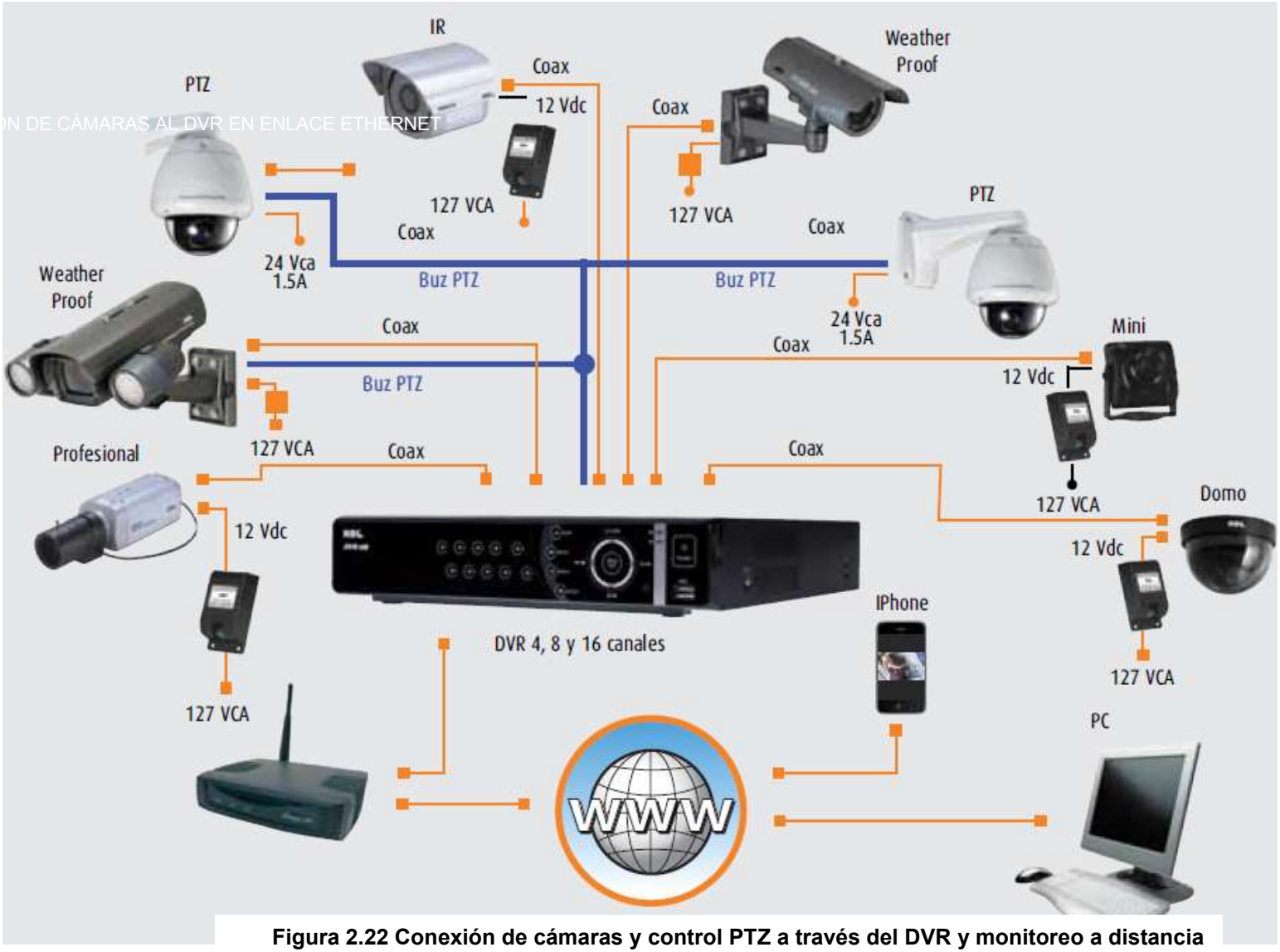


Figura 2.22 Conexión de cámaras y control PTZ a través del DVR y monitoreo a distancia

2.4 Programas de control de cámaras

- **Windows.** Una DVR basada en un sistema operativo Windows tiene más características y funciones, debido a que el disco duro no está limitado en su tamaño, como sucede con las memorias Flash. Figura 2.23

Figura 2.23 Logo Windows[3]

- **LinuxMCE**. Es una solución de código abierto que combina medios y entretenimiento con un servidor de música y vídeo, además de un PVR (grabador de vídeo personal), como TiVo o Sky +. Aporta beneficios para implementar domótica para el control del hogar, desde las luces hasta la calefacción, con una tableta de pantalla táctil en el teléfono móvil. Cuenta con un sistema de video en directo, direccionado a un dispositivo móvil durante un evento que represente una amenaza de seguridad[4]. Figura 2.24

Figura 2.24 Logo LinuxMCE.

[3] Logo que cuenta con permiso de publicación por parte del fabricante y que es usado con fines de educación
[4] Ibídem

- **ZoneMinder** está diseñado para aplicaciones de seguridad individual o de varias cámaras de vídeo, incluyendo circuito cerrado de televisión comercial o en el hogar. Es compatible con la captura, análisis, registro y monitoreo de datos de vídeo procedentes de una o más cámaras de red conectada a un sistema Linux. Como ventaja adicional, es posible conectar al sistema de cámaras un dispositivo x-10, ya sea una alarma, encendido de luces, etc. Este dispositivo será accionado en cuanto se detecte alguna anomalía en el área vigilada, por medio de las cámaras, este software se puede adquirir de forma gratuita desde su portal de internet[5]. Figura 2.25

Figura 2.25 ZoneMinder

2.5 Puntos de monitoreo

Después de decidir la tecnología más conveniente, siendo este un sistema inalámbrico, se toman algunas consideraciones para la ubicación de las cámaras una vez definidos los puntos que se van a monitorear, por ejemplo, lugares donde se encuentren grandes cantidades de dinero, objetos de alto valor, entradas y salidas, o supervisión de personal.

Siempre se debe evitar colocar las cámaras frente a los rayos solares o en sitios donde la luz le afecte directamente a la cámara, de esta forma se podrán obtener imágenes mucho más claras y se evitarán efectos molestos como los contraluces. Al mismo tiempo, es bueno que las cámaras de seguridad no estén situadas en sitios con poca luz o completamente oscuros, si es que éstas no son infrarrojas o de visión nocturna.

[5] Logo que cuenta con permiso de publicación por parte del fabricante y que es usado con fines de educación

En caso de que el lugar en donde se tenga que ubicar el dispositivo sea oscuro, se tendrá que agregar luces adicionales para mejorar la obtención de imágenes. Si las cámaras de seguridad deben ubicarse en entornos donde la iluminación es muy variable, se aconseja optar por modelos de dispositivos que contengan lente auto iris. La función de este tipo de cámaras de seguridad es ajustar automáticamente el iris de acuerdo a la cantidad e intensidad de la luz que se recibe, tal como lo hace el ojo humano.

- **Conexión de red** Cuentan con una conexión de red Ethernet y de un software gratuito que le permite controlar el grabador desde un ordenador conectado de forma local. Esto es muy útil por ejemplo para poder visualizar las grabaciones desde un ordenador de la oficina, mientras que el aparato se encuentra instalado físicamente en la sala de máquinas. Además se puede configurar, visualizar las cámaras o hacer copias de seguridad sin que nadie lo sepa, con independencia de lo que se está viendo en el monitor principal, el inconveniente es que el software será útil para cámaras del mismo fabricante, y se deseara ampliar el sistema es necesario adquirir un nuevo software y licencia con el proveedor de las cámaras.

- **Servidor DNS Domain Name System (Sistema de nombres de dominio**). Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a internet o a una red privada. La función más importante es resolver nombres inteligibles para las personas, en identificadores binarios asociados con los equipos conectados a la red, con el propósito de poder localizar y direccionar los equipos mundialmente.

  Para la operación del sistema DNS se utilizan 3 componentes principales: Los clientes DNS: Un programa DNS que se ejecuta en la computadora del usuario y que genera peticiones DNS de resolución de nombres a un servidor DNS.

Los servidores DNS: Se encargan de contestar las peticiones de los clientes. Los servidores tienen la capacidad de reenviar la petición a otro servidor si no disponen de la dirección solicitada. Zonas de autoridad: Son porciones del espacio de nombres de dominio para almacenar datos. Cada zona de autoridad abarca al menos un dominio y en varias ocasiones sus subdominios, esto es posible solo si no pertenecen a otra zona de autoridad. Un DNS se divide en dos o más partes, separadas por puntos cuando se escriben en forma de texto. Por ejemplo, A la etiqueta ubicada más a la www.mohamedali.org derecha se le llama dominio de nivel superior (en inglés top level domain). Como org en www.ejemplo.org. Cada etiqueta a la izquierda especifica una subdivisión o subdominio. Lo cual consiste en una dependencia. Esta subdivisión puede tener hasta 127 niveles, y cada etiqueta puede contener hasta 63 caracteres, pero restringidos a que la longitud total del nombre del dominio no exceda los 255 caracteres, aunque en la práctica los dominios son casi siempre mucho más cortos. Finalmente, la parte más a la izquierda del dominio suele expresar el nombre de la máquina (en inglés hostname). El resto del nombre de dominio simplemente especifica la manera de crear una ruta lógica a la información requerida.

Considerando el proveedor del servicio solo se puede hacer con Axtel o Telmex ya que cablevisión total play y otros servicios no dan el servicio que necesitamos de apertura de puertos ya que usan una red virtual y no tienen una salida a internet fija. En cambio las dos primeras empresa mencionadas si proporcionan este servicio de apertura de puertos de manera gratuita. En caso de que el usuario tenga servicio de internet por cablevisión se podrá realizar la apertura de puertos pero tiene un costo de 900 pesos mensuales.

Capítulo 3
Instalación y configuración del CCTV, ejemplo de un caso práctico

Para comenzar con una instalación profesional de un sistema de video vigilancia, la primera etapa es hacer un estudio detallado del lugar donde se hará la instalación, en esta etapa se consideran varios factores, los cuales se describen a continuación:

- Interior/exterior: Necesitamos definir la ubicación de las cámaras, si será en el interior o exterior del edificio, teniendo en cuenta éste dato se selecciona el modelo adecuado.
- Iluminación: Después de tener definida la ubicación, se debe observar la cantidad de luz que hay en el área de observación, esto es para determinar las funciones especiales de la cámara.
- Longitud focal: Si la cámara será colocada lejos del objetivo, entonces se debe optar por una con lente varifocal de mayor milimetraje, así tendremos la ventaja de ajustar el lente hasta obtener el acercamiento deseado.
- Ángulo de visión: Si el área del objetivo es muy ancho, entonces debemos optar por una cámara de lente menor a 3.6 mm (ej. 2.5 mm), con este elemento tendremos un ángulo de visión de aproximadamente 95°, suficiente para observar un cuarto de tamaño medio (aprox. 5m x 6 m).
- Obstrucciones: Debemos considerar todas las posibles obstrucciones para la línea de vista de la cámara (ej. árboles, columnas, muebles, paredes, entre otras), si alguna está de por medio, entonces debemos elegir otro lugar para su montaje sin perder el área a vigilar.
- Altura: Este aspecto se tiene que definir con precisión, si la instalación es en un lugar con techos muy altos, entonces la colocación deberá ser a una altura de aproximadamente 2.5 m (distancia estándar de un techo de casa) desde el suelo para no perder el ángulo de visión.

- Ruta de cableado: Es muy importante definir la ruta de cables, si es por un conducto específico para el sistema, si es aéreo (colgado de postes) o subterráneo. Por ningún motivo debe hacerse cerca o por el mismo conducto de una línea eléctrica, ya que se podría generar interferencia con la señal de video.
- Distancia a la central de monitoreo: Para un sistema eficiente en cuanto a calidad de video la distancia típica es de 300 m con la ayuda de transmisores de video pasivos1, en caso de ser mayor la distancia entonces se usan transmisores activos.
- Conexiones de red Si el usuario requiere de una conexión a internet para monitoreo remoto, se debe considerar el proveedor del servicio, el ancho de banda existente y contar con un router (si no se tiene un modem no se podría hacer la configuración).

3.1 Cálculo del rango del lente de una cámara de CCTV

Antes de comprar una cámara de circuito cerrado de televisión (CCTV, por sus siglas en inglés) o un lente para una de estas cámaras, necesitamos saber cómo calcular el rango del lente. Esto lo dirá el campo de visión vertical y horizontal. Es posible que necesitemos un campo de visión amplio para vigilar un estacionamiento o uno mucho más pequeño para reconocer a alguien frente a tu puerta.

Pasos a seguir

1. Medir la distancia que hay entre la cámara y el área que se desea cubrir
2. Medir el ancho del área que se desea observar.
3. Dividir la medida del ancho entre la distancia medida. Por ejemplo, si la distancia desde la cámara hasta el área que deseas ver es de 20 pies (6 m) y quieres una vista de 5 pies (1,5 m) de ancho a esa distancia, dividir 20 por 5 y tu respuesta será 4.

4. Averiguar el tamaño del sensor de tu cámara y multiplicar la respuesta conseguida en el Paso 3 por el multiplicador correspondiente. Multiplicador de sensor de una pulgada (2,5 cm): 12,8. Multiplicador de sensor de 2/3 de pulgada (1,6 cm): 8,8. Multiplicador de sensor de 1/2 pulgada (1,2 cm): 6,4. Multiplicador de sensor de 1/3 de pulgada (0,8 cm): 4,8. Si se tiene un sensor de 1/3 de pulgada (1,6 cm), siguiendo el ejemplo anterior, multiplicarás 4,8 por 4 = 19,2; por lo tanto el tamaño lente que se necesita es de 19,2 mm.
5. Multiplicar el campo de visión horizontal por 0,75 para obtener el campo visión vertical aproximado. Usando el ejemplo del Paso 3, el campo de visión horizontal es de 5 pies (1,5 m) por 0,75, así que el campo de visión vertical será de 3,75 pies (1,1 m). Este es un buen campo de visión para ver los detalles del rostro y el torso superior de una persona con claridad a unos 20 pies (6 m).

La fórmula es: Longitud focal de lente = Multiplicador X (distancia a la cámara/campo de visión horizontal). Estos cálculos son aproximados y variarán dependiendo de varios factores, incluyendo variaciones entre los fabricantes de cámaras y lentes. Si se desea calcular el rango de los lentes usando una calculadora[1] para este propósito (Probablemente no se encontrara un lente que coincida exactamente con los cálculos, pero se podrá conseguir un lente bastante cercano a ellos que será adecuado para la instalación de la cámara

3.1.1 Tamaño de la imagen angula de observación

Los CCD (Sensor de imagen o CCD: Dispositivo que conviértela luz visible en energía eléctrica para ser almacenada, procesada y enviada a través del cable, principalmente se componen de un número determinado de condensadores y células fotovoltaicas que registran la imagen.) más grandes captan más luz, y por

[1] http://www.webcamsoft.com/en/faq/lens_calc.html Página recuperada 31 de octubre de 2014

lo tanto tienden a ser más sensibles que los CCD en formato más pequeño. Los precios de las cámaras se incrementan con el tamaño del sensor Por tanto, la selección del tamaño del sensor debe adecuarse tanto a su presupuesto como a la aplicación. Figura 3.1

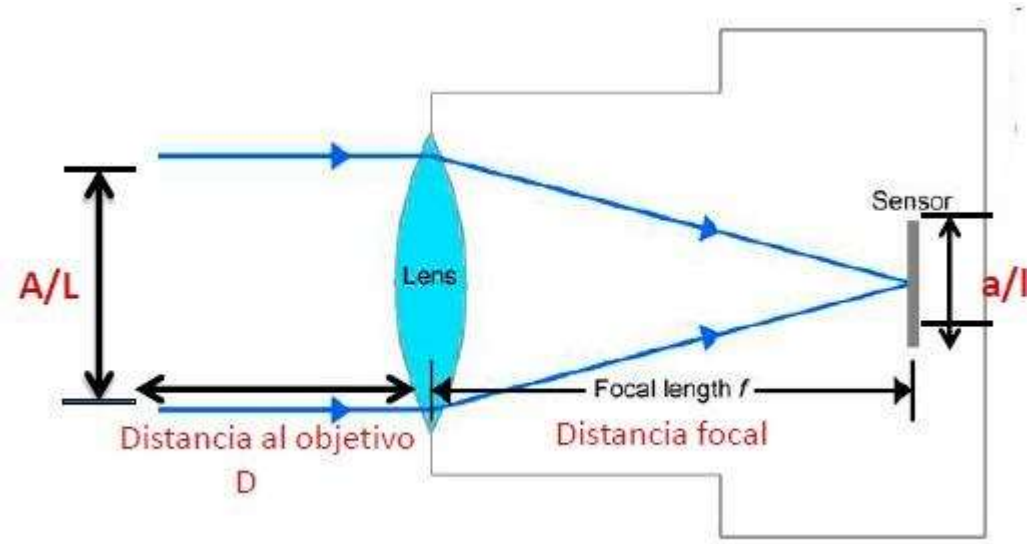


Figura 3.1 Sensor de imagen o CCD:

$$\frac{a}{A}=\frac{l}{L}=\frac{f}{D} \qquad \textbf{Ec. 3.1}$$

Dónde:

A=Altura de la imagen

L=Largo de la imagen a=altura del CCD (mm)

l=largo del CCD (mm)

f=Distancia Focal

D=Distancia al objetivo

Al incrementar la distancia focal de la lente disminuye la distancia percibida al área visualizada, pero también disminuye el área que la cámara es capaz de observar.

Observe el diagrama de ángulos que se encuentra a continuación para las visualizaciones aproximadas con diferentes lentes de distancia focal[2]. Figura 3.2

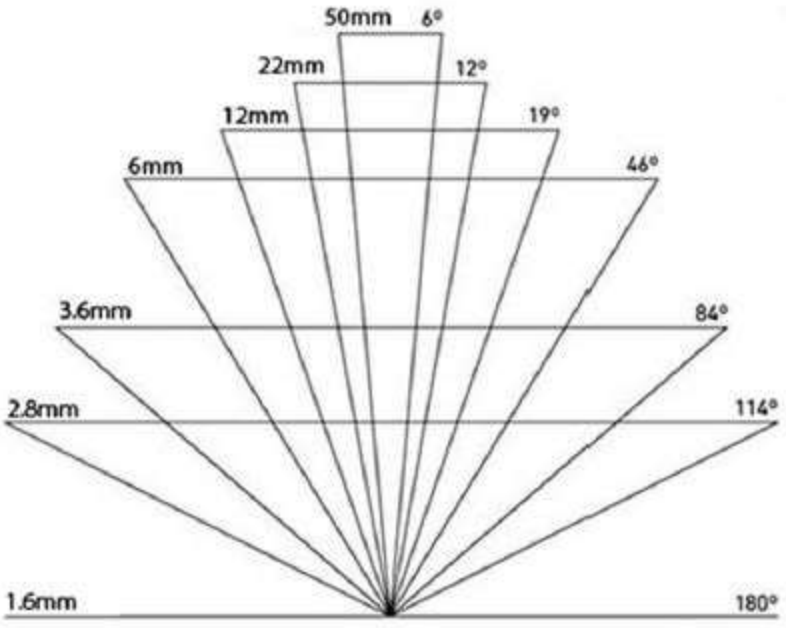


Figura 3.2 Diagrama de ángulos

Ejemplo

Si se quiere que la imagen completa de una persona alta (1,8 m.) aparezca en el monitor de CCTV. La persona se encuentra a aproximadamente 6m. De distancia de la cámara de seguridad. La cámara utiliza un sensor CCD formato 1/3".

Datos:

a= 3.6 mm.

A= 1.8 m. = 1800 mm.

D = 6 m = 6000 mm.

[2] Para observar el diagrama de ángulos dirigirse a la siguiente dirección electrónica http://www.apexcctv.com/Lens-Field-of-View-Comparison.html, pagina consultada, 31 de octubre de 2014

$$\frac{a}{A}=\frac{f}{D}\circledR\frac{3.6}{1800}=\frac{f}{6000}=12mm$$

Por lo tanto se requiere una lente de 12 mm. Para alcanzar los mayores resultados en esta aplicación[3].

3.2 Implementación y puesta en funcionamiento de un sistema de circuito cerrado de televisión (CCTV)

A continuación se muestra el proyecto que consta de

- DVR marca Meriva Security 8CH Video, 4CH Audio, 1 Salida de Audio, 240 fps, HDMI, Multiplex, soporta hasta un máximo de 2 Tbytes en HDD. Cantidad 1
- Cámara marca Meriva Security 700 TVL, IR 24 leds., tipo Bullet o Domo, Antivandálica, CCD Sony Effio 1/3", Cantidad 8.
- Fuente de Poder 12 Volts, 5 Amp tipo Laptop marca Enson, Cantidad 2.
- Monitor 15.6" marca HP o Lenovo (según existencias), tecnología LED Pantalla Plana. Cantidad 1.
- Disco Duro 2 Terabytes SATA II, 7200 rpm para respaldo de 2 meses. Cantidad 1.
- Transductores pasivos para acoplamiento de señal de video. Cantidad 16
- Cableado y protección con tubería (o Canaleta según se requiera).

[3] http://www.tecnosinergia.com/ Página consultada 31 de octubre de 2014

El plano del proyecto es el siguiente:

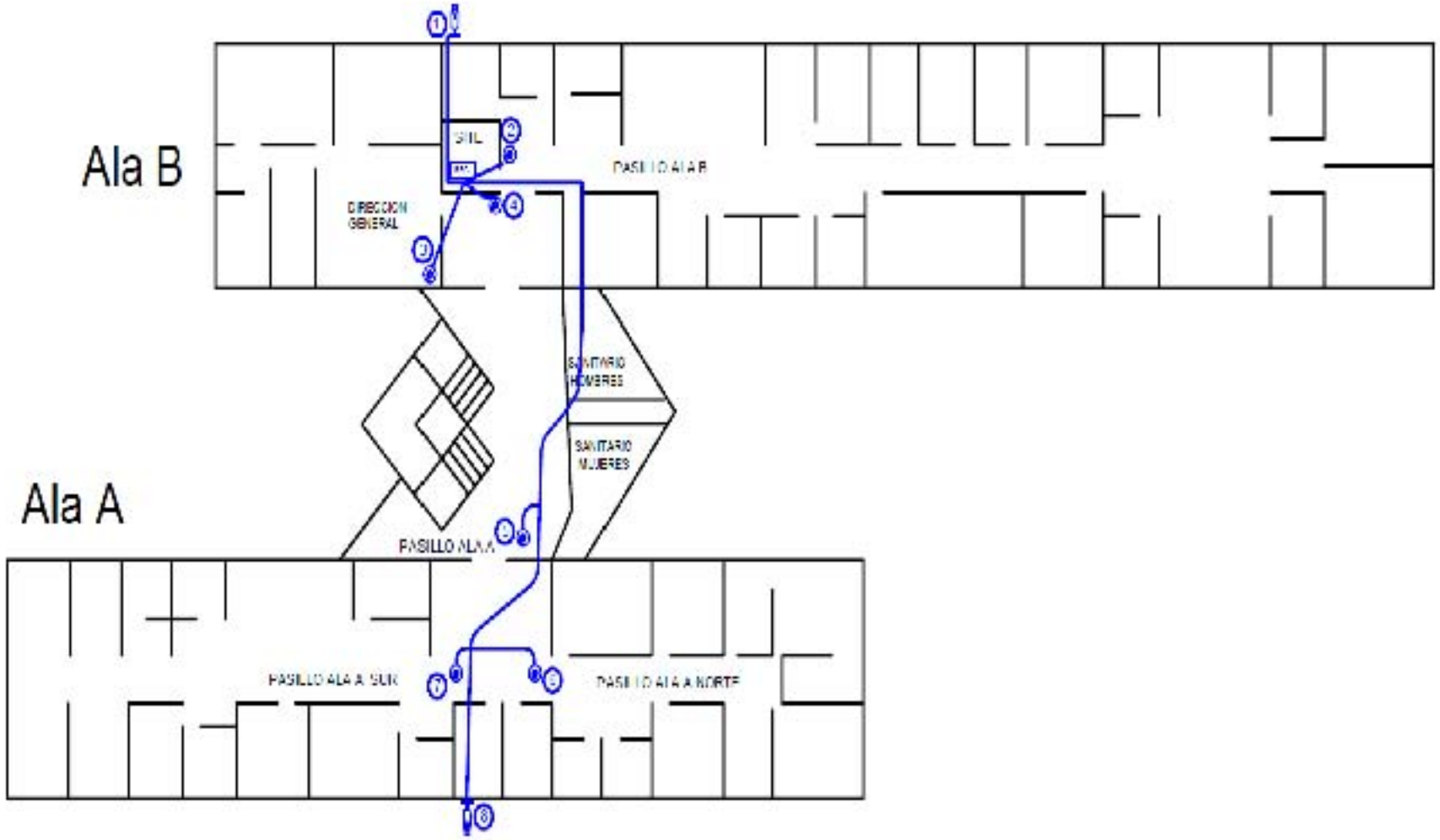


Figura 3.3 Diagrama de instalación de las cámaras de video vigilancia

La simbología se muestra en la figura 3.4

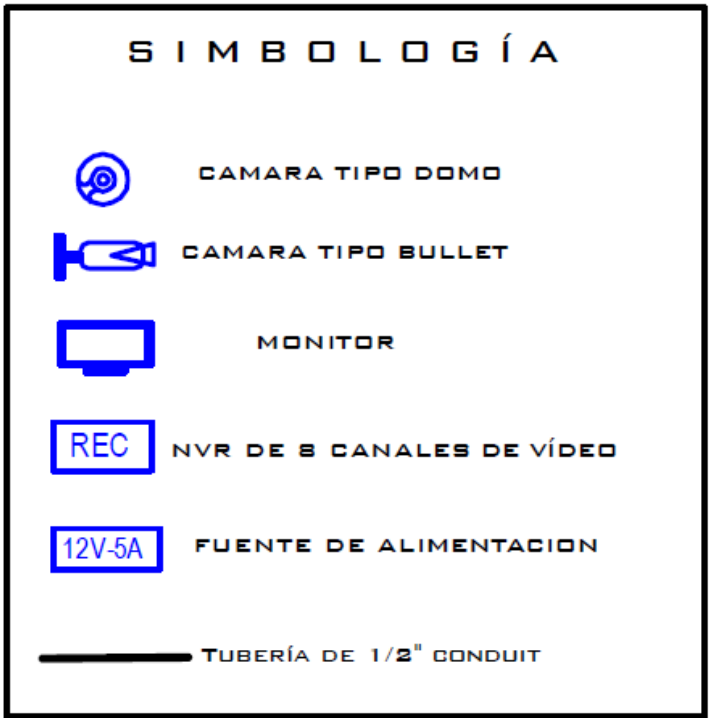


Figura 3.4 Simbología

El proyecto consta de tres cámaras exteriores (1,5 y 8) y cinco cámaras interiores (2, 3, 4,6 y 7)

Prácticamente en todo el lugar se tiene solo un tono de iluminación, por lo tanto, en 5 de las cámaras las funciones son básicas. Las tres restantes tienen que ser con características especiales ya que ésta estará dirigida hacia el exterior del edificio, en la cual se percibe un alto índice de luz.

- La instalación de las cámaras cerca del techo del local, el cual tiene una altura de 2.5 a 3 m aproximadamente.
- El cableado se ocultó en la cavidad que da el plafón con el techo del edificio, ya que era la forma más eficiente de hacerlo y de manera estética.

En este caso, el usuario solicitó una conexión de red, lo cual no implicó ningún problema ya que se cuenta con un proveedor de internet eficiente con un ancho de banda de 2 Mbps (suficientes para la transmisión de las 8 cámaras en forma no pausada) y un router.

Esta etapa se hace junto con el usuario, de esta manera ellos tienen una idea de lo que quieren vigilar y al mismo tiempo el proveedor se encarga de asesorarlo y darle a conocer otros puntos de vista para complementar y mejorar el sistema.

3.3 Instalación

En esta etapa es cuando ya se tiene la disposición de hacer la instalación, pero antes de comenzar, lo primero que se debe hacer es un recorrido por el lugar para inspeccionar las ubicaciones de los equipos y ruta de cableado, con esto se confirma si en realidad lo que se había definido en el estudio es lo que se puede implementar en la práctica. En ocasiones, el usuario puede cambiar de parecer en cuanto a la ubicación de uno o varios dispositivos, es por eso que este recorrido se hace junto con él para confirmar la instalación.

Si durante el recorrido se observa que no se puede hacer como se tenía previsto, se busca una ruta o ubicación distinta pero sin perder de vista el objetivo (área de vigilancia, estética, distancia, etc).

Aquí es donde se comienza a hacer la instalación del sistema, se comienza con el cableado que es lo que más tiempo implica. En esta parte usualmente se encuentran problemas como:

- Obstáculos internos de una pared cuando sea necesario perforar un muro para atravesar el cable (piedras o varillas), uniones en el trayecto (por corte accidental del cable), líneas eléctricas paralelas, entre otros.
- Existen diferentes materiales con los que se hace un muro, entre estos están: ladrillo, block ligero, block rígido, concreto, tablaroca, lámina. Cada

material tiene distinta rigidez y debemos ser cautelosos y saber si el material del muro puede soportar el peso de la cámara que se requiere colocar. El cableado debe hacerse de manera que parta desde el centro de monitoreo y de ahí distribuirse a cada punto de ubicación de los dispositivos.

Teniendo el cableado listo para cada una de las cámaras, el paso siguiente es colocar las bases de las mismas en los lugares que se habían definido anteriormente para después montar los dispositivos en las bases. Aquí no hubo mayor problema, al contrario, se facilitó mucho el montaje por ser una superficie de tablaroca (no se requirió usar un rotomartillo para hacer las perforaciones de la tornillería) y además de eso se recuperó el tiempo que se perdió con el cableado.

Después de colocar las cámaras en sus posiciones, el paso siguiente es el de enfocar y ajustar el ángulo de vista hacia el área de vigilancia. Para este paso se hace uso de un monitor portátil de mano, con el cual podemos hacer el ajuste directamente en la cámara (esto ahorra tiempo porque evita tener que ir hacia el centro de monitoreo y revisar si ya quedó en perfecta posición). Este procedimiento se hace en cada una de las cámaras instaladas.

Cuando ya se tiene un enfoque deseado, se procede a conectar los dispositivos que nos ayudarán con la transmisión de video y la alimentación de voltaje. Se necesitan dos hilos de alambre de cobre para transmitir el video hacia la DVR con la ayuda de transceptores pasivos de un canal (se necesita un par de transceptores; uno se conecta directamente en la cámara y otro se conecta en la DVR, éstos deben conectarse con la misma polaridad en ambos extremos) y dos hilos más para la alimentación de la cámara.

Teniendo los dispositivos de apoyo conectados en cada cámara y así mismo en cada canal de la DVR, podemos decir que la instalación física está completa y podemos pasar a la siguiente etapa de la instalación.

Se muestra a continuación por medio de fotografías el procedimiento que se siguió para la instalación de las videocámaras.

Fig. 3.5 Cableado de cámaras

Fig. 3.6 Guía del cableado

Fig. 3.7 Colocacion de tubos para el cableado de las videocámaras

Fig. 3.8 Tubería escondida sobre plafón

Fig. 3.9 Cámaras interiores

Fig. 3.10 Cámaras interiores en pasillo

Fig. 3.11 Cámaras exteriores

Fig. 3.12 Cámara exterior (Patio)

Fig. 3.13 Monitoreo de las 8 cámaras instaladas

3.4 Configuración del DVR

3.4.1 Apertura de puertos

Antes de comenzar es importante que verifique los siguientes puntos

- Estar conectado al ruteador que quiere configurar, ya sea de manera alámbrica o inalámbrica.
- Contar con internet disponible y funcionando
- Conocer la contraseña del ruteador, regularmente es la clave WEP KEY que se encuentra en una etiqueta de su ruteador o la que usted le haya asignado.
- Para realizar el procedimiento se requiere conocimientos básicos de redes, no intentar realizarlo si no cuenta con dichos conocimientos.

1. Abrir una ventana de explorador de Internet e Ingrese la siguiente dirección IP* para accesar a la interfaz de configuración de su Ruteador Thomson (Es el modem utilizado por el operador telefonico preponderante en nuestro país) http://192.168.1.254 o bien http://home. Figura 3.14

Figura 3.14 Dirección IP

Esta dirección hace referencia a la puerta de enlace principal de la red, en algunos casos y esto dependiendo de la administración esta puede variar.

A continuación aparecerá la siguiente pantalla:
Donde tendremos que introducir usuario y contraseña de nuestro Ruteador.
Por Default: Usuario: TELMEX Contraseña: WEP KEY, Figura 3.15

Figura 3.15 Inserción de usuario y contraseña.

A continuación aparecerá la siguiente pantalla: Seleccione la opción de HERRAMIENTAS Resaltada en la figura 3.16

Figura 3.16 Sección herramientas

Aparecerá la siguiente Pantalla

2. Lo siguiente es Seleccionar la opción de COMPARTICION DE JUEGOS Y APLICACIONES resaltada en la figura 3.17

Figura 3.17 Pantalla de aplicaciones.

3. En la siguiente pantalla seleccione la opción de ***CREAR UN NUEVO JUEGO O APLICACIÓN*** resaltada en la figura 3.18

Figura 3.18 Crear una aplicación

4. A continuación introduzca un **NOMBRE** para la aplicación que se va a crear y seleccione la opción de ***ENTRADA MANUAL DE MAPAS DE PUERTOS*** como se muestra en la figura 3.19.

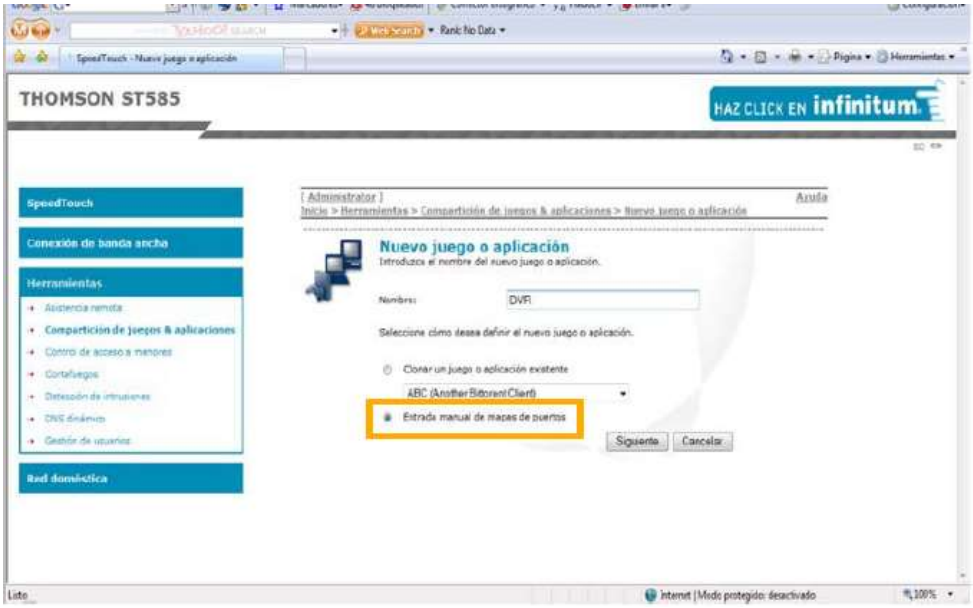


Figura 3.19 Mapas de Puerto.

5. A continuación selección el tipo de PROTOCOLO a utilizar seguido del INTERVALO DE RANGOS que se desean abrir como se muestra en la figura 3.20

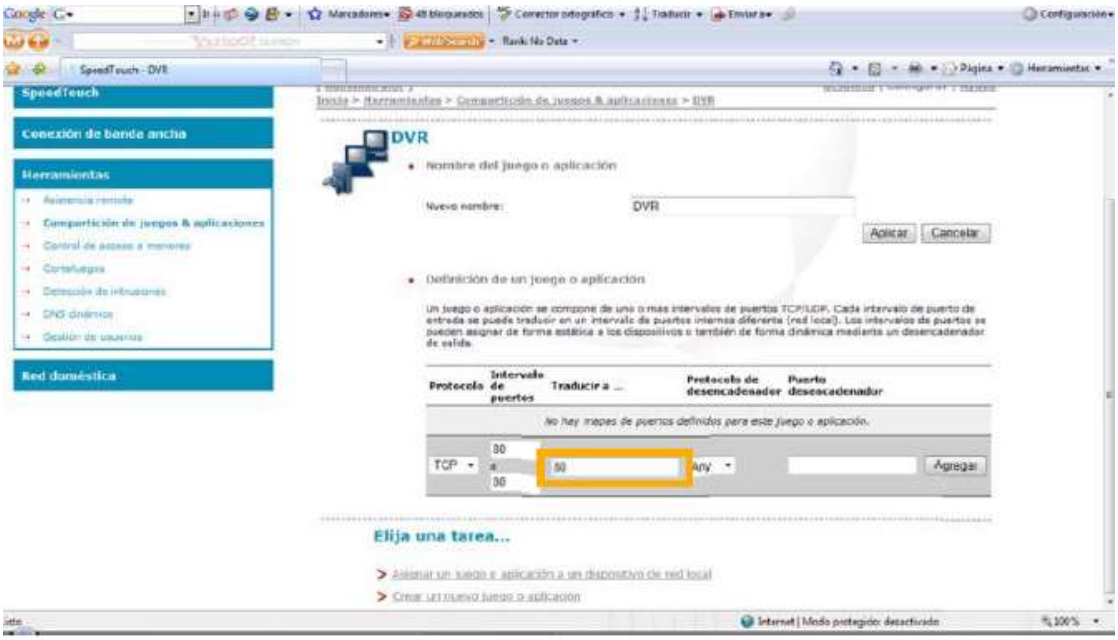


Figura 3.20 Tipo protocolo.

6. Enseguida seleccione la opción de ASIGNAR UN JUEGO O APLICACIÓN A UN DISPOSITIVO DE LA RED LOCAL. Figura 3.21

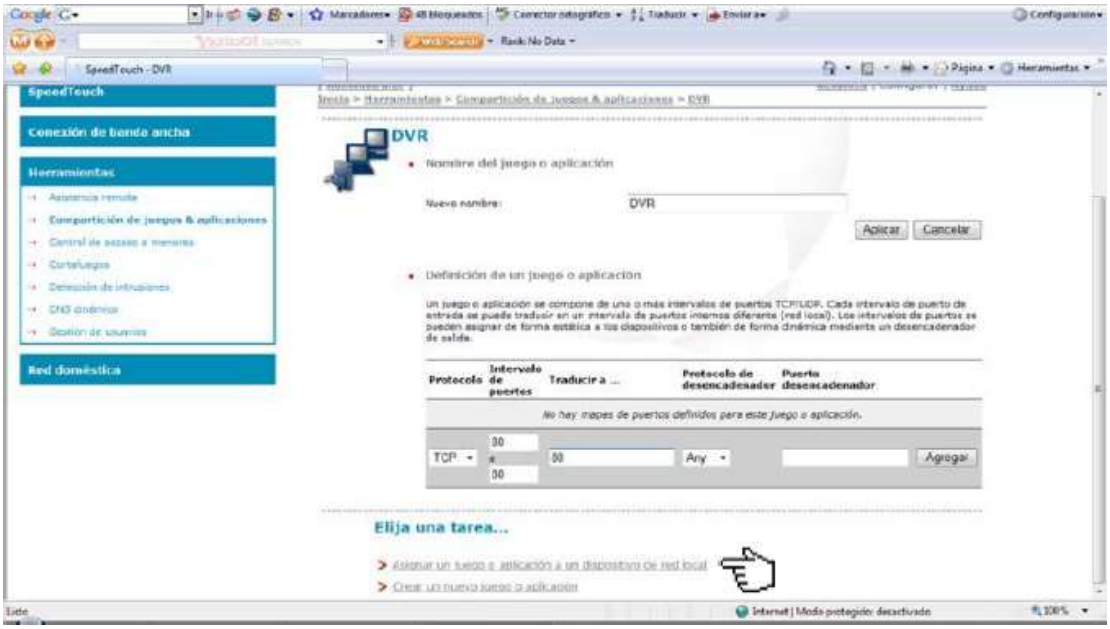


Figura 3.21 Dispositivo local

En esta siguiente pantalla, seleccionamos de la lista de aplicaciones asignadas, la aplicación creada seguida del dispositivo al que se va a asignar la aplicación. Figura 3.22

Figura 3.22 Lista de aplicación para asignar

Finalmente podemos observar que la aplicación fue asignada al dispositivo. Figura 3.23

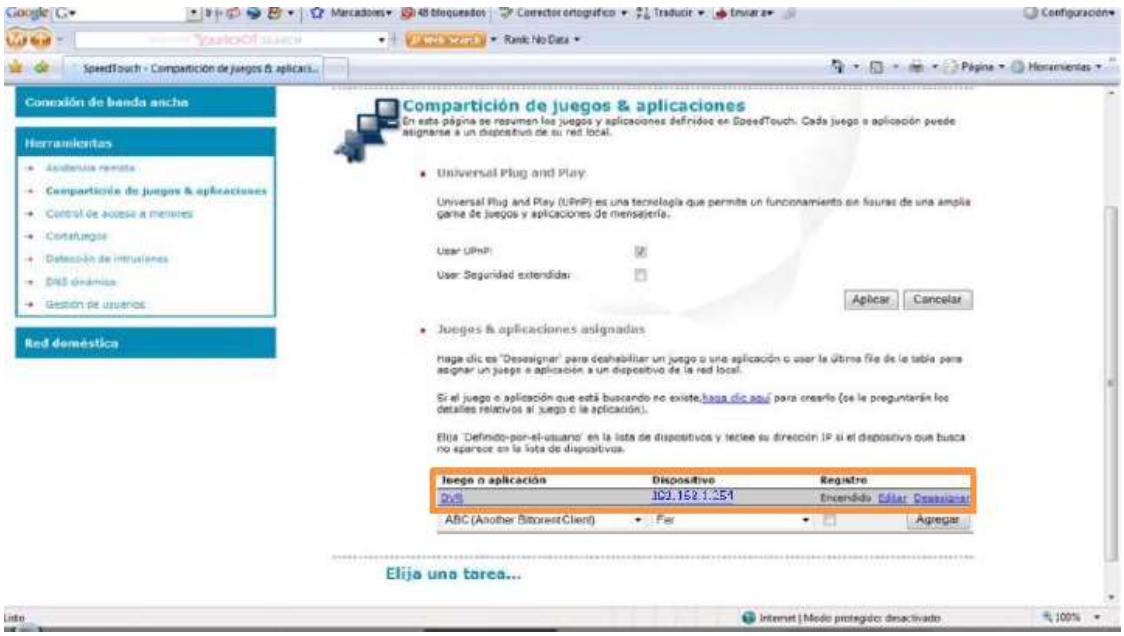


Figura 3.23 Aplicación asignada.

Como información adicional, para los diferentes DVR's que manejamos los puertos que regularme se abren son:

- DVR Meriva tiene los puertos 80 y 6036
- DVR Elikon tiene el puerto 7000
- DVR Elikon RT tiene los puertos 80,10101 al 10104.

3.4.2 Configuración DDNS DVR

Para poder tener acceso a su DVR de manera remota, debe realizar la apertura de puertos y la configuración de DDNS. A continuación se explica cómo realizar la configuración de DDNS para un DVR Meriva, utilizando el dominio propio de Meriva.

1. Teclear la siguiente dirección: http://www.dvrdydns.com/ Como resultado nos aparece la siguiente pantalla. Figura 3.24

Figura 3.24 Dominio propio del fabricante.

2. En este paso damos Clic en “Registration” para registrarnos, con el previo llenado de todos los campos mencionados en este formulario.

   Se recomienda que la contraseña se a de al menos 6 caracteres, no incluir caracteres alfanuméricos y en sensible a mayúsculas o minúsculas. Figura 3.25

Figura 3.25 Registro de DVR

3. El siguiente paso, es crear nuestro nombre de dominio, mismo que teclearemos para entrar al DVR desde cualquier sitio. Por lo que se sugiere darle un nombre según ubicación o empresa .Figura 3.26

Figura 3.26 Nombre de dominio.

4. Finalmente aparecerá la última pantalla de confirmación de parámetros en el que nos muestra que sea dado de alta tal nombre de dominio para la cuenta. Figura 3.27

Figura 3.27 Confirmación de parámetros.

La opción “Create additional domain names”, que se encuentra a la parte inferior de la pantalla anterior, le permite crear más dominios utilizando la misma cuenta.

5. En este último paso, solo tendremos que cargar los datos de la cuenta que se creó en el DVR, para eso ingresamos al DVR ya sea de manera directa o a través de la IP local. Recuerde que los puertos deben estar abiertos antes de ingresar a través de la Ip local, si se encuentran abiertos entonces debe teclear la Ip local, dos puntos y el puerto que abrió, por ejemplo: http://192.168.1.100:80

   Una vez ingresando a la interfaz del DVR, damos clic en la opción o icono de “Configuración”, después de clic en la opción o icono de “Red”, y una vez ahí en el apartado de que dice “DDNS” marque el recuadro, y cargue los datos del dominio creado, para esto seleccione de la lista de tipos de DDNS: “mintdns”, el Nombre de usuario que es la cuenta correo utilizo para dar de alta el dominio, la contraseña que utilizo y finalmente el “Host de dominio” que es dominio que dio de alta anteriormente. Figura 3.28

Figura 3.28 Host de dominio

Finalmente de clic en el botón que dice “Prueba”, y que una vez que le muestre el mensaje de “prueba exitosa”, de clic en “Aplicar”. A partir de este momento puede ingresar a su DVR de manera remota únicamente haciendo referencia al DDNS que registro y el o los puertos que abrió, ejemplo: http://examenprofesional.dvrdydns.com:80

3.4.3 Configuración de Gateway o puerta de enlace

Dentro de la configuración de los DDNS en el DVR Meriva, al momento de presionar el botón “Prueba” que realiza el test de la conexión con el dominio registrado, en algunas ocasiones llega a aparecer un mensaje de “Pruebas fallidas”. Figura 3.29

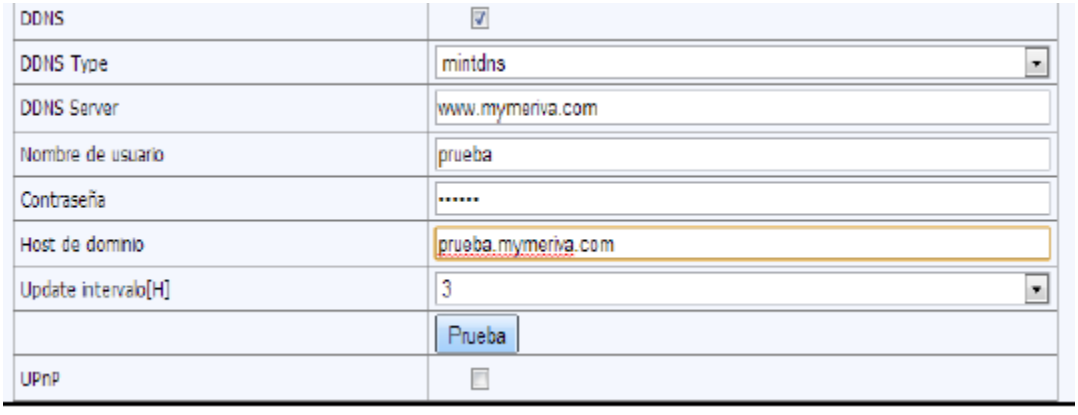


Figura 3.29 Pruebas fallidas

Y para resolver este problema, se sugiere lo siguiente:

- Primero: Se recomienda verificar el “Nombre de usuario”, “Contraseña” y “Nombre de dominio”.
- Segundo: Cuando realice la configuración de la red es necesario que en el grabador se encuentre marcada la opción de:

1. “Obtener una dirección IP automáticamente”

   Esta opción permite obtener todos los parámetros de red y sean asignados de manera automática en el grabador.

2. Es necesario que el parámetro “Puerta de enlace o Gateway” tenga de dirección correcta. Para módems del operador telefonico preponderante, el parámetro normalmente es: 192.168.1.254, Figura 3.30

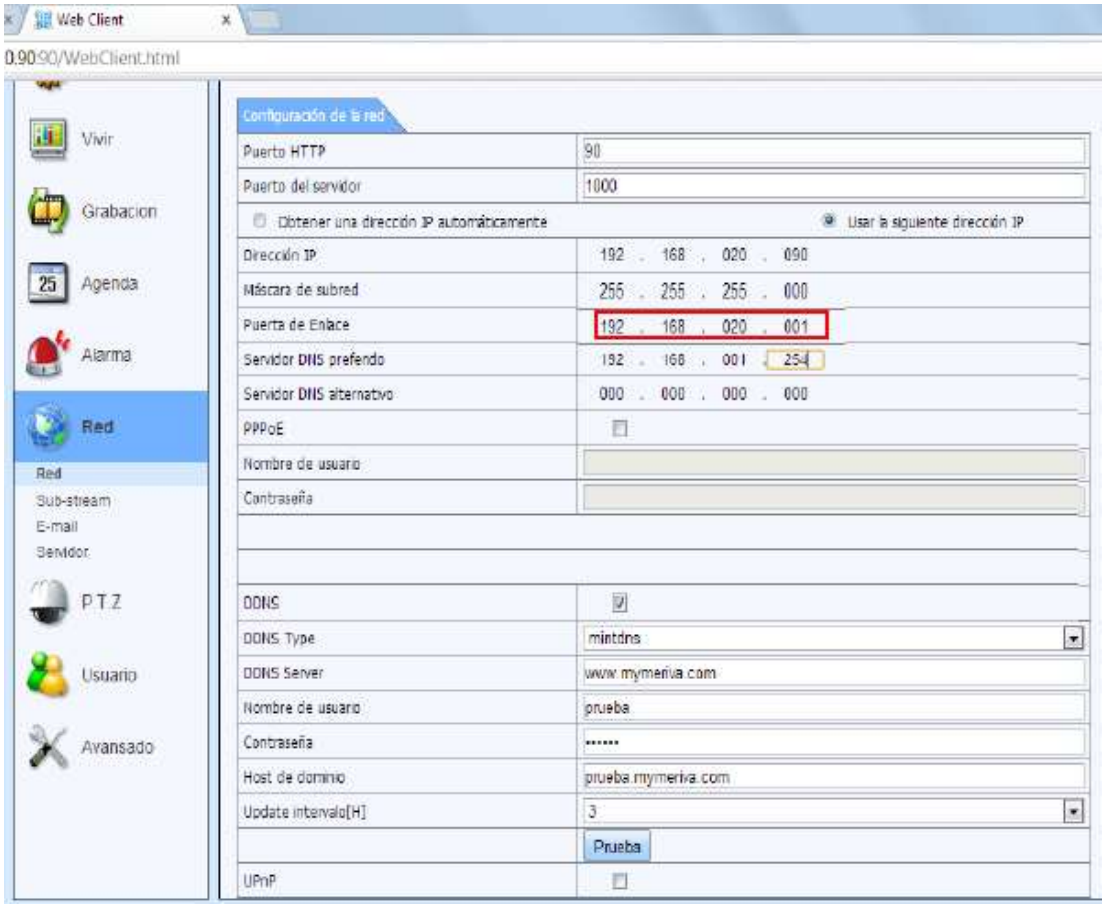


Figura 3.30 IP Automática

Después de que hayan asignado los parámetros de manera automática como:

- Dirección IP
- Mascara de subred
- Puerta de enlace

Entonces debe seleccionar la opción “Usar la siguiente dirección IP”, y esta dirección IP es con la que se abrirán los puertos y la cual debe ser ESTATICA.

3.4.4 Ajuste de imagen

En esta etapa se hacen las configuraciones necesarias en la DVR, ajustes de imagen, modo de grabación, reconocimiento del disco duro, textos individuales de cada canal (nombre de la cámara, ej. cámara 1 = entrada principal), fecha y hora locales, usuarios, entre otros.

Todas estas configuraciones son necesarias para que el sistema obtenga imágenes de calidad y rendimiento máximo de funcionamiento. Figura 3.31

Figura 3.31 Menú principal de una grabadora digital de video.

3.4.5 Conceptos básicos locales

Estos conceptos se refieren a cambios simples como: fecha y hora locales, ajustes de imagen (brillo, saturación, contraste), detección de movimiento, etc. Para nuestro sistema, estos parámetros fueron configurados de manera que la imagen fuera la mejor en pantalla para cada cámara, tomando en cuenta la cantidad de luz que percibe el CCD de la misma, la opción de detección de movimiento se usa con fines de ahorro de espacio en disco duro, es decir, si la grabación la configuramos en este modo, tendremos más días de almacenamiento ya que solo comenzará a grabar cuando se perciba movimiento (esta aplicación es muy útil en la noche porque no debe haber nadie en el lugar y si un intruso entrara ahí sería grabado solo el tiempo que este moviéndose dentro del área de vista de las cámaras, esto aplica para todos los canales de video) en cambio si la grabación es de modo continuo el disco duro se llenará más rápido ya que, estaría grabando aún y cuando no suceda nada.

3.4.6 Conceptos avanzados locales

En estos conceptos entran las configuraciones de alarmas (se pueden incluir en la grabadora sensores de movimiento, contactos magnéticos, sensores de vibración, etc. como entradas y también sirenas, estrobos, etc como salida del sistema), usuarios, grabaciones calendarizadas, parámetros de red, entre otros.

Configuraciones locales básicas de la DVR. Figura 3.32. 3.33 y 3.34

Figura 3.32 Ajustes de cámara.

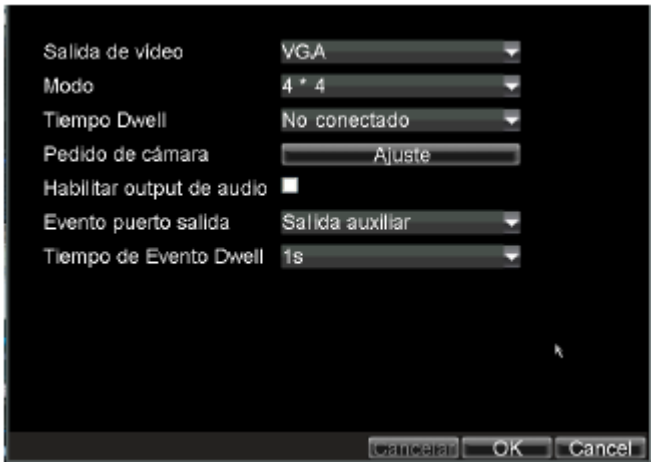


Figura 3.33 Ajustes de pantalla.

Figura 3.34 Ajustes de detección de eventos

En el sistema no se usa el sistema de alarma. Se da de alta solo un usuario en modo jefe – para la administración de usuarios se tienen diferentes niveles, entre ellos están: administrador (es el nivel del instalador, tiene acceso a todos las configuraciones sin excepción), jefe y operador, a estos últimos se les restringen movimientos manualmente, por ejemplo, solo podrían reproducir una grabación localmente pero no pueden descargar el archivo y no tienen acceso a los demás cambios. – el cual estará disponible para el jefe directo del local.

También se hizo la configuración de tipo de resolución de grabación, en la cual usaremos la resolución CIF[4] (Capitulo 2) para tener un mayor tiempo de grabación en el disco duro, si se usara la resolución 4CIF[5] se tendría una mejor calidad de imagen pero se sacrifica espacio en el disco duro, es decir, si con resolución CIF se tienen 15 días de grabación, con la resolución CIF solo se tendrán 7 días de grabación (esto es porque el archivo es más pesado).

3.4.7 Configuraciones de red

Este concepto es muy importante y de gran utilidad, con el sistema configurado en internet el usuario final tiene la ventaja de supervisar su casa o negocio sin tener que estar presente y lo que es mejor aún, puede hacerlo desde cualquier lugar que tenga acceso a internet, solo es necesario introducir una dirección IP, un nombre de usuario y una contraseña para poder accesar al sistema de grabación. Configuraciones locales avanzadas del DVR. Figura 3.35 a) y 3.35 b)

Figura 3.35 a) Ajustes de grabación.

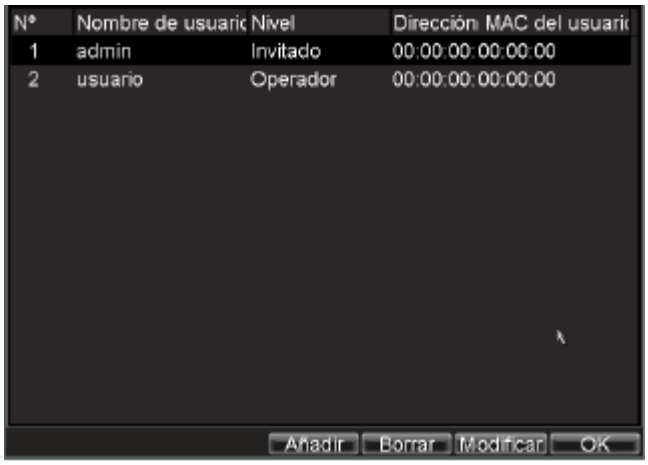


Figura 3.35 b) Ajustes de usuario.

[4] Formato de intercambio común; Tamaño de imagen en pixeles estandarizado por los fabricantes de CCTV en área de DVR'S (352 x 240 pixeles).
[5] Tamaño de imagen de 704 x 480 pixeles estandarizado por los fabricantes de CCTV en área de DVR'S.
http://ftp3.syscom.mx/usuarios/ftp/GUIASEG2014/01_SECCION_SOLUCIONES.pdf
Página recuperada 31 de octubre de 2014

Esta configuración se debe hacer tanto en la DVR como en el servidor que será usado para acceder a la red de internet y así mismo en el router que se usa para el servicio de internet.

Una vez que el DVR se da de alta en el servidor podemos continuar la configuración en el router local, para tener comunicación entre el router y la DVR se necesita hacer la conexión de ambas por medio de un cable de red plano, así automáticamente el router reconoce el dispositivo conectado, después lo que se debe hacer es abrir los puertos que se necesitan para la grabadora (en este caso solo necesitamos abrir los puertos 80 y 8000), dar un nombre al dispositivo (de preferencia el mismo que se da en el DVR).

Al terminar con esta configuración ya se tiene en línea la DVR en la red de internet, para comprobar que en realidad es así, al escribir la dirección IP local en el buscador de internet, debemos tener acceso al monitoreo de las cámaras (con la IP local solo se podrá entrar estando conectados a internet en el mismo lugar).

Si se tiene éxito al ingresar la IP local, entonces ya se puede usar el DDNS para accesar desde cualquier lugar del mundo, para hacer esto solo es necesario ingresar la dirección IP, usuario y contraseña previamente configurados y listo.

Cuando se está monitoreando por medio remoto en internet el usuario tendrá el mismo acceso a los parámetros definidos en la DVR, es decir, si solo esta autorizado para reproducir una grabación, no podrá descargar el archivo y tampoco podrá hacer ajustes en la configuración.

3.4.8 Monitoreo remoto por medio de internet Explorer

Para poder tener acceso al sistema de video vigilancia por medio remoto en internet, se necesita introducir la dirección IP o dirección DDNS (previamente dada de alta en el servidor) en la barra de búsqueda de nuestra interfaz de internet. Por

medio de este método de acceso tenemos varias opciones de navegar en el sistema, entre los movimientos que se pueden hacer son:

- Visualizar en vivo las áreas monitoreadas por las cámaras.
- Configurar ajustes de imagen de cada uno de los canales de video.

Figura 3.36 Visualización por internet

- Reproducción de grabaciones almacenadas en el disco duro de cada una de las cámaras.
- Configuraciones totales del sistema (nombre del equipo, parámetros de red, nombre de la cámara, usuarios, servidor de conexión, etc).
- Respaldar archivos de grabación en una unidad de almacenamiento externo o interno de la computadora.

Después de introducir correctamente los códigos requeridos se tendrá el acceso a la visualización de las cámaras en tiempo real, la interfaz de la aplicación es muy sencilla de operar, ya que se tienen a la mano todos los controles necesarios para su manipulación. Aquí se tiene la opción de elegir el número de imágenes simultáneas que se quieren ver, es decir, se puede elegir ver 1, 4 u 8 imágenes simultáneamente en la pantalla, enseguida se muestra la ventana de visualización

en vivo del sistema. Para nuestro proyecto utilizamos 8 cámaras y así es la visualización. Figura 3.37

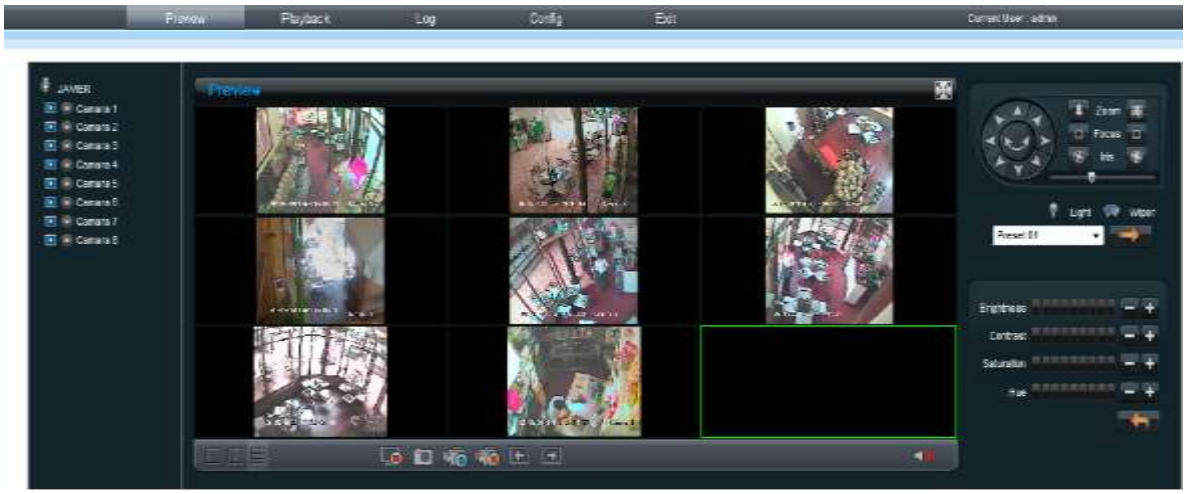


Figura 3.37 Ventana de visualización en vivo de 8 cámaras simultáneamente en modo normal

También se puede visualizar el monitoreo remoto en pantalla completa, con esto se tendrá un tamaño de cuadro de la imagen más grande, por lo tanto, la imagen estará ampliada un poco, en la figura 3.38 se muestra la imagen correspondiente:

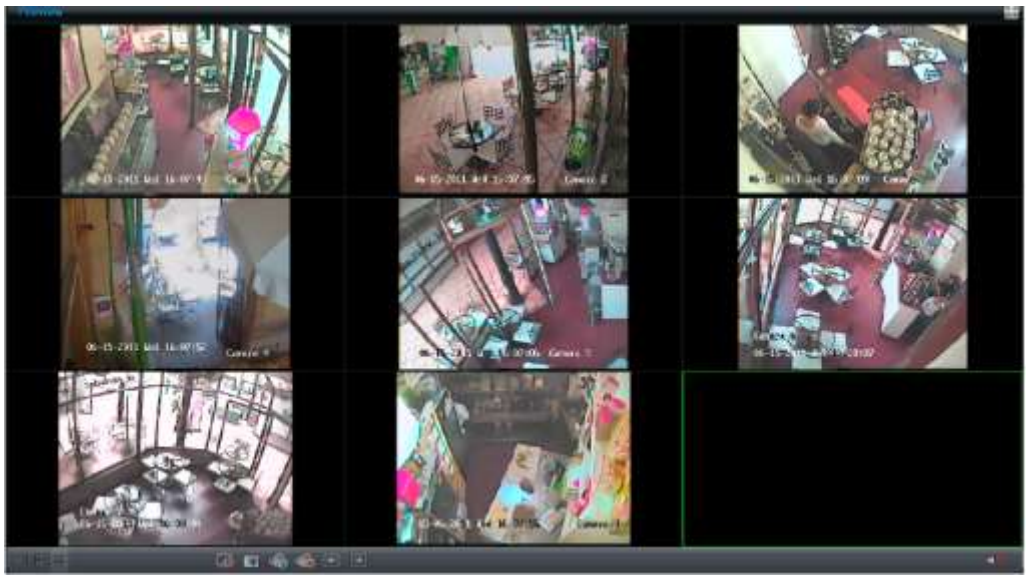


Figura 3.38 Ventana de visualización en vivo de 8 cámaras simultáneamente en modo de pantalla completa.

Si se requiere de revisar eventos pasados de algún canal de video, podemos hacerlo desde este mismo modo de monitoreo remoto, dentro de las opciones que se tienen a disposición del usuario está la de reproducción de videos. En esta opción el usuario puede reproducir un archivo de un evento pasado, ya sea del mismo día o de días anteriores (tiene como límite el marcado según la capacidad de disco duro utilizado. En este caso se utiliza un disco duro de 1000 GB de memoria, suficientes para cubrir 15 días de grabación) de cualquier hora del día. Una desventaja que se tiene en la reproducción de videos por medio remoto es que, solo podemos reproducir el video de un solo canal, es decir, no se pueden reproducir los 8 canales simultáneamente (esto solo aplica para este modelo de DVR). En seguida se muestra la ventana de reproducción de videos de manera remota. Figura 3.39

Figura 3.39 Ventana de reproducción de videos de eventos pasados.

3.5 Vigilancia móvil

También es posible monitorear el sistema por medio de un teléfono celular, existen varios teléfonos denominados smartphones que cuentan con un sistema operativo que soporta el monitoreo de un DVR, soporta vigilancia móvil IPhone, Gphone, BlackBerry o smartphones con Windows Mobile y symbian OS. Al mismo tiempo, es compatible con red 3G.. para activar la vigilancia móvil, necesita

primero activar el servicio de red (punto 3.3.7) a continuación las instrucciones de uso extremo de cliente móvil para dos OS.

3.5.1 Teléfonos con sistema operativo Windows Mobile

1. En primer lugar activar el acceso a la red en el teléfono móvil y luego ejecute "Internet Explorer". Entrada de la dirección del servidor y la conexión se construye a continuación como imagen de la izquierda
2. Click en el nombre del software. Un cuadro de diálogo aparece como debajo de la imagen en el medio
3. Click "Yes" para iniciar la descarga e instalación
4. PCam se abrirá automáticamente después de instalado. Consulte el cuadro a la derecha. Figura 3.40

Figura 3.40 Procedimiento de instalación con Windows M

5. Input dirección del servidor, ID y contraseña respectivamente en las columnas del "Server", "Usuario" y "Contraseña" hacer click en "Go" para iniciar sesión en el servidor. Se mostrará la imagen si accede con éxito. Consulte por debajo de la foto de la izquierda:

6. Camera 1. es el canal por defecto después de inicio de sesión. Cambiar el canal en el menú del balanceo del "Canal": consulte cuadro en la derecha abajo, Figura 3.41

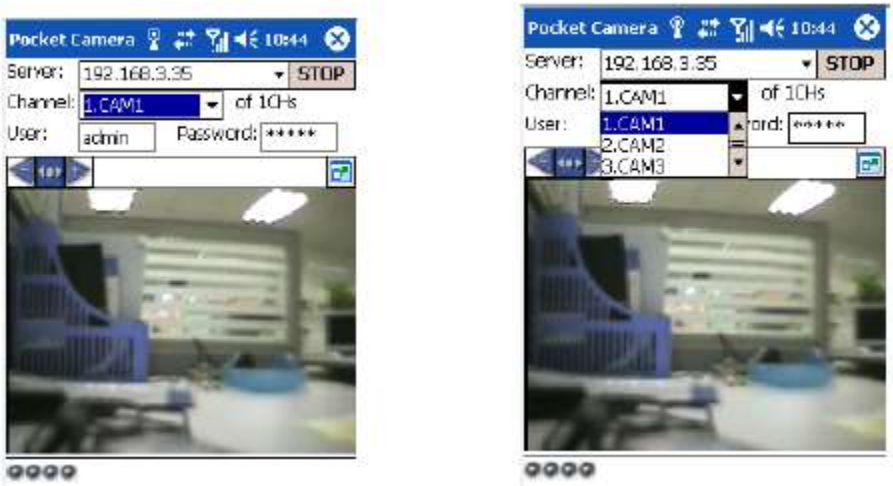


Figura 3.41 Inicio de sesión.

3.5.2 Teléfonos con sistema operativo Symbian

Usar los teléfonos inteligentes con versión Symbian compatible con esta unidad. La información detallada es la siguiente:

Tabla 3.1Version Symbian

Symbian S40	support
Symbian UIQ	support
Symbian S80	support
Symbian S60	support
Symbian S60 3rd Edition-Symbian OS v9.1	support
Symbian S60 3rd Edition with FP 1-Symbian OS v9.2	support
Symbian S60 3rd Edition with FP2-Symbian OS v9.3	support
Symbian S60 5th Edition-Symbian OS v9.4	support
Symbian S60 5.1 Edition-Symbian OS v9.5	support

1. En primer lugar permitir el acceso a la red de telefonía móvil. Luego ejecute el navegador Web.

2. Input dirección IP del servidor DVR en un marcador de nueva construcción. Haga click en este marcador para conectarse a la DVR. Consulte el cuadro a la izquierda.
3. La ventana de bienvenida se abrirá y requiere un paquete. Haga clic en el nombre del software para descargar. Consulte el cuadro a la derecha:

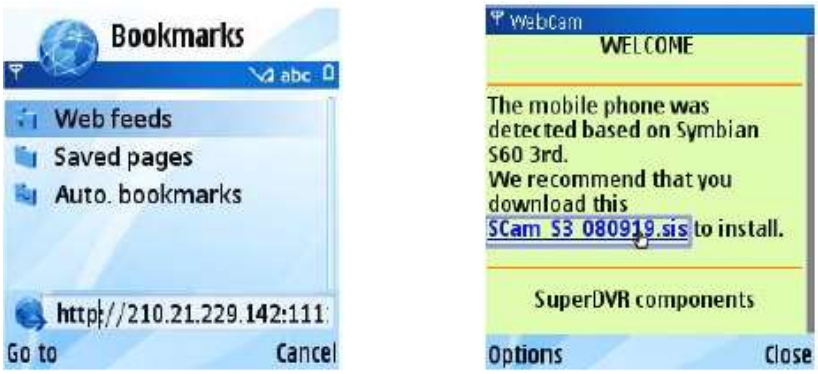


Figura 3.42 Dirección IP

4. Aparecerá una ventana de seguridad se abrirá después de la descarga y pregunte si instalar el paquete. Haga clic en Sí para instalar.
5. Un icono de acceso directo Scam aparece en el menú del sistema después de terminado.
6. Ejecutar programa de estafa. Entrará una interfaz de función. Consulte la imagen de la izquierda:
7. Haga click en Configuración del sistema ---> Config inic para entrar en la interfaz de inicio de sesión. Consulte la imagen de la derecha:

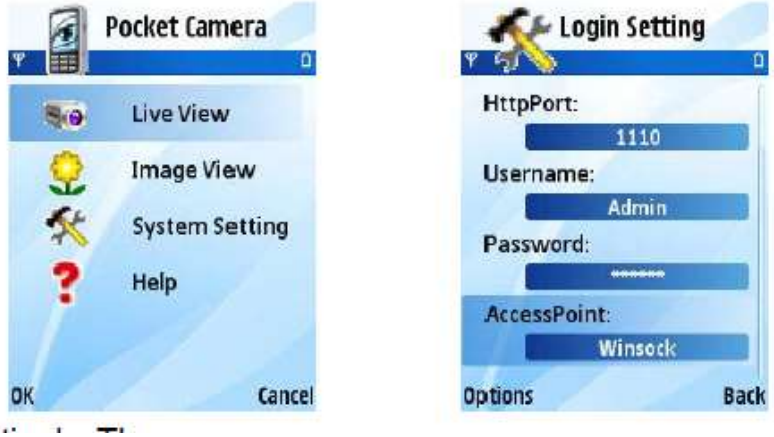


Figura 3.43 Configuración del sistema

8. Introducir la dirección del servidor, el ID y la contraseña, respectivamente. A continuación, guarde.
   - Sobre el punto de acceso, puede haber diferentes puntos de acceso en diferentes países o de los proveedores de servicios.
9. Ingrese Live View, se conectará al servidor e imágenes para mostrar. Consulte la imagen de la izquierda:
   - nombre de usuario y contraseña son los mismos que los utilizados en el DVR. El valor predeterminado es admin y 123456.
10. En Live View, los usuarios pueden hacer instantáneas, cambiar de canal y control PTZ. Consulte la imagen de la derecha. Figura 3.44

Figura 3.44 Inicio de sesión.

3.5.3 Instalación de software para los clientes móviles de iPhone

1. Instalar a través de iphone.
   a) función Open App Store de iPhone
2. Activar la función "Buscar" para buscar "SuperLive"
3. Haga click en SuperLive, dar clikcven "introduce" y en "FREE", cambiar en "INSTALL"

Figura 3.45 Habilitación del IPhone.

4. Introducir la contraseña de iTunes Store y luego haga clic en "Aceptar", el software se instalará automáticamente. Nota: si se trataba de la primera vez que el usuario funcione, por favor, introduzca su ID de usuario; si no hay ninguna cuenta de la tienda, el usuario tiene que aplicar uno.
5. Instalar a través de PC

Figura 3.46 Instale iTunes en PC y luego Iniciar sesión

Figura 3.47 Conecte el IPhone de la PC.

Figura 3.48 Activar la función "Buscar" para buscar "Superlive"

Figura 3.49 Haga clic en botón "aplicación gratuita

6. Introducir ID de Apple y contraseña, a continuación, haga clic en "adquirir": botón de marcar la casilla "sincrónicamente aplicar programa" y "SuperLive", y luego haga clic en "aplicar"

Figura 3.50 Login interface

【Playback】	playback record file	【Image】	image view
【Log】	log record	【Server List】	device list
【Live】	live view	【Settings】	software setting
【Information】	device information view	【Help】	software help center
【Logoff】	logoff and return to login interface		

Figura 3.51 Interfaz principal

Figura 3.52 Live View Interface.

3.5.4 Método de instalación y de operación para los clientes móviles Android

Instalación de Software

Figura 3.53 Ejecutar el programa de Google

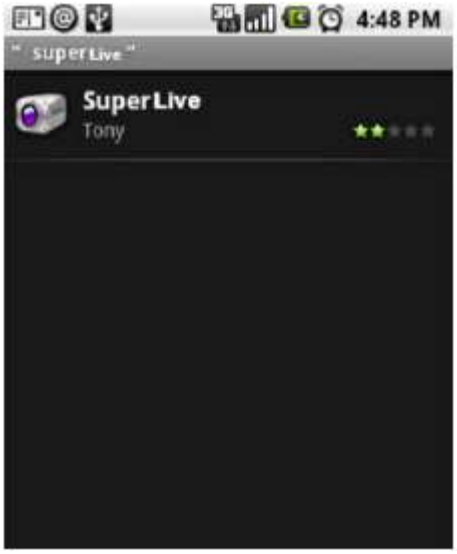


Figura 3.54 Habilitar "SuperLive"

Figura 3.55 Presione Install

Figura 3.56 Presione Ok

Puede ver el proceso de descarga e instalación en las notificaciones; cuando la descarga haya finalizado, el software se instalará automáticamente.

Figura 3.57 Proceso de descarga del Software

Entrar en la dirección IP del servidor (o nombre de dominio), ID de usuario y contraseña. Haga clic en "Remenber Server " para guardar la configuración; hacer click en el botón e introduzca, nombre de usuario y contraseña

Figura 3.58 Inserte el Login.

A continuación observe las imagines de la cámara en tiempo real

Figura 3.59 Vista en vivo.

Terminada la instalación y ajuste de parámetros en las configuraciones, el responsable del proyecto tiene la obligación de asesorar al(los) usuario(s) en el uso de la DVR, los conceptos principales que debe dar a conocer en el uso del sistema local son: reproducción de una grabación, extender un canal de video en pantalla, visualizar el número total de canales en pantalla, respaldo de archivos de video en dispositivos externos (USB, CD/DVD RW, disco duro externo USB).

Del mismo modo, debe dar a conocer el uso del sistema remoto, los conceptos principales son: cómo entrar a la página designada, cómo visualizar las imágenes en tiempo real, cómo reproducir una grabación, cómo descargar un archivo de video, cómo salir del sistema. El usuario debe quedar convencido de la capacitación que se le proporciona, ya que él será el encargado de usar y administrar el sistema de ahora en adelante.

3.5 Presupuesto del proyecto

ALEVALDI
CAMARAS DE VIGILANCIA Y SISTEMAS DE SEGURIDAD

Hacienda de Enmedio #10 Col. Impulsora
Cd. Nezahualcóyotl, Edo. Méx. CP. 57130
RFC: VADU750104V6A

Tels. (55)5780-2452
(55)5710-2682
www.alevaldi.com.mx
grupoalevaldi@hotmail.com

México D.F. a 13 de septiembre de 2014

Asunto: Cotización para proyecto de 8 cámaras de seguridad a CCTV a 700 TVL de Resolución..

At´n. De Haro Pérez Alma Viridiana
P R E S E N T E

A través de la presente, me permito hacer llegar a usted el siguiente presupuesto solicitado, que consta de lo siguiente:

Presupuesto de Proyecto

Código	Concepto	Unidad	Costo	Cantidad	Importe
01	DVR marca Meriva Security 8CH Video, 4CH Audio, 1 Salida de Audio, 240 fps, HDMI, Multiplex, soporta hasta un máximo de 2 Tbytes en HDD.	Pza	$3,500.00	1	$3,500.00
02	Cámara marca Meriva Security 700 TVL, IR 24 leds., tipo Bullet o Domo, Antivandálica, CCD Sony Effio 1/3"	Pza	$2,000.00	8	$16,000.00
03	Fuente de Poder 12 Volts, 5 Amp tipo Laptop marca Enson	Pza	$350.00	2	$700.00
04	Monitor 15.6" marca HP o Lenovo (según existencias), tecnología LED Pantalla Plana.	Pza	$1,500.00	1	$1,500.00
05	Disco Duro 2 Terabytes SATA II, 7200 rpm para respaldo de 2 meses.	Pza	$1,900.00	1	$1,900.00
06	Transductores pasivo para acoplamiento de señal de video	Pza	$100.00	16	$1,600.00
07	Cableado y protección con tubería (o Canaleta según se requiera).	Pza	$4,000.00	1	$4,000.00

Subtotal = $29,200.00
16% IVA = $4,672.00

TREINTA Y TRES MIL OCHOCIENTOS SETENTA Y DOS PESOS 00/100 M.N. **Total = $33,872.00**

(Si no requiere factura, favor de no considerar el 16% de IVA)

Incluye estructura para montar monitor a muro. Dominio y configuración de Smartphones para monitoreo remoto. Capacitación del personal que operará el sistema.

CONDICIONES DE PAGO: 50% al iniciar y 50% al término del proyecto.

GARANTIA: Garantía de 1 año en mano de obra y 1 año en equipo contra defecto de fábrica.
ENTREGA: La fecha de entrega será de 4 dias hábiles.

NOTA: LOS PRECIOS NO INCLUYEN TRABAJOS DE ALBAÑILERIA, RANURAS EN MUROS,HERRERIA, ELECTRICIDAD. ETC.

SIN MAS POR EL MOMENTO QUEDO DE USTED PARA CUALQUIER DUDA O ACLARACION.

Atentamente ALEVALDI

Ing. Quijano Bazán Héctor Abraham

Conclusiones

Antes de invertir una importante parte del tiempo y recursos financieros en la instalación de equipamiento de vigilancia por video dentro de su empresa, el empleador debería planificar prudentemente su instalación. De hecho, la ley está en permanente evolución y en la actualidad existen muy pocos ejemplos jurisprudenciales en los cuales confiar para la aplicación de los criterios arriba mencionados.

- Primero, debe preguntarse a sí mismo acerca de la necesidad de proceder con esa instalación a los efectos de proteger su empresa.
- En segundo lugar, el empleador debe delimitar cuáles son sus necesidades y el alcance de éstas a los efectos de asegurarse de que la intrusión a sus empleados se reduzca a su mínima expresión. Asimismo, a los efectos de evitar posibles conflictos, el empleador puede en determinadas circunstancias, informar a sus empleados acerca de las ubicaciones exactas en las que se instalarán las cámaras y con qué objeto. De este modo los empleados podrían tener la opción de alejarse del campo visual de las cámaras si quisieran proteger su privacidad.

Las razones por la cual instalar un sistema de CCTV en una empresa o una casa habitación. Al planificar es importante estar al tanto de todos los beneficios posibles para aprovecharlos al máximo. Hay que evaluar bien los objetivos, y tomar en cuenta todas las funciones de los sistemas actuales para que la empresa planifique mejor la inversión, y de una vez considere cambios en procesos y efectividad a largo plazo.

Los sistemas de videovigilancia pueden ser sencillos o avanzados. Existen sistemas digitales de segunda generación que sencillamente ofrecen grabación digital con monitoreo vía redes, y sistemas inteligentes que ofrecen más ventajas y por lo tanto más beneficios.

Para empresas grandes normalmente los objetivos son mayores, y necesitan obtener más beneficios y mejorar varias áreas, y deben considerar sistemas más avanzados, que dan mayores beneficios, y que paga la inversión más rápido.

Para poder aprovechar los beneficios posibles de un sistema de seguridad, prevenir y controlar riesgos y pérdidas, es importante cooperar con un proveedor profesional, que tiene la experiencia y el conocimiento necesario en el área y que se transforme en un socio tecnológico del futuro, con soportes técnicos, mantenimiento y actualizaciones futuras.

Podemos concluir que Las soluciones de video seguridad ayudan a proteger las personas e instalaciones, a prevenir las pérdidas y daños, y a mejorar la eficiencia de sus negocios. a continuación se enumeran los beneficios al implementar este tipo de sistema de vigilancia

1. **Disuadir a la delincuencia**. Si se esta está preocupado por los altos índices de delincuencia, las cámaras de seguridad no sólo sirven para sorprender a los criminales en el acto, también actúa como medio de disuasión ante algún evento delictivo.
2. **Prevenir el robo de los empleados**. "Incluso los mejores empleadores pueden cometer un error". El instalar cámaras de seguridad cerca de las cajas registradoras o en otros lugares como depósitos, almacén, etc. donde los empleados suelen realizar sus tareas, no solo puede mostrar si está siendo robando, sino que puede disuadir a un empleado de cometer el hecho al saberse observado.
3. **Ser utilizados como evidencia**. Si se comete un delito en o alrededor de su negocio y la persona acusada de cometer el hecho fue captado por la cámara, se cuenta con esta herramienta como evidencia para un juicio.
4. **Ayudar a la policía a resolver crímenes**. Este es probablemente uno de los mayores motivos por los cual se utilizan cámaras en las empresas o negocios. La policía y otros agentes del orden público puede utilizar este material (vídeo o fotos) para difundir en diferentes medios, ya que el contar

con una imagen del sospechoso puede hacer un mundo de diferencia cuando se trata de hacer un arresto y conseguir la captura de un criminal.

5. **Mantener su negocio siempre bajo control**. Si no puede estar en la oficina todo el tiempo pero quisiera saber lo que está pasando, una cámara de seguridad puede ayudar a hacer justamente eso. Mantiene al tanto de todo lo que ocurre en su empresa o negocio con tan solo unos clics en su computadora o dispositivo móvil (smartphone) y asegurar que su negocio está funcionando bien y que nada fuera de lo común está sucediendo.

A pesar que a nivel mundial la base instalada de cableado para CCTV usa cable coaxial y protocolos análogos, el crecimiento de las comunicaciones usando protocolo IP sobre cable UTP es mucho mayor que el de tipo coaxial.

Los anchos de banda de las nuevas categorías de cableado estructurado y sus altas velocidades de transmisión facilitan el uso de esta plataforma para extraer el máximo provecho a cada CCTV con una relación de costo sobre la inversión razonable, por ese motivo recomendamos siempre trabajar en equipo con el ánimo de conseguir la satisfacción del usuario en su CCTV.

Anexo
Normatividad

La videovigilancia y la protección de los datos personales en la Ciudad de México
A nivel global, las tecnologías de la información y los medios de comunicación han observado vertiginosos avances durante las últimas dos décadas. Herramientas eficaces en la transmisión y difusión de todo tipo de información son utilizadas actualmente. Ya no sorprende el hecho de que los flujos de datos de carácter personal, ya sea entre entidades privadas y públicas, en entornos de corte doméstico e internacional.

Sin duda, la Ciudad de México no es la excepción de este sello distintivo de la sociedad digital ya que, por ejemplo, desde finales del año de 2008 se puso en operación el ambicioso Proyecto Bicentenario, ahora denominado Centro de Atención a Emergencias y Protección Ciudadana de la Ciudad de México, consistente inicialmente en la instalación de más de 8 mil cámaras de videovigilancia en vía pública, conectadas a una red primaria o anillo de fibra óptica, y que a la fecha se cuenta con 10 mil 956 cámaras de un total final de 11 mil 592 (192 para control de tránsito, 3 mil 312 en 175 estaciones de las 11 líneas del STC-Metro y 7 mil 452 urbanas distribuidas en las 16 delegaciones políticas).

Este proyecto tecnológico, adicionalmente, incluye botones de emergencia y altavoces para poder interactuar con la ciudadanía y con ello fortalecer el nivel de vigilancia y la acción policial, ya que al realizarse un trabajo coordinado de más de 45 áreas de gobierno, el tiempo de respuesta se delimita en tan sólo 5 minutos desde el momento en que la autoridad toma conocimiento de la emergencia o del acto ilícito. Previo a su instrumentación, las autoridades capitalinas analizaron cuidadosamente las estrategias de videovigilancia que se implementaron en distintas ciudades como Jerusalén, Londres, Liverpool, Singapur, París, Baltimore, Chicago, Medellín y Bogotá.

LEY QUE REGULA EL USO DE TECNOLOGÍA PARA LA SEGURIDAD PÚBLICA DEL DISTRITO FEDERAL

MARCELO LUIS EBRARD CASAUBON, Jefe de Gobierno del Distrito Federal, a sus habitantes sabed:
Que el H. Asamblea Legislativo del Distrito Federal, IV Legislatura se ha servido dirigirme el siguiente:

DECRETO

(Al margen superior izquierdo un sello con el Escudo Nacional que dice: ESTADOS UNIDOS MEXICANOS.- **ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL, IV LEGISLATURA**)

ASAMBLEA LEGISLATIVA DEL DISTRITO FEDERAL
IV LEGISLATURA.

D E C R E T A

DECRETO POR EL QUE SE EXPIDE LA LEY QUE REGULA EL USO DE TECNOLOGÍA PARA LA SEGURIDAD PÚBLICA DEL DISTRITO FEDERAL.

ÚNICO.- Se expide la Ley que Regula el Uso de Tecnología para la Seguridad Pública del Distrito Federal, para quedar como sigue:

LEY QUE REGULA EL USO DE TECNOLOGÍA PARA LA SEGURIDAD PÚBLICA DEL DISTRITO FEDERAL.

CAPÍTULO I
DISPOSICIONES GENERALES

Artículo 1.- Las disposiciones de esta Ley son de orden público e interés social y de observancia general en el Distrito Federal y tienen por objeto:

- **I.** Regular la ubicación, instalación y operación de equipos y sistemas tecnológicos a cargo de la Secretaría de Seguridad Pública del Distrito Federal;
- **II.** Contribuir al mantenimiento del orden, la tranquilidad y estabilidad en la convivencia así como prevenir situaciones de emergencia o desastre e incrementar la seguridad ciudadana;
- **III.** Regular la utilización de la información obtenida por el uso de equipos y sistemas tecnológicos en las materias de seguridad pública y procuración de justicia; y
- **IV.** Regular las acciones de análisis de la información captada con equipos o sistemas tecnológicos para generar inteligencia para la prevención de la delincuencia e infracciones administrativas.

Artículo 2.- Para los efectos de esta Ley, se entenderá por:

- **I.** Cadena de Custodia: al documento oficial donde se asienta la obtención de información por el uso de equipos y sistemas tecnológicos por la Secretaría así como sus características específicas de identificación; con el objeto que cada persona o servidor público a la que se le transmite la información, suscriba en la misma su recepción así como toda circunstancia relativa a su inviolabilidad e inalterabilidad, haciéndose responsable de su conservación y cuidado hasta su traslado a otra persona o servidor público;
- **II.** Conductas Ilícitas de alto impacto: aquellas que tengan amplia repercusión por su recurrencia y cercanía con el entorno familiar y vecinal;

III. Equipos tecnológicos: al conjunto de aparatos y dispositivos, para el tratamiento de voz o imagen, que constituyen el material de un sistema o un medio;

IV. Instituciones de Seguridad Pública: a la Secretaría de Seguridad Pública y Procuraduría General de Justicia, que como dependencias del ámbito local del Distrito Federal, por sus funciones legales les compete la prevención, investigación y persecución de delitos e infracciones administrativas;

V. Inteligencia para la prevención: al conocimiento obtenido a partir del acopio, procesamiento, diseminación y aprovechamiento de información, para la toma de decisiones en materia de Seguridad Pública competencia del Distrito Federal;

VI. Ley: a la Ley que regula el Uso de Tecnología para la Seguridad Pública del Distrito Federal;

VII. Medio: al dispositivo electrónico que permite recibir y/o transmitir información para apoyar las tareas de seguridad pública;

VIII. Procuraduría: a la Procuraduría General de Justicia del Distrito Federal;

IX. Registro: al Registro de Equipos y Sistemas Tecnológicos para la Seguridad Pública;

X. Reglamento: al Reglamento de la Ley que Regula el Uso de Tecnología para la Seguridad Pública del Distrito Federal;

XI. Secretaría: a la Secretaría de Seguridad Pública del Distrito Federal;

XII. Sistema tecnológico: al conjunto organizado de dispositivos electrónicos, programas de cómputo y en general todo aquello basado en tecnologías de la información para apoyar tareas de seguridad pública; y

XIII. Tecnología: conjunto de técnicas de la información, utilizadas para apoyar tareas de seguridad pública.

Artículo 3.- Se crea el Registro de Equipos y Sistemas Tecnológicos para la Seguridad Pública, a cargo de la Secretaría, que integrará el registro de aquellos cuya instalación y operación previa deba ser inscrita en el mismo, de conformidad con la presente Ley y otras disposiciones aplicables.

La organización del Registro estará prevista en el Reglamento.

CAPITULO II
DE LOS LINEAMIENTOS A QUE SE SUJETARÁ LA COLOCACIÓN DE TECNOLOGÍA

Artículo 4.- La instalación de equipos y sistemas tecnológicos, se hará en lugares en los que contribuya a prevenir, inhibir y combatir conductas ilícitas y a garantizar el orden y la tranquilidad de los habitantes del Distrito Federal.

La ubicación estará basada en los criterios y prioridades establecidos en la presente Ley.

Artículo 4 Bis.- Los equipos y sistemas tecnológicos instalados al amparo de la presente Ley, no podrán ser retirados bajo ninguna circunstancia.

Exceptuará lo establecido en el párrafo anterior, solo en aquellos casos en los que la Secretaría previa consulta y autorización de la demarcación territorial correspondiente, determine que los equipos y sistemas tecnológicos instalados, ya sea por su ubicación o sus características:

I. No contribuyen a los objetivos establecidos en el artículo 1, fracción II de la Ley.

II. Se determine un deterioro físico que imposibilite el adecuado cumplimiento de sus funciones, en cuyo caso deberá repararse o sustituirse en un término no mayor a 30 días naturales.

Artículo 4 Ter.- Cuando la inversión realizada por el Gobierno del Distrito Federal en la instalación de equipos y sistemas tecnológicos o cualquier infraestructura que se encuentre dentro del marco de regulación de esta ley, sea superior a los cinco mil días de salario mínimo vigente en el Distrito Federal, no podrá ser modificada o retirada sin previo informe a la Contraloría General del Distrito Federal en el que se justifique dicha acción.

Artículo 5.- Queda prohibida la colocación, de equipos y sistemas tecnológicos al interior de los domicilios particulares, así como aquella instalada en cualquier lugar, con el objeto de obtener información personal o familiar, por parte de la Secretaría.

Sólo podrán ser instalados, sin previa autorización, los equipos tecnológicos fijos en bienes del dominio público o bienes del dominio privado del Distrito Federal. Para la instalación en cualquier otro lugar, se requerirá autorización por escrito del propietario o poseedor del lugar donde se pretenda ubicar los equipos y sistemas tecnológicos.

Dicha autorización será clasificada como confidencial y deberá resguardarse junto con la información obtenida por esos sistemas tecnológicos, de conformidad con lo dispuesto en la presente Ley y la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Artículo 5 Bis.- Queda prohibida la colocación de propaganda, mantas, lonas, carteles, espectaculares, estructuras, señalizaciones y en general, cualquier objeto que impida, distorsione, obstruya o limite el cumplimiento de las funciones de los equipos y sistemas tecnológicos.

Artículo 6.- Podrán solicitar que la Secretaría, bajo su operación, resguardo y presupuesto, instale equipos y sistemas tecnológicos para la seguridad pública en los bienes de uso común del Distrito Federal:

I. El Titular de la Procuraduría, a propuesta de los Subprocuradores, Fiscales Desconcentrados y Centrales de Investigación y de Procesos así como del Director General de Política y Estadística Criminal;

II. La Consejería Jurídica y de Servicios Legales, con información a propuesta de los Jueces Cívicos;

III. Otras Dependencias de la Administración Pública Local del Distrito Federal, que justifiquen la necesidad de su instalación, para prevenir situaciones de emergencia o desastre, o incrementar la seguridad ciudadana; y

IV. Los Jefes Delegacionales, a la propuesta de los Comités de Seguridad Pública de sus correspondientes demarcaciones.

Artículo 7.- Para la instalación de equipos y sistemas tecnológicos en bienes del dominio público del Distrito Federal, la Secretaría tomará en cuenta los siguientes criterios:

I. Lugares registrados como zonas peligrosas;

II. Áreas públicas de zonas, colonias y demás lugares de concentración o afluencia de personas, o tránsito de las mismas, registradas en la estadística criminal de la Secretaría y de la Procuraduría, con mayor incidencia delictiva;

III. Colonias, manzanas, avenidas y calles, que registran los delitos de mayor impacto para la sociedad;

IV. Intersecciones más conflictivas así clasificadas por la Subsecretaría de Control de Tránsito de la Secretaría de Seguridad Pública del Distrito Federal, en las 16 Delegaciones del Distrito Federal;

V. Zonas registradas con mayor incidencia de infracciones a la Ley de Cultura Cívica; y

VI. Zonas con mayor vulnerabilidad a fenómenos de origen natural o humano. La definición de los lugares de ubicación de equipos tecnológicos, se basará en la inteligencia para la prevención, las herramientas para la toma de decisiones, comprendidas por Atlas Delincuencial, el Atlas de Riesgos, las intersecciones más conflictivas, los índices delictivos, destacando las conductas ilícitas de alto impacto y su incidencia delictiva, las zonas peligrosas, los índices de percepción de seguridad, los registros de llamadas de denuncias así como por cualquier otro instrumento de análisis, diferente de la inteligencia para la prevención, que permita la toma de decisiones en materia de seguridad pública, y demás información que posibilite su adecuada colocación, para el cumplimiento de sus finalidades.

Artículo 8.- La solicitud se hará por escrito dirigida a la Secretaría, la que determinará lo procedente de conformidad con los criterios a que hace referencia el artículo anterior.

Una vez cumplidos los requisitos previstos en esta Ley, la Secretaría dará prioridad a la instalación en las zonas escolares, recreativas y lugares de mayor afluencia de público.

Artículo 9.- La información generada por la utilización de los equipos y sistemas tecnológicos, en poder de la Secretaría, podrá ser preservada en la forma y plazos dispuestos en el Reglamento de esta Ley, especialmente la que sean utilizada en un procedimiento a los que se refiere el artículo 15 de esta Ley.

CAPÍTULO III
DE LOS CENTROS DE CONTROL, COMANDO, CÓMPUTO Y COMUNICACIONES.

Artículo 10.- El Gobierno del Distrito Federal instalará los Centros de Control, Comando, Cómputo y Comunicaciones, para el manejo de la información obtenida con equipos y sistemas tecnológicos, los cuales estarán operados y coordinados por la Secretaría y sujetos a la regulación de esta Ley.

Artículo 11.- Los Centros de Comando y Control en las Demarcaciones Territoriales del Distrito Federal, serán operados, coordinados e instalados por la Secretaría, a través de los Centros de Control, Comando, Cómputo y Comunicaciones existentes; pero en todos los casos existirá representación de la autoridad Delegacional correspondiente, para los asuntos que recaigan en el ámbito de su competencia. Se coordinarán y compartirán información con otras instancias, en los términos de la presente Ley y el Reglamento.

Artículo 12.- Las áreas de la administración pública central, desconcentrada y paraestatal del Gobierno del Distrito Federal y las Instituciones Privadas que instalen y operen equipos o sistemas tecnológicos, dentro de un Centro de Control, Comando, Cómputo y Comunicaciones, o dentro de un Centro de Comando y Control, requerirán justificar su participación, su aportación al mantenimiento del orden y tranquilidad en la convivencia social, así como el tipo de servicio que dará a la población.

Artículo 13.- Los equipos y sistemas tecnológicos utilizados por las áreas de la administración pública central, desconcentrada y paraestatal del Gobierno del Distrito Federal y las Instituciones Privadas que operen en los Centros de Control, Comando, Cómputo y Comunicaciones, o dentro de un Centro de Comando y Control, deberán incorporarse al Registro, en términos del artículo 3 de la presente Ley.

Las Instituciones de Seguridad Pública deberán unificar sus equipos y sistemas tecnológicos entre sí; procurarán que estos equipos y sistemas tecnológicos estén homologados con las bases de datos metropolitanas y nacionales que se establezcan en el marco del Sistema Nacional de Seguridad Pública.

El Reglamento normará la actuación y coordinación de las Dependencias del Distrito Federal y las Instituciones Públicas y Privadas en los Centros a que hace referencia el párrafo anterior, de conformidad con esta Ley y otras disposiciones aplicables.

CAPÍTULO IV
DEL USO DE TECNOLOGÍA EN LA SEGURIDAD PÚBLICA

Artículo 14.- Para el óptimo aprovechamiento y oportuna actualización de los equipos y sistemas tecnológicos, el Gobierno del Distrito Federal establecerá el Consejo Asesor en Ciencia y Tecnología para la Seguridad Pública, constituido por los Titulares de las áreas tecnológicas de las Instituciones de Seguridad Pública así como del área que designe el Director del Instituto de Ciencia y Tecnología del Distrito Federal o bien que sea creada para ese efecto por la Junta Directiva del Instituto de Ciencia y Tecnología del Distrito Federal.

Las funciones del Consejo Asesor en Ciencia y Tecnología para la Seguridad Pública, serán las siguientes:

I. Diseñar políticas para la adquisición, utilización e implementación de equipos y sistemas tecnológicos por la Secretaría y la Procuraduría General de Justicia del Distrito Federal;

II. Asesorar las labores que el Instituto de Ciencia y Tecnología realice en el Comité de Autorizaciones de Adquisiciones, Arrendamiento y Prestación de Servicios de la Secretaría, siempre y cuando se relacionen con la adquisición de Tecnología para la misma;

III. Atender las consultas que, en materia de ciencia y tecnología para la seguridad pública, solicite el Jefe de Gobierno por sí o a través de las Instituciones de Seguridad Pública;

IV. Emitir opinión sobre los procesos, equipos y sistemas tecnológicos para una segura, eficiente, debida y sustentable destrucción de la información a que hace referencia esta Ley; y

V. Las demás que se señalen en el Reglamento de la presente Ley.

Artículo 15.- La información materia de esta Ley, compuesta por imágenes o sonidos captados equipos o sistemas tecnológicos, sólo pueden ser utilizados en:

I. La prevención de los delitos, principalmente, a través de la generación de inteligencia para la prevención y de las herramientas para la toma de decisiones en materia de seguridad pública;

II. La investigación y persecución de los delitos, especialmente aquella información que la Secretaría debe poner del conocimiento de la autoridad ministerial, ya sea para sustentar una puesta a disposición o por requerimiento de ésta, al constar en ella la comisión de un delito o circunstancias relativas a esos hechos;

III. La prevención de infracciones administrativas, principalmente a través de la generación de inteligencia para la prevención y de las herramientas para la toma de decisiones en materia de seguridad pública;

IV. La sanción de infracciones administrativas, especialmente aquella información que la Secretaría debe poner del conocimiento del Juez Cívico u otra autoridad administrativa competente, ya sea para sustentar una puesta a disposición o por requerimiento de ésta, conforme a los plazos que permita el procedimiento que se ventile, al constar en ella la comisión de una falta administrativa o circunstancias relativas a esos hechos;

V. La justicia para adolescentes, principalmente a través de la generación de inteligencia para la prevención y de las herramientas para la toma de decisiones de seguridad pública, relativas a adolescentes, así como de la información obtenida con equipo o sistemas tecnológicos que la Secretaría deba poner del conocimiento de la autoridad ministerial especializada, ya sea para sustentar una puesta a disposición o por requerimiento de ésta, al constar en ella la comisión de una conducta sancionada como delito en las leyes penales y cometida por una persona que tenga entre doce años cumplidos y menos de dieciocho años de edad, o bien que se aprecien circunstancias relativas a esos hechos; y

VI. Reacción inmediata, preferentemente a través de los procedimientos que se establezcan en la Secretaría, para actuar, de forma pronta y eficaz, en los casos en que, a través de la información obtenida con equipos y sistemas tecnológicos, se aprecie la comisión de un delito o infracción administrativa y se esté en posibilidad jurídica y material de asegurar al probable responsable, de conformidad con la Ley que regula el Uso de la Fuerza de los Cuerpos de Seguridad Pública del Distrito Federal.

Artículo 16.- La información a que se refiere esta Ley no podrá obtenerse, clasificarse, analizarse, custodiarse o utilizarse como medio de prueba en los siguientes supuestos:

I. Cuando provenga de la intervención de comunicaciones privadas, salvo cuando sea autorizada por la autoridad judicial federal de conformidad con la Constitución Política de los Estados Unidos Mexicanos y las leyes secundarias;

II. Cuando se clasifique, analice, custodie, difunda o distribuya en contravención a la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal; y

III. Cuando se obtenga al interior de un domicilio o violente el derecho a la vida privada de las personas, excepto en los casos de flagrancia o mandamiento judicial, en cuyo caso, deberá observarse lo siguiente:

a) Si con el uso de equipos o sistemas tecnológicos se obtiene información que violente esta disposición, la Secretaría, de forma oficiosa y expedita, deberá destruir la misma, motivando la razón de tal hecho, asegurándose de que no sea archivada, clasificada, analizada o custodiada de forma alguna; y

b) En el supuesto de que, junto con información relevante para la seguridad pública, obtenida con el uso de equipos o sistemas tecnológicos, a que hace referencia el artículo anterior, se obtuviere información que afecte los derechos preservados en esta fracción y dicha parte no pueda ser eliminada por riesgo a afectar la integridad de la información, la Secretaría clasificará sólo esa parte como confidencial y le dará el trato correspondiente, de conformidad con esta Ley y la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Artículo 17.- Los particulares que así lo deseen podrán conectar sus equipos y sistemas tecnológicos privados al sistema que para el efecto instale la Secretaría, con la finalidad primaria de atender eventos con reacción inmediata.

En el Reglamento de la presente Ley se establecerán los requisitos formales y tecnológicos para que se permita tal conexión.

Toda información obtenida con equipos o sistemas tecnológicos de particulares conectados al sistema implementado por la Secretaría, deberá recibir el tratamiento establecido en la presente Ley.

Artículo 18.- Las Instituciones de Seguridad Pública podrán convenir con instituciones similares de la Federación, otras Entidades Federativas o Municipios, la utilización conjunta de equipos y sistemas tecnológicos o procedimientos para la obtención de información, conforme a lo siguiente:

I. Los convenios a que se refiere este artículo, deben incluirse en el informe anual que rinda el Titular de la Secretaría, a la Asamblea Legislativa del Distrito Federal; y

II. La autoridad que suscriba el convenio, debe cerciorarse de que en los procesos de obtención, clasificación, análisis y custodia de información, referente a lugares del Distrito Federal, se observen los lineamientos que esta Ley dispone para la información obtenida por las Instituciones de Seguridad Pública del Distrito Federal.

Artículo 19.- Los permisionarios de servicios de seguridad privada en el Distrito Federal, que utilicen tecnología a través de la cual se capte información, tendrán las siguientes obligaciones:

I. Inscribir en el Registro establecido en esta Ley así como en el Registro de Servicios de Seguridad Privada la utilización de estos sistemas tecnológicos, conforme a la Ley de la materia;

La instalación de equipos o sistemas tecnológicos fijos en bienes de uso privado de la Federación o del Distrito Federal o de bienes particulares requerirá autorización por escrito de los titulares de esos derechos o de sus representantes legales, de la cual se remitirá copia certificada a la Secretaría;

Para instalar equipos o sistemas tecnológicos fijos en bienes de uso común del Distrito Federal o que, por su dirección o manejo, capten información acontecida en los mismos, el permisionario de servicios de seguridad privada solicitará autorización para ello a la Secretaría la que, en caso de proveer afirmativamente, asentará tal circunstancia en el Registro de Servicios de Seguridad Privada;

II. Remitir a la Secretaría, dentro de un término de 30 días hábiles, copia fiel e inalterada, de toda información obtenida con sus sistemas tecnológicos, en la forma y modalidades que se establezcan en el Reglamento respectivo;

III. Proporcionar a la Secretaría, en un plazo de cinco días hábiles contados a partir del momento en que se registró el hecho, copia fiel e inalterada, de toda información obtenida con sus sistemas tecnológicos, y que se relacione con las materias establecidas en el artículo 15 de la presente Ley, así como un informe emitido por el permisionario en donde, bajo protesta de decir verdad, se describan las circunstancias en que se captó dicha información, el tramo de la grabación, cinta o cualquier otro medio electrónico en el que se aprecian esos hechos así como una descripción de los mismos; No tendrán esta obligación los prestatarios de servicios de seguridad privada que obtengan información con los equipos o sistemas tecnológicos, registrados ante la Secretaría, y que capten hechos probablemente constitutivos de delito o conducta antisocial, perseguibles sólo por querella de parte ofendida; y

IV. Proporcionar a la Secretaría copia fiel e inalterada de toda información obtenida con sus sistemas tecnológicos, en un plazo de cinco días hábiles contados a partir del momento en que sea requerida por esa Dependencia. Dicha información se remitirá mediante documento suscrito bajo protesta de decir verdad por el permisionario.

Cuando cualquier autoridad judicial o administrativa del Distrito Federal necesite con motivo de sus funciones, la información a que hace referencia esta fracción, la solicitará a la Secretaría, la que desahogará el procedimiento para recabarla en términos del presente artículo.

Artículo 20.- En los procesos de clasificación, análisis, custodia y remisión a cualquier autoridad, de la información a que hace referencia el artículo anterior, la Secretaría atenderá lo establecido en los artículos 15 y 16 de esta Ley.

Artículo 21.- Los particulares tienen las obligaciones y limitaciones en la utilización de equipos o sistemas tecnológicos así como en la obtención, análisis, custodia y difusión de información captada con ellos, establecidas en la Constitución Política de los Estados Unidos Mexicanos así como en las Leyes federales y locales aplicables.

CAPÍTULO V
DE LA RESERVA, CONTROL, ANÁLISIS Y UTILIZACIÓN DE LA INFORMACIÓN OBTENIDA CON TECNOLOGÍA

Artículo 22.- Toda información obtenida por la Secretaría con el uso de equipos o sistemas tecnológicos, conforme a los lineamientos de la presente Ley, debe registrarse, clasificarse y tratarse de conformidad con lo establecido en la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.

Artículo 23.- Toda información recabada por la Secretaría, con arreglo a la presente Ley, se considerará reservada en los siguientes casos:

I. Aquella cuya divulgación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, sistemas, tecnología o equipos útiles a la generación de inteligencia para la prevención o el combate a la delincuencia en el Distrito Federal;

II. Aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza a la seguridad pública o las instituciones del Distrito Federal; y

III. La información y los materiales de cualquier especie que sean producto de una intervención de comunicaciones privadas autorizadas conforme a la Constitución Política de los Estados Unidos Mexicanos y las Leyes reglamentarias correspondientes.

Artículo 24.- Toda información recabada por la Secretaría con el uso de equipos o sistemas tecnológicos, independientemente de su clasificación, deberá ser remitida, con

los documentos a que hace referencia la presente Ley, a cualquier autoridad judicial o administrativa del Distrito Federal que la requiera para el cumplimiento de sus atribuciones.
La Secretaría sólo podrá requerir que se le informe el número de Averiguación Previa, asunto o expediente y autoridad ante la que se encuentra radicado el asunto para remitir, a la brevedad, la información solicitada.
Artículo 25.- La Secretaría debe garantizar la inviolabilidad e inalterabilidad de la información recabada con equipos o sistemas tecnológicos, mediante la Cadena de Custodia correspondiente.
Los servidores públicos que tengan bajo su custodia la información a que hace referencia este artículo, serán responsables directamente de su guarda, inviolabilidad e inalterabilidad, hasta en tanto no hagan entrega de la misma a otro servidor público, dando cuenta de dicho acto en el documento donde conste la Cadena de Custodia de la misma.
Artículo 26.- Los servidores públicos de la Secretaría que participen en la obtención, clasificación, análisis o custodia de información para la seguridad pública a través de tecnología, deberán abstenerse de obtener o guardar o transferir el original o copia de dicha información.
Asimismo, dichos servidores públicos deberán otorgar por escrito una promesa de confidencialidad que observarán en todo tiempo, aún después de que hayan cesado en el cargo en razón del cual se les otorgó el acceso.
Los servidores públicos del Ministerio Público, Autoridad especializada en Justicia para Adolescentes o Autoridad que ventile un procedimiento administrativo, seguido en forma de juicio, establecido en la normativa del Distrito Federal, deberán acatar las disposiciones de este artículo cuando, por razón de su encargo, conozcan o manejen información reservada a que hace referencia esta Ley y la Ley de Transparencia y Acceso a la Información Pública del Distrito Federal.
Artículo 27.- La inobservancia a lo dispuesto en los dos artículos precedentes, constituye responsabilidad administrativa grave, para los efectos de la Ley Federal de Responsabilidades de los Servidores Públicos, sin perjuicio de la sanción correspondiente al delito de ejercicio ilegal de servicio público, previsto en el Código Penal para el Distrito Federal.
Artículo 28.- La información obtenida por la Secretaría y por particulares, con el uso de los equipos o sistemas tecnológicos a que hace referencia la presente Ley, podrá utilizarse en el análisis de inteligencia para la prevención a través del diseño de los medios y productos a que hace referencia el Capítulo III de esta Ley.

CAPÍTULO VI
DE LOS MEDIOS DE PRUEBA OBTENIDOS CON EQUIPOS O SISTEMAS TECNOLÓGICOS

Artículo 29.- La información obtenida con equipos o sistemas tecnológicos obtenida en términos de esta Ley, constituye un medio de prueba en los procedimientos ministeriales y judiciales; de Justicia para Adolescentes; y, administrativos, seguidos en forma de juicio, establecidos en la normativa del Distrito Federal, con los que tenga relación.
Artículo 30.- La Secretaría deberá acompañar la información obtenida con equipos o sistemas tecnológicos regulados por esta Ley, autentificada por escrito, en las remisiones y puestas a disposición en que se considere necesario, precisando su origen y las circunstancias en que se allegó de ella.
Artículo 31.- La Secretaría deberá remitir la información obtenida con equipos o sistemas tecnológicos regulados por esta, en el menor tiempo posible, cuando le sea requerida por Ministerio Público; Autoridad Judicial; Autoridad Especializada en Justicia para Adolescentes; o Autoridad Administrativa, que ventile procedimiento, seguido en forma de juicio, establecidos en la normativa del Distrito Federal.

Artículo 32.- La información obtenida con equipos o sistemas tecnológicos por particulares o por Instituciones de Seguridad Pública Federales, de una Entidad Federativa diferente al Distrito Federal o Municipales, será solicitada, obtenida y valorada, en su caso, por el Ministerio Público, Autoridad Judicial o especializada en Justicia para Adolescentes, o Autoridad Administrativa que ventile procedimiento seguido en forma de juicio, establecido en la normativa del Distrito Federal, de conformidad con la Ley aplicable al caso.

Artículo 33.- Los medios de prueba obtenidos con equipos o sistemas tecnológicos por la Secretaría, podrán valorarse en un procedimiento ministerial o judicial; de Justicia para Adolescentes; o, administrativos, seguidos en forma de juicio, establecidos en la normativa del Distrito Federal, cuando reúnan los requisitos siguientes:

I. Se obtengan con estricto apego a los requisitos exigidos en la presente Ley; y

II. Se acompañen de un escrito de autentificación de la Secretaría que obtuvo la información, que deberá contener:

a) Descripción de las circunstancias de tiempo, modo y lugar en las que se obtuvo la información, especificando la tecnología utilizada y circunstancias particulares del proceso de obtención relevantes para la debida valoración e interpretación de la prueba, así como del o los servidores públicos que la recabaron, sus cargos y adscripciones;

b) Descripción detallada de los elementos visuales o de otra índole que se aprecian en la información obtenida con los equipos o sistemas tecnológicos así como transcripción de las partes inteligibles de los elementos sonoros contenidos en la misma;

c) Copia certificada de la Cadena de Custodia de la información obtenida;

d) Señalar expresamente que la información remitida no sufrió modificación alguna, sea por medio físico o tecnológico, que altere sus elementos visuales, sonoros o de otra índole; y

e) Firma del servidor público autorizado para ello por acuerdo del Titular de la Secretaría, mismo que debe ser publicado en la Gaceta Oficial del Distrito.

Artículo 34.- La información obtenida con equipos y sistemas tecnológicos a que hace referencia esta Ley hará prueba plena, salvo el caso en que, durante el transcurso del procedimiento correspondiente, se acredite que fue obtenida en contravención de alguna de las disposiciones de la presente Ley. En todo caso el juzgador apreciará el resultado de las pruebas de refutabilidad a que haya sido sometida para determinar su alcance probatorio.

El valor de la prueba tendrá alcance pleno sólo en cuanto a los hechos y circunstancias objetivos que se desprendan de la probanza obtenida por la Secretaría con el uso de equipos o sistemas tecnológicos; para todas las demás circunstancias, su alcance será indiciario.

CAPÍTULO VII
DE LA COORDINACIÓN PARA LA OBTENCIÓN E INTERCAMBIO DE INFORMACIÓN RECABADA CON EQUIPOS Y SISTEMAS TECNOLÓGICOS.

Artículo 35.- La información en poder de Instituciones de Seguridad Pública obtenida a través del uso de equipos o sistemas tecnológicos puede ser suministrada o intercambiada con la Federación, Estados y Municipios del país, de conformidad con la Constitución Política de los Estados Unidos Mexicanos, la Ley General que Establece las Bases de Coordinación del Sistema Nacional de Seguridad Pública, la Ley de Seguridad Nacional y la Ley de Seguridad Pública del Distrito Federal, conforme a los siguientes lineamientos:

I. La información recabada por la Secretaría a través del uso de equipos o sistemas tecnológicos, sólo puede ser suministrada o intercambiada cuando ésta reúna todos y cada uno de los requisitos exigidos en la presente Ley;

II. Dicha información puede proporcionarse tal y como se obtuvo de los equipos o sistemas tecnológicos y sólo se remitirá con los requisitos que establece el artículo 33 o cualquier otra especificación cuando así se pacte en el convenio respectivo;

III. La información obtenida por particulares a través del uso de equipos o sistemas tecnológicos, en poder de Instituciones de Seguridad Pública, sólo podrá ser materia de suministro o intercambio con la Federación, Estados o Municipios de los Estados Unidos Mexicanos, cuando se recabe conforme a lo establecido en el Capítulo IV y no violente las disposiciones del artículo 21 de esta Ley;

IV. Para la comunicación e intercambio con la Federación, Estados o Municipios de los Estados Unidos Mexicanos, de productos de inteligencia para la prevención de la delincuencia, en los que las Instituciones de Seguridad Pública hubieran analizado información obtenida a través del uso de equipos o sistemas tecnológicos, cualquiera que fuese el ente que la recabó, el Gobierno del Distrito Federal deberá vigilar que no se vulnere alguno de los requisitos exigidos en el artículo 16 ni se ponga en riesgo la seguridad de las Instituciones del Distrito Federal; y

V. No se autoriza el suministro o intercambio de información en poder de Instituciones de Seguridad Pública, obtenida a través del uso de equipos o sistemas tecnológicos, o de productos de inteligencia para la prevención, derivada de dicha información, con personas físicas o morales particulares de nacionalidad mexicana o extranjera, cualquiera que sea su naturaleza.

Artículo 36.- Se exceptúa de la prohibición contenida en la fracción IV del artículo anterior, a los permisionarios de servicios de seguridad privada, por lo que el Gobierno del Distrito Federal podrá suscribir con los mismos, convenio de suministración de información obtenida a través del uso de equipos o sistemas tecnológicos o productos de inteligencia para la prevención derivada de dicha información, conforme a lo siguiente:

I. Que los permisionarios de los servicios de seguridad privada cuenten con autorización, licencia, permiso o aviso de registro, vigente, expedido por la Secretaría;

II. Que el suministro de información o productos de inteligencia tenga como función principal la debida actuación de los permisionarios en el desempeño de sus servicios de seguridad privada, así como el combate a la delincuencia y otras conductas ilícitas, en ejercicio de sus actividades auxiliares o complementarias de la seguridad pública;

III. Que no existan antecedentes de haber incumplido las obligaciones de suministro de información, contenidas en esta Ley, así como la consistente en proporcionar apoyo y colaboración a las autoridades e Instituciones de Seguridad Pública, cuando éstas lo requieran en caso de emergencia, siniestro o desastre, conforme al artículo 32 de la Ley de Seguridad Privada para el Distrito Federal;

IV. Que las empresas de seguridad privada no hayan sido sancionadas en los últimos seis meses por la Secretaría, de conformidad con la Ley de Seguridad Privada para el Distrito Federal; y

V. Que el Gobierno del Distrito Federal procurará que con la suscripción del convenio no se beneficie indebidamente a un permisionario de servicios de seguridad privada en perjuicio de otros.

En caso de tratarse de un peligro inminente a la seguridad pública, el Gobierno del Distrito Federal podrá suscribir convenio de suministro de información con permisionarios de servicios de seguridad privada de forma provisional y urgente, siempre y cuando se reúnan los requisitos exigidos en las fracciones II y V del presente artículo.

Artículo 37.- Para realizar los suministros o intercambios a que hace referencia este capítulo, el Jefe de Gobierno de Distrito Federal por sí o a través del servidor público que designe para tal efecto, suscribirá los convenios correspondientes.
En dichos convenios, el Gobierno del Distrito Federal deberá garantizar que las autoridades que reciban la información obtenida a través del uso de equipos o sistemas tecnológicos, le proporcionen un trato igual al exigido en esta Ley, respetando en todo momento las Garantías Individuales y Derechos Humanos.
Artículo 38.- El Gobierno del Distrito Federal promoverá la suscripción de los convenios necesarios con la Federación, Estados y Municipios colindantes a efecto de unificar sus equipos y sistemas tecnológicos así como sus programas y políticas de utilización de los mismos, en el marco del Sistema Nacional de Seguridad Pública.
Asimismo, se procurará que estos equipos y sistemas tecnológicos se homologuen con las bases de datos metropolitanas y nacionales que se establezcan en el marco del Sistema Nacional de Seguridad Pública.
Artículo 39.- El Gobierno del Distrito Federal, en la suscripción de convenios de suministro o intercambio de información a que hace referencia este capítulo, atenderá prioritariamente los respectivos a las Entidades Federativas y Municipios colindantes, así como a los compromisos contraídos en el marco del Sistema Nacional de Seguridad Pública.
El proceso de suscripción de estos convenios, además de lo establecido en la presente Ley, atenderá a lo preceptuado en la Ley de Desarrollo Metropolitano para el Distrito Federal.
Artículo 40.- La información obtenida a través del uso de sistemas tecnológicos o los productos de inteligencia derivados del análisis a los mismos, proporcionados por otros órdenes de gobierno, deberá ser procesada y resguardada en los términos establecidos en la presente Ley.

CAPITULO VIII
DE LA FORMACIÓN DE UNA CULTURA DEL USO Y APROVECHAMIENTO DE TECNOLOGÍA

Artículo 41.- Todo sistema y equipo tecnológico relacionado con servicios de alertamiento al público, deberá contar previamente con un plan operativo, que establezca con precisión las acciones de coordinación entre Dependencias responsables, la participación que corresponde a la población, antes, durante y después de una situación de emergencia o desastre, de conformidad con la legislación aplicable en la materia de que se trate.
Artículo 42.- Las Instituciones de Seguridad Pública implementarán el método de procesamiento y validación de información estadística, que garantice la veracidad en los datos que reportan.
Las Instituciones de Seguridad Pública procurarán la estandarización de los criterios técnicos y de compatibilidad e interoperabilidad de sus respectivos equipos y sistemas tecnológicos, conforme a los convenios a que hace referencia esta Ley.
Artículo 43.- Para contribuir a la formación de una cultura preventiva en la población del Distrito Federal, las Instituciones de Seguridad Pública difundirán de manera permanente y actualizada, los índices delictivos y las zonas y colonias más peligrosas, acompañando dicha información con recomendaciones específicas para la autoprotección.
Artículo 44.- Para fomentar en la población una cultura vial y peatonal, las Instituciones de Seguridad Pública difundirán de manera permanente y actualizada información de las intersecciones más conflictivas, estadísticas de percances viales y sus causas que los ocasionan, acompañadas de recomendaciones específicas para la autoprotección.
Artículo 45.- En el informe anual a la Asamblea Legislativa del Distrito Federal, la Secretaría dará a conocer los resultados obtenidos en la seguridad pública, con la utilización de equipos y sistemas tecnológicos y su repercusión en las zonas de mayor

incidencia delictiva, de mayor comisión de faltas administrativas e intersecciones viales más conflictivas.

TRANSITORIOS.

PRIMERO.- Publíquese en la Gaceta Oficial del Distrito Federal y en el Diario Oficial de la Federación, para su mayor difusión.

SEGUNDO.- La presente Ley entrará en vigor al día siguiente de su publicación en la Gaceta Oficial del Distrito Federal. El registro establecido en la presente Ley, entrará en vigor a los 6 meses de su publicación en la Gaceta Oficial del Distrito Federal.

En el término de 90 días, la Asamblea Legislativa del Distrito Federal deberá armonizar los Códigos Procesales aplicables a lo establecido en esta Ley para la valoración de la información obtenida con equipos y sistemas tecnológicos.

TERCERO.- El Jefe de Gobierno del Distrito Federal, expedirá el Reglamento de esta Ley dentro de los 90 días naturales después de la publicación del presente Decreto en la Gaceta Oficial del Distrito Federal.

CUARTO.- El Jefe de Gobierno deberá constituir el Consejo Asesor en Ciencia y Tecnología para la Seguridad Pública, dentro del término de 90 días naturales contados a partir de la publicación de la presente Ley en la Gaceta Oficial del Distrito Federal.

QUINTO.- El Instituto de Ciencia y Tecnología del Distrito Federal deberá adecuar sus Estatutos, a más tardar dentro de los treinta días posteriores a la entrada en vigor de la presente ley, para establecer la Dirección General Adjunta en esta materia, responsable de ejecutar las atribuciones respectivas establecidas en esta Ley.

SEXTO.- El Jefe de Gobierno por conducto del Secretario de Finanzas, hará las previsiones necesarias en el Proyecto de Presupuesto de Egresos 2009, para someter a la aprobación de esta Asamblea Legislativa del Distrito Federal la dotación de los recursos necesarios para la operación de la presente Ley.

Recinto de la Asamblea Legislativa del Distrito Federal, a los nueve días del mes de octubre del año dos mil ocho.- POR LA MESA DIRECTIVA.- DIP. MARTÍN CARLOS OLAVARRIETA MALDONADO, PRESIDENTE.- SECRETARIO, DIP. BALFRE VARGAS CORTEZ.- SECRETARIA, DIP. MARÍA ELBA GÁRFIAS MALDONADO.- FIRMAS.

En cumplimiento de lo dispuesto por los artículos 122, apartado C, Base Segunda, fracción II, inciso b), de la Constitución Política de los Estados Unidos Mexicanos; 48, 49 y 67, fracción II, del Estatuto de Gobierno del Distrito Federal, para su debida publicación y observancia, expido el presente Decreto Promulgatorio, en la Residencia Oficial del Jefe de Gobierno del Distrito Federal, en la Ciudad de México, a los dieciséis días del mes de octubre del año dos mil ocho.-

EL JEFE DE GOBIERNO DEL DISTRITO FEDERAL, MARCELO LUIS EBRARD CASAUBON.-

FIRMA.

TRANSITORIOS DEL DECRETO POR EL QUE SE ADICIONAN DIVERSAS DISPOSICIONES A LA LEY QUE REGULA EL USO DE TECNOLOGÍA PARA LA SEGURIDAD PÚBLICA DEL DISTRITO FEDERAL, PUBLICADO EN LA GACETA OFICIAL DEL DISTRITO FEDERAL EL 6 DE JULIO DE 2012.

PRIMERO.- El presente decreto entrará en vigor al día siguiente de su publicación en la Gaceta Oficial del Distrito Federal.

SEGUNDO.- Publíquese en la Gaceta Oficial del Distrito Federal y para su mayor difusión en el Diario Oficial de la Federación[1].

[1] http://www.aldf.gob.mx/archivo-d0fb3cbb02f63ffc09643199ceb04011.pdf Página recuperada 31 de octubre de 2014

Glosario

°C. [Celcius]. Grados centrígrados de temperatura.

1.3M. [1.3 Megapixeles]. Resolución de video de 1280 x 1024 pixeles.

1080p. Nombre corto de video de alta definición con resolución de 1920 x 1080 pixeles con “scan progresivo”.

2CIF. Tamaño de imagen de 704 x 240 pixeles estandarizado por los fabricantes de CCTV en área de DVRs.

2M. [2 Megapixeles]. Resolución de video de 1600 x 1200 pixeles.

3DNR. [3 Digital Noise Reduction]. Reducción de ruido digital en la cámara.

3G. [3G]. Tercera generación en transmisión de datos, GPS, MMS, SMS que maneja 3.6Mbps de bajada y 384Kbps de subida.

4CIF. Tamaño de imagen de 704 x 480 pixeles estandarizado por los fabricantes de CCTV en área de DVR’S.

720p. Nombre corto de video de alta definición con resolución de 1280 x 720 pixeles con “scan progresivo”.

A1. Tecnología de SAMSUNG que incluye: 600TVL, XDR, , DIS, OSD, Zonas de Privacidad Poligonales, Detección de Movimiento.

ADPCM. [Adaptive Differential Pulse Code Modulation]. Codificación de audio en audiograbadoras y videograbadoras.

ADSL. [Asymmetric Digital Subscriber Line]. Red de datos soportada por medio de línea telefónica compartida con voz.

AE. [Auto Exposure]. Producto de multiplicar iluminancia por tiempo. Control de velocidad de obturación y el nivel de iluminación.

AES. [Automatic Electronic Shutter]. Control automático y electrónico de obturación e iris.

AGC. [Automatic Gain Control]. Control automático de ganancia que amplifica la señal de video en baja iluminación. Da un efecto de granulado.

AH. [Ampere-Hora]. Capacidad de suministro de corrriente por tiempo.

ALL IN ONE. Todo en Uno (Incluye cámara, unidad PTZ y Housing).

ARP. [Address Resolution Protocol]. Protocolo de resolución de direcciones. Protocolo de nivel de enlace responsable de encontrar la dirección de hardware que corresponde a determinada dirección.

ASPHERICAL. Lente no esférico que elimina aberraciones en la imagen.

ATM. [Automatic Teller Machine]. Cajero automático.

ATR. [Adaptive Tone Reproduction]. Proporciona una compensación para mejorar el contraste de los objetos durante casos en que en la misma imagen existan zonas de baja y alta luminosidad.

ATW. [Auto Tracing White Balance]. Variante predefinida del AWB (obtiene imagen con colores reales).

AutoFlip. Permite tener movimiento vertical de 180° con auto ajuste de imagen mecánico o digital para ver un plano derecho.

AVI. [Audio Video Interleaved]. Compresión de video y audio con calidad estándar.

AWB. [Automatic White Balance]. Balance de blancos automático que consigue una reproducción de color correcta sin que predomine ningún color en la imagen y se acerque lo más posible al color real.

AWC. [Automatic White Balance Compensation]. Característica predefinidadel balance de blancos que permite colores reales.

BLC. [Back Light Compensation]. Control de imágenes claras a contraluz.

BMP. [Bit Map Picture]. Formato de compresión de imagen. Puede variar desde 8 hasta 24 bits. (256 a 16.7 millones de colores).

BNC. [Barrel Network Connector]. Conector para CCTV aplicado a cable coaxial RG59 de impedancia de 75 Ω.

CCC. [Chinese Compulsory Certificate]. Certificación obligatoria China. Certificación china que obliga a fabricantes a construir productos electrónicos de calidad.

CCD. [Charged Coupled Device]. Dispositivo fotosensible que capta la imagen en la cámara. Se fabrican para B/N, Color, D/N.

CCIR. [Comité Consultatif International des Radiocommunications]. Señal de TV adecuada para operar en Europa, Asia y Brasil a 220Vca, 50Hz, B/N.

CD/M2. [Candel/meters2]. Cantidad de brillantez en monitores de LCD.

CDWR. [Compac Disc Writter]. Quemador de discos compactos (700MB).

CIF. [Common Interchange Format]. Tamaño de imagen en pixeles estandarizado por los fabricantes de CCTV en área de DVRs. (352 x 240 pixeles).

CLIP. Segmento de video tipo respaldo rápido.

CMOS. [Complementary Metal Oxide Semiconductor]. Dispositivo fotosensible que capta la imagen en la cámara, muy usado en cámaras IP y celulares.

COAXITRON®. Interface que permite la transmisión de video y datos en Domos PTZ por cable coaxial.

CODEC. [Coder and Encoder]. Describe una especificación capaz de codificar una señal original para motivos de transmisión, almacenaje o cifrado, y recuperarlo o descifrarlo del mismo modo para reproducción o manipulación.

CRT. [Catodic Ray Tube]. Cinescopio convencional con tubos de rayos catódicos.

D/N. [Day Night]. Función día y noche (color en día y blanco y negro en la noche).

D1. Máxima resolución de grabación en CCTV analógico. (720 x 480 pixeles).

dB. [Decibel]. Ganancia en unidades de señal.

DCP. [Death Pixel Cancelation]. Cancelación de Pixeles Muertos.

DDNS. [Dynamic Domain Name Server]. Servidor de servicios dinámicos asociados a un nombre fijo en direccionamiento IP no homologado.

DEPA. [Distributed Enhanced Processing Architecture]. Tecnologia de sistema de inteligente de videoanálisis de video con el que cuentan algunos modelos de cámaras SONY y su Software Real shot Manager.

DHCP. [Dynamic Host Configuration Protocol]. Permite el autodireccionamiento IP en redes de datos.

Dial-Up. Acceso vía módem telefónico.

DIP SWITCH. Componente electrónico con mini interruptores para cambios de función en cámaras, teclados, DVR, etc.

DIS. [Digital Image Stabilitation]. Estabilización de imagen cuando existe vibración en la cámara.

DIS HIKVISION. [Digital Image Sensor]. Integra al sensor de imagen y al DSP para proveer alta resolución, mejor procesamiento y menor consumo.

DNR. [Digital Noise Reduction]. Reducción de ruido digital en la cámara.

DSA. [Digital Self Adjusting]. Integra al sensor y al DSP.

DSP. [Digital Signal Procesor]. Procesador de la imagen capturada por los sensores de imagen.

DSS. [Digital Slow Shutter]. Reducción de la velocidad de captura para video en baja iluminación.

DVDRW. [Digital Versatil Disc Writer]. Unidad de lectura/escritura de DVD de 4.7GB.

DVI. [Digital Visual Interface]. Interfaz para video de alta resolución en pantallas LCD planas y proyectores; con resolución WUXGA 1920 x 1200 pixeles.

DVR. [Digital Video Recorder]. Videograbadora digital.

DVRNS.[Digital Video Recorder Name Server]. DDNS propietario de SYSCOM para direcciones IP dinámicas públicas.

D-Zoom. [Digital Zoom]. Acercamiento digital de una imagen.

EFFIO DSP. [Enhanced Features and Find Image Procesor]. Procesador que ofrece imagenes de alta resolución y características especiales como OSD, WDR, 3DNR. Existen varios tipos de EFFIO (S, P y E).

EHLC. [Excesive High Light Compensation]. Permite el enmascaramiento de zonas con alta iluminación de forma automática.

EI. [Electronic Iris]. Iris electrónico incorporado, sirve cuando se utilizan lentes de iris manual.

EIA. [Electronic Industries Asosiation]. Señal de TV adecuada para operar en América a 110Vca, 60Hz, B/N. EIA/TIA568 Esta norma especifica un sistema de cableado de telecomunicaciones genérico para edificios comerciales que soportará un ambiente multiproducto y multifabricante.

ELC. [Electronic Light Compensation]. Control de velocidad de captura de imágenes en relación con el shutter e iluminación (tiene sub menús).

Exterior. Indica que se encuentra fuera pero con cierto grado de protección (techo, marquesina, tejabán, etc.).

EXLUX. Función que permite ver a colores en condiciones de ultra baja iluminación (se reduce la velocidad del video).

Freeze. Congelado de imagen en algunos DVR's o cámaras especiales.

FTP. [File Transfer Protocol]. Protocolo de transferencia de archivos entre sistemas conectados a una red TCP. Se utiliza para compartición de archivos.

FULL DUPLEX. Configuración que permite la comunicación entre un equipo y otro de manera bidireccional y simultánea.

F-STOP. Apertura máxima en lente que permite pasar cierto porcentaje de luz (A mayor F-STOP menor cantidad de luz que permite pasar).

G711/G726. Es un estándar de la ITU-T para la compresión de audio.

GND. [Ground]. Tierra Física.

GPS. [Global Positioning System]. Sistema que permite determinar en todo el mundo la posición de un objeto, persona o vehículo con precisión de pocos metros. Consta de 32 satélites con trayectorias sincronizadas para cubrir toda la superficie terrestre.

GUI. [Graphic Unit Interface]. Medio con que el usuario se puede comunicar con una máquina, incluyendo DVRs. Normalmente esta interfaz suele de ser gráfica, fácil de entender y fácil de accionar.

H.264. [H.264 (MPEG4-10)]. Formato de compresión de video que no compromete calidad en video con el menor peso en datos procesados.

HAD. [Hole Acumulation Diode]. CCD de Alta Calidad SONY.

HALF DUPLEX. Comunicaion de Datos PTZ a dos hilos.

HB. [Heater and Blower]. Abanico y desempañador en gabinetes o housings.

HDD. [Hard Disk Drive]. Disco duro de almacenamiento de datos por medio magnético regrabable.

HDMI. [High Definition Multimedia interface]. Interface para transmisión de video y audio cifrado de alta definición con resoluciones desde 480i hasta 1080p.

HOME FUNCTION. Función de casa en domos que ejecuta un comando en tiempo de arranque programado (Preset, Tour, Scan, Pattern).

HOT KEY. Tecla directa para llamar una función o una macro en Controladores de cámaras PTZ o Matriciales.

Hot Swap. Permite intercambio amigable de discos duros sin necesidad de apagar el equipo.

HSBLC. [Highlight Supression BLC]. Permite el enmascaramiento de zonas con alta iluminación de forma automática.

HTTP. [Hyper Text Transfer Protocol]. Interfaz Web con texto y gráficos en Intranet e Internet .

HUB. Concentrador que en CCTV permite la centralización y transmisión de video, alimentación y datos PTZ por Módulos UTP.

HYPERLUX®. [Visión en Oscuridad sin LEDs]. Calidad con extremo detalle de imagen bajo cualquier tipo de iluminación.

ICR. [Infrared Cut Filter Removal]. Filtro sensible a la luz Infrarroja en cámaras día/noche real.

IDE. [Integrated Drive Electronics (ATA)]. Interface que controla los dispositivos de almacenamiento masivo como discos duros no volátil de 7200rpm.

IE. [Internet Explorer]. Explorador web de páginas HTML.

IEEExxx.xxb/g. [Institute Electric Electronic Engineers]. Procotolo de transferencia de datos en medios inalámbricos en bandas 2.4Ghz, 5.8Ghz; lo utilizan las cámaras IP por WiFi, Acces Point, ruteadores inalámbricos, etc.

IK10. Resistencia a impactos enérgicos. Norma capaz de soportar impactos de 20 Joules.

Intemperie. Se refiere al exterior sin protección de ningún tipo (a cielo abierto).

IO. [Input Output]. Dispositivo de entrada / salida.

IP. [Internet Protocol]. Protocolo de comunicación a través de una red de paquetes conmutados. En CCTV es usado para transmisión de video, audio y datos PTZ a calidad estándar y a alta definición.

IPv6. [Internet Protocolo Version 6]. Protocolo de internet mejorado que proporciona direcciones de internet propias a los dispositivos.

IPxx. [Ingress Protection]. Protección contra el ingreso de polvo o líquidos en cámaras, housings o gabinetes (Ver tabla al final del glosario de Términos).

IR. [Infrarred]. Luz infrarroja con frecuencia de luz que va desde los 715 hasta los 850 nm. Luz usada en cámaras, iluminadores y gabinetes de CCTV para visión en baja iluminación.

Iris Aut/DC. [Automatic Iris (Direct Control)]. Iris de lente tipo plug and play controlado automáticamente por cámaras tipo caja dependiendo del nivel de iluminación de la imagen.

J-BOX. [Junction Box]. Caja de conexiones en controladores PTZ (Incluye puertos RS-232, MUX y RS-485).

JOG. Palanca o Joystick en controladores PTZ.

JPEG. [Joint Photographic Experts Group]. Formato de compresión basado en imágenes en fotografía.

JUMPERS. Cables cortos para interconexión de equipos de video en CCTV con lazos en RG59 y conectores BNC.

Kbps. [K Bits Per Second]. Velocidad de datos en redes TCP/IP o ancho de banda medida en kilobits por segundo.

LAN. [Local Area Network]. Red de área local de datos.

LCD. [Liquid Cristal Display]. Monitor con pantalla de cristal líquido y resolución en pixeles.

LED. [Light Emition Diode]. Diodos emisores de luz infrarroja, blanca o de colores.

Linux. Sistema operativo multitarea cuya plataforma es utilizada en DVR´s autónomas.

LL. [Line Lock]. Permite la sincronía de la cámara con frecuencia de fuente de alimentación externa.

LOOP. Duplicado físico del canal de video para generar imagen.

LPR. [LLicense Plates Recognition]. Reconocimiento de placas vehiculares.

LUX. [Luxes]. Unidad de medida para iluminancia o nivel de iluminación. La iluminación mínima requerida para que la cámara vea está dada en luxes.

mA. [Mili Ampere]. Milésima parte de un ampere, unidad de medida de intensidad de corriente eléctrica.

MAP. Función de Mapa en Software para DVRs que permite crear un plano del edificio o área del usuario donde se agregar íconos representando la localización física de las cámaras y de donde se manda llamar el video de cada cámara.

MAT. [Motion Adaptive Transmission]. Transmisión de video adaptada al movimiento. Permite reducir la sobre carga del ancho de banda enviando menos cuadros por segundo cuando no es detectado movimiento. El sistema considera que no hay movimiento cuando no ha habido cambio alguno entre dos cuadros consecutivos.

MB. [Megabyte]. Unidad de medida de cantidad de datos informáticos. Equivale a 1 millón de bytes que a su vez cada byte equivale a 8 bits. Se utiliza para especificar la capacidad de almacenamiento de medios correspondientes.

Mbps. [Mega bit per second]. Unidad para cuantificar el caudal o ancho de banda de datos equivalente a 1000 kbps. Aunque estrictamente no lo es, suele ser referido como la velocidad de transmisión en una red.

MINIBANK. Archivo de video y audio ejecutable con reproductor incorporado.

mm. [Milímetro]. Milésima parte de un metro. En CCTV, es la unidad de medida de longitud focal de lentes. Varían ángulo de apertura y profundidad de zoom.

Mot. Det. [Motion Detection]. Detección de movimiento. La DVR detecta cuando existe movimiento en el campo de visión de las cámaras conectadas a ella comparando cada imagen con la anterior. Si existe algún cambio en alguno de los pixeles de la imagen, el sistema lo detecta como movimiento y actúa dependiendo de la configuración establecida por el usuario.

Motion Wavelet. Sistema de compresión propietario de AXXON.

MP. [Megapixel]. Un pixel es la mínima parte de una imagen y el producto de la cantidad de pixeles horizontales por la cantidad de éstos verticales es llamada resolución. Un megapixel es equivalente a 1 millón de pixeles y representa una imagen de alta resolución y calidad.

MPEG. [Moving Picture Experts Group]. Estándar internacional para compresión de video. MPEG-1 es un formato de baja resolución actualmente usado para videos pequeños en la red. MPEG-2 involucra más resolución y es usado en televisión digital y películas. MPEG-4. [Moving Picture Experts Group versión 4]. Algoritmo de compresión de video y gráficos. Esta versión resuelve la imagen más eficientemente y por lo tanto puede comprimir una secuencia más rápido y en un tamaño más pequeño.

MUX. [Multiplexer]. Dispositivo que puede recibir varias entradas y transmitirlas por un solo medio de transmisión. En CCTV se usa para poder monitorear señales de varias cámaras en un solo monitor.

MTBF. [Main Time Between Failures]. Tiempo Estimado de Fallas.

NAS. [Network Attached Storage]. Dispositivo de almacenamiento masivo para sistemas en red.

N/C. [Normally Close]. Contacto Normalmente Cerrado.

N/O. [Normally Open]. Contacto Normalmente Abierto.

NEMA. [National Electrical Manufacturers Association]. Asociación que estableció ciertos estándares dirigidos al encapsulamiento para protección contra condiciones ambientales como agua, polvo, aceites, etc.

NTSC. [National Television System Committee]. Señal de TV adecuada para operar en América a 110Vca, 60Hz, Color.

NVR. [Network Video Recorder]. Video Grabadoras de cámaras IP sobre redes de datos.

OGGVORBIS. Formato de compresión de audio.

ONVIF. [Open Network Videointerface Forum]. Es un estándar cuyo principal objetivo es facilitar la integración de varias marcas de equipo de video IP en red y ayudar a los fabricantes, desarrolladores de software y fabricantes independientes para asegurar la interoperabilidad de los productos.

OSD. [On Screen Display]. Permite ver menú gráfico de la cámara o DVR en pantalla.

PAL. [Phase Alternative Line]. Señal de TV adecuada para operar en Europa, Asia y Brasil a 220Vca, 50Hz, Color

PALANCA 3D. Joystick con palanca de movimiento en 3 posiciones, Pan-Tilt-Zoom.

PARK ACTION. [Funcion de casa]. Ejectuta un comando en tiempo de arranque programado (Preset, Tour, Scan, Pattern).

PATROL/PATTERN [Patron]. Memoriza movimientos normales de usuario en cámaras PTZ y los ejecuta posteriormente, manual o automáticamente.

PBP. [Picture by Picture]. Imagen por imagen.

PC Based. DVRs que operan sobre el sistema operativo Windows® Embedded.

PCM. [Pulse Code Modulation]. Compresión de audio para Audiograbadoras y Videograbadoras bajo muestreo de señal original análoga.

Pinhole. Lente miniatura con apertura del diámetro de un alfiler utilizado en cámaras ocultas.

PIP. [Picture In Picture]. Imagen dentro de Imagen.

PIR Camara. [Pasive Infrared]. Cámara Oculta en Sensor de Movimiento.

PoE. [Power over Ethernet]. Tecnología que incorpora alimentación eléctrica a una infraestructura LAN estándar. Permite alimentar un equipo o cámara IP por medio del mismo cable de datos UTP.

POP. [Picture over Picture]. Imagen sobre Imagen.

POS. [Point of Sale]. Punto de venta para inserción de texto (Cajas registradoras).

PPPoE. [Point to Point Protocol over Ethernet]. Servicio de banda ancha usado a través de cable módem tipo tunel.

PRESET. Posición predefinida de cámara PTZ por medio de programación. Punto de visualización preprogramado.

PSI. [Pound Square Inches]. Libras por pulgada cuadrada.

PTZ. [Pan Tilt Zoom]. Carácterística que tienen las cámaras con unidad motora para hacer movimientos en 3 dimensiones: Horizontal, vertical y zoom.

QCIF. Tamaño de imagen de 176 x 120 pixeles estandarizado por los fabricantes de CCTV en áreas de DVRs.

RAID. [Redundant Array of Independent Disks]. Sistema de almacenamiento que usa múltiples discos duros entre los cuales distribuye o replica los datos con el fin de mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad.

RAM. [Random Access Memory]. Memoria física dinámica en equipo de procesamiento de datos de cómputo. Permite que funcionen las aplicaciones o programas.

RCA. [Radio Corporation of America]. Conector analógico usado para video y audio en forma independiente.

RCM. [Reability Centered Maintenance]. Mantenimiento concentrado en seguridad. Certificación para desarrollar productos fáciles de dar mantenimiento.

Reconocimiento Facial. Reconocimiento de rostros humanos mediante un algoritmo por software integrado en los sistemas de CCTV.

RESET. Restablecimiento de funciones a un valor predeterminado.

RF. [Radio Frecuency]. Radiofrecuencia.

RJ45. Interfaz física comúnmente usada para conectar redes de cableado estructurado. Posee ocho "pines" o conexiones eléctricas. En CCTV es usado para fácil conexión de video y datos PTZ.

RS485. Interfaz serial de comunicaciones de la capa física del Modelo OSI. En CCTV es usada como protocolo de transmisión de datos en domos PTZ.También es utilizada para redes de datos.

RTP. [Real-Time Transport Protocol]. Protocolo de nivel de sesión utilizado para la transmisión de información en tiempo real, como por ejemplo video y audio en una videoconferencia.

RTSP. [Real Time Streaming Protocol]. Establece y controla uno o varios flujos sincronizados de datos ya sean de audio o video. El RTSP actúa como un mando a distancia mediante la red para servidores multimedia.

SASD. [Silicon Avalanche Diode]. Tecnologia: Diodo de avalancha de silicio, no se degrada al oponerse a las sobretenciones, a diferencia de otras tecnologías que se van degradando.

SATA. [Serial Advanced Technology Attachment]. Interfaz de transferencia de datos entre la tarjeta madre y algunos dispositivos de almacenamiento como discos duros. Esta interfaz permite mayores velocidades mejor rendimiento.

SCAN. Característica de los domos PTZ que permite al usuario definir un rango en el que el domo realice un movimiento panorámico horizontal.

SCSI. [Small Computers System Interface]. Interfaz de sistema para pequeñas computadoras. Interfaz estándar para la transferencia de datos entre dispositivos.

SDHC. [Secure Digital High Capacity]. Versión 2.0 de la memoria SD y es utilizada en dispositivos portátiles con capacidad desde 2 hasta 128 GB.

SDK. [Software Development Kit]. Paquetes de software que permiten a un desarrollador de software generar una aplicación concreta o derivada.

S.M.A.R.T. [Self Monitoring Analisis And Reporting Technology]. Autodetección de fallos de disco duro. Esta detección con anticipación permite al usuario tomar medidas antes de una pérdida de datos irrecuperable.

SENS UP. [Sens Up]. Ajuste de la velocidad de captura de video para captar imagen a color en muy baja iluminación.

SHUTTLE. Perilla para avance lento o rápido en reproducción de grabación en DVR's.

SHUTTER. Característica del CCD que controla el tiempo durante el cual llega la luz al CCD.

SIM. [Subscriber Identify Module]. Tarjeta inteligente desmontable que almacena de forma segura la clave de servicio del suscriptor usada para identificarse ante la red celular.

SMS. [Short message system]. Sistema para mensages de texto.

SMTP. Protocolo simple de transferencia de correo utilizado para el intercambio de mensajes de correos electrónicos salientes.

SO. [Sistema Operativo]. Software que actúa de interfaz entre dispositivos de hardware y el usuario para utilizar un equipo de cómputo.

SOAP. [Simple Objets Access Protocol]. Protocolo estándar que define como 2 objetos en diferentes procesos pueden comunicarse por medio de intercambio de datos xml. Administra recursos y actúa como intermediario para aplicaciones ejecutables. Algunos ejemplos son Windows, Linux, Mac OS.

SONY 960H CCD. Nuevo fotosensor Sony con 976 x 494 pixeles y 650 TVL.

SONY 760H CCD. Nuevo fotosensor Sony con 768 x 494 pixeles y 580 TVL.

SPDT. [Single Pole Double Throw]. Relevador Electrónico de 1 Polo 2 Tiros.

SPOT. Salida de video auxiliar secuencial en una DVR dada en BNC. Algunos modelos permiten una vista multiplexada.

SSL. [Secure Socket Layer]. Protocolo de Capa de Conexión Segura. Protocolo criptográfico que proporcionan comunicaciones seguras por una red, comúnmente Internet y correo electrónico.

SSNR. [Samsung Super Noise Reduction]. Tecnología desarrollada por Samsung que permite un mejor desempeño de la cámara en niveles bajos de iluminación reduciendo considerablemente el ruido.

Standalone. Equipo que opera sin asistencia o supervisión capaz de autorecuperar y regresar a su función predeterminada después de alguna pérdida de energía. En CCTV se dice que las DVRs basadas en LINUX son StandAlone, pues funcionan con el sistema cargado sobre una memoria Flash difícilmente accesible.

STP. [Shielded Twisted Pair]. Cable par trenzado que incluye una pantalla protectora por cada par, además de tener una lámina externa de aluminio o de cobre trenzado alrededor del conjunto de cables diseñada para reducir la absorción del ruido eléctrico.

S-Video. [Super-Video]. Tipo de señal analógica de video con más calidad que el video compuesto ya que dispone por separado de la información de brillo y la de color, mientras que en el video compuesto se encuentran juntas.

SV V. Tecnología de SAMSUNG de 600/650 TVL, SSNR, SSDR, Control Coaxial y WDR.

SW. [Software]. Programa generado para ser usado en computación o redes.

SWDR. [Super Wide Dynamic Range]. Ajuste Mejorado que permite operar con diferentes niveles de iluminación simultáneos (Mejora del WDR).

SYSCOM Cloud. Servicios de nombres de dominio que es soportado a través de conexiones UDP Hole Punching (Peer to Peer) y que ayuda a eliminar la apertura de puertos en ruteadores. No es efectivo con Firewalls ni con excepciones Peer to Peer como puede ser en proveedores de internet celular 3G.

TCP/IP. [Transfer Control Protocol/Internet Protocol]. Protocolo de transferencia de datos con respuesta de datos recibidos (redundante).

TEXT IN. Inserción de Texto de puntos de venta para ser desplegado en las grabaciones de la DVR.

TFT. [Thin Film Transistor]. Tipo especial de transistor fabricado a base de delgadas películas de un semiconductor activo. La principal aplicación de este transistor es la fabricación de pantallas de cristal líquido como celulares y monitores pequeños.

TOUCHSCREEN. Pantalla que mediante un toque directo sobre su superficie permite la entrada de datos y órdenes al dispositivo. En CCTV se utiliza para control por contacto dactilar en Joystick de cámaras PTZ.

TOUR. Característica de los domos PTZ que permite secuenciar los presets que el usuario requiera con velocidad y tiempo por preset configurables.

TUV-GS. Certificación de que es un producto seguro. Aprobado por la ley de seguridad para equipos Alemanes.

TVL. [TV Lines]. Especificación que establece cuántas líneas pueden ser vistas en cierta área delimitada. Es utilizada para medir la resolución de cada cámara. A más líneas, mayor resolución.

TX/RX. [Transmition/Reception]. Transmisión y recepción.

UDP. [User Datagram Protocol]. Protocolo que permite el envío de datagramasa través de la red sin haber establecido una conexión previa.

UL. [Underwriters Laboratories]. Certificación en equipos electrónicos que son seguros para el medio ambiente.

No tiene confirmación de control de flujo ni de recepción.

USB. [Universal Serial Bus]. Especificación que establece comunicación serial entre dispositivos periféricos y un equipo de cómputo.

uPnP. [Universal Plug and Play]. Permite interoperabilidad entre dispositivos con esta característica (DVRs y Routers) de forma libre y sincronizada, incluso sin abrir puertos de comunicación.

Maneja velocidades de hasta 480 Mbps (60MB/s) en versión 2.0.

UTP. [Unshielded Twisted Pair]. Cable de par trenzado utilizado para transmisión de datos que consiste en dos alambres de cobre aislado que se trenzan en forma helicoidal con el fin de reducir y cancelar el campo electromagnético generado por la circulación de electrones en el medio, y a su vez, reducción de ruido eléctrico.

UV. [Ultra Violet]. Rayos ultravioleta.

VCR. [Video Cassette Recorder]. Tipo de magnetoscopio que utiliza videocinta extraíble que contiene una cinta magnética para grabar audio y video.

Se utilizaba en CCTV para grabaciones.

VCD. [Direct Current Voltage]. Voltaje en Coriente Directa.

VCA. [Altern Current Voltage]. Voltaje en Corriente Alterna.

VGA. [Video Graphics Array]. Sistema gráfico de pantallas para PC y DVRs.

Maneja una resolución de 640 x 480 pixeles. Así también se le llama al conector utilizado de 15 pines.

VLAN. [Virtual LAN]. Red de acceso local virtual.

VPD. [Video Power and Data]. Interfaz que permite la transmisión de video, alimentación y datos PTZ a través del mismo cable UTP.

VTDU. Unidad de transferencia de video de dispositivos móviles propietaria de HIKVISION.

W. [Watts]. Unidad de consumo y/o potencia.

WAN. [Wide Area Network]. Red informática que se extiende sobre un área geográfica extensa. Es la comunicación e interacción entre dos o más LAN.

WATCHDOG. Mecanismo de seguridad que provoca un reset del sistema en caso de que éste se haya bloqueado.

WDI. Tecnología propietaria de HIKVISION que cumple con los estándares más altos de calidad y orientado a la grabación de cámaras de ultra alta resolución que va de las 600 a las 750 TVL sin perder ningún detalle de la imagen.

WDR. [Wide Dynamic Range]. Ajuste que permite operar con diferentes niveles de iluminación simultáneos.

WDR Doble Escaneo. WDR Mejorado, tambinén llamado sWDR.

WEB. [World Wide Web]. Sistema de documentos de hipertexto (texto que conduce a otro texto relacionado) enlazados y accesibles a través de Internet.

WiFi. [Wireless Fidelity]. Tecnología inalámbrica a base de ondas de radiofrecuencia para proveer conexiones de red e Internet a dispositivos con una tarjeta de red WiFi. La tecnología está basada en estándares 802.11 propuestos por el "Institute of Electrical and Electronics Engineers" (IEEE).

W V. Tecnología de SAMSUNG de 600 TVL, SSNR, SSDR y Control Coaxial.

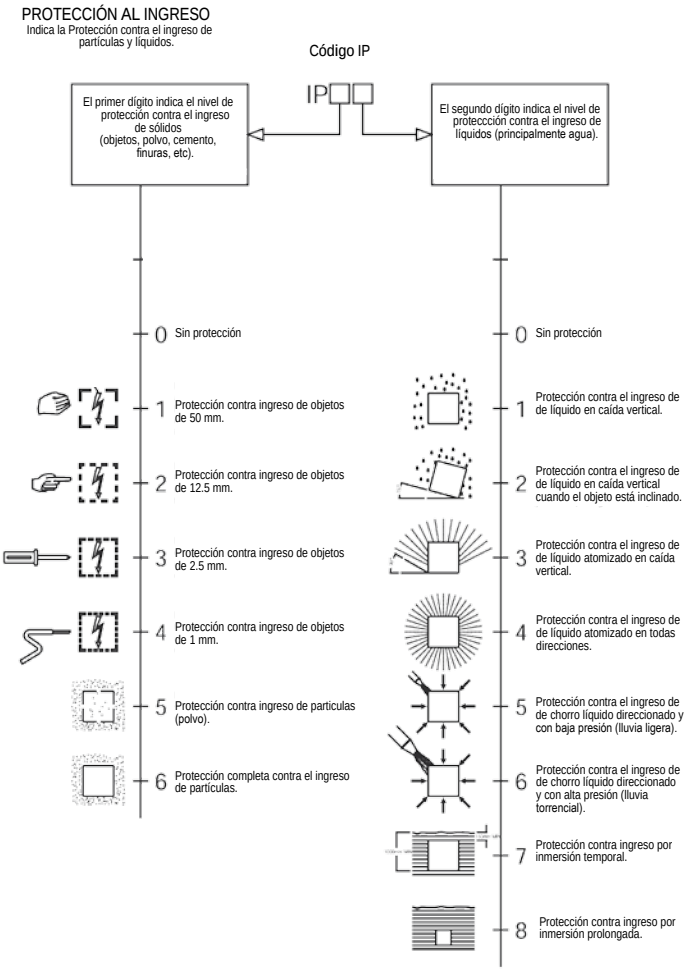
XDR. [Extended Dinamic Range]. Compensación de bajos niveles de iluminación Extendido.

xG. Norma para Impacto en cámaras y housings de CCTV.

xxVA. [Volt Ampere]. Unidad de potencia en transformadores de CA de pared.

Y/C. Salida de video a 75Ω 1Vpp.

Ω. [Ohoms]. Unidad de medida de resistencia eléctrica mejor conocido como impedancia.



Bibliografia

1. Albusac Jiménez Javier Alonso, Vigilancia Inteligente: Modelado de Entornos Reales e Interpretación de Conductas para la Seguridad. Universidad de Castilla-La Mancha 9 de Julio del 2008
2. Biticino Circuito cerrado de televisión, Guía técnica 10
3. Espinoza Palacios Julio Enrique. Desarrollo de un circuito cerrado de televisión en un local comercial, Unidad Académica de Ingeniería Eléctrica Zacatecas, Zac., 11 de noviembre de 2011.
4. DVR User Manual, For H.264 4/8/16-channel digital video recorder All rights reserved
5. Filipo rugeles, Fundamentos de diseño para un circuito cerrado de televisión Scientia Et Technica, vol. XV, núm. 42, agosto, 2009, pp. 46-547 Universidad Tecnológica de Pereira Pereira, Colombia.
6. Fundamentos de diseño para un circuito cerrado de televisión, Scientia Et Technica, vol. XV, núm. 42, agosto, 2009, pp. 46-50 Universidad Tecnológica de Pereira Pereira, Colombia
7. Gómez González Emilio, Guía básica de conceptos de óptica geométrica, Departamento de Física Aplicada III E.S. Ingenieros, Universidad de Sevilla, 2006/07
8. Montalvo Arenas César Eduardo, Óptica agosto de 2010. http://goo.gl/AQI9Pd
9. Rivas Cruz Juan Antonio, Implementación de sistema de seguridad con video-vigilancia y software libre. Instituto politécnico nacional escuela superior de ingeniería mecánica y eléctrica unidad profesional "Adolfo López mateos".15 de julio de 2012.
10. Syscom. Sistema de Vigilancia para Vialidad y Sitios Remotos, Sistema de Videograbación en el Sitio
11. Téllez Valdés Julio, La regulación jurídica de la videovigilancia bajo una perspectiva de derecho comparado, http://www.juridicas.unam.mx/

Referencias Electrónicas

1. http://laprimeraplana.com.mx/2011/10/07/publican-video-con-mujeres-peleando-y-cayendo-a-las-vias-del-metro/ , Pagina recuperada Septiembre 16 2014
2. http://www.e-guarderias.com/funciona.php , Página recuperada Septiembre 16 2014
3. http://www.sc.ehu.es/sbweb/fisica/cursoJava/fundamentos/clases1/arays.htm Página recuperada Septiembre 16 2014
4. http://www.taringa.net/posts/info/13327840/Errores-comunes-en-las-camaras-de-seguridad-CCTV.html Página recuperada, Septiembre 20 2014
5. www.bticino.com.mx/index.php?id=810 Página recuperada, Septiembre 20 2014
6. http://www.dvrdydns.com/ Página recuperada 31 de octubre de 2014

7. http://ftp3.syscom.mx/usuarios/ftp/GUIASEG2014/01_SECCION_SOLUCIONES.pdf,Página recuperada 31 de octubre de 2014
8. http://www.aldf.gob.mx/archivo-d0fb3cbb02f63ffc09643199ceb04011.pdf Página recuperada 31 de octubre de 2014